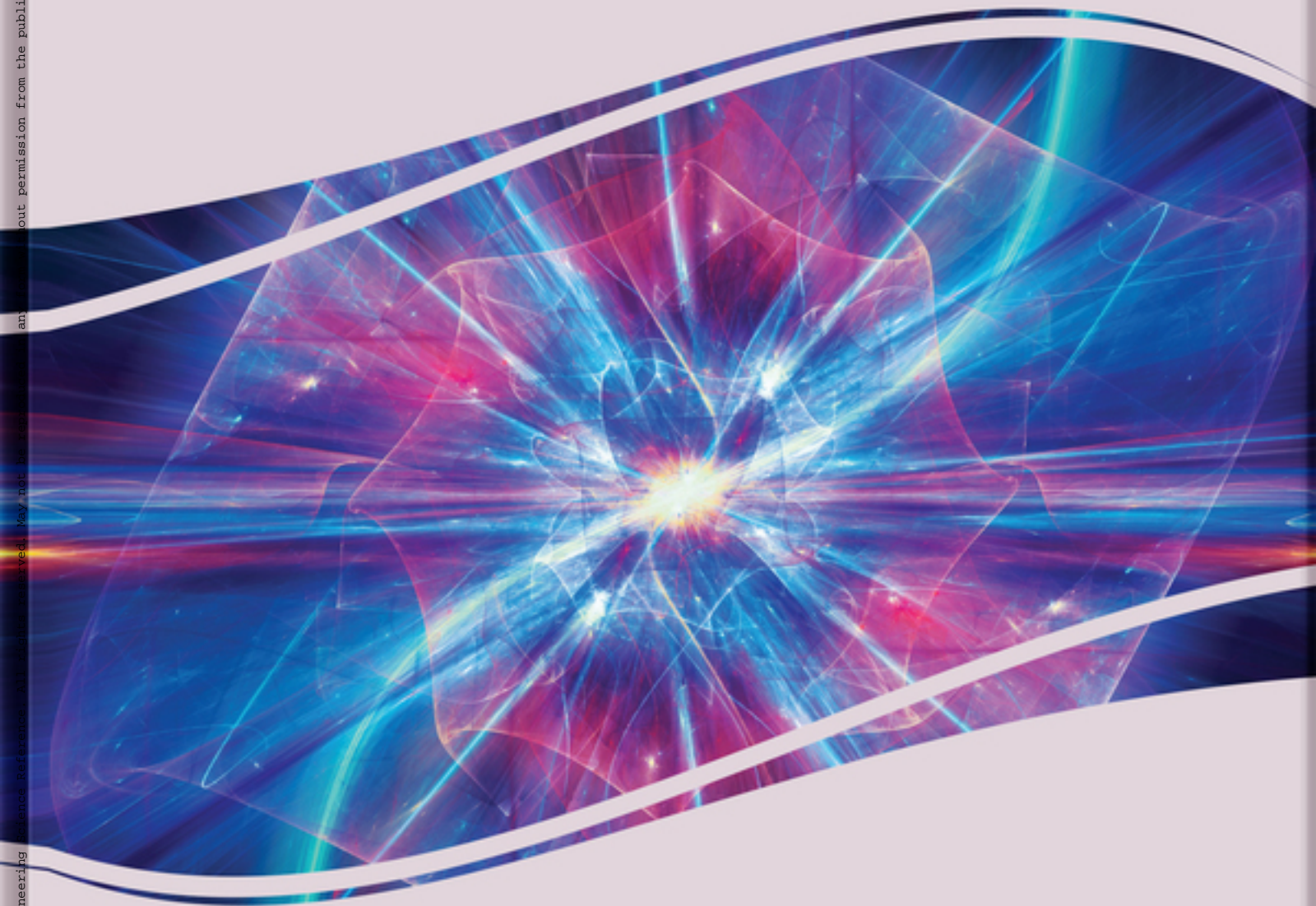


Critical Explorations

Research Anthology on Advancements in Quantum Technology



Information Resources Management Association



Copyright 2021. Engineering Science Reference. All rights reserved. May not be reproduced without permission from the publisher, except fair uses permitted under U.S. or applicable copyright law.

Research Anthology on Advancements in Quantum Technology

Information Resources Management Association
USA



Published in the United States of America by

IGI Global
Engineering Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA, USA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: <http://www.igi-global.com>

Copyright © 2021 by IGI Global. All rights reserved. No part of this publication may be reproduced, stored or distributed in any form or by any means, electronic or mechanical, including photocopying, without written permission from the publisher. Product or company names used in this set are for identification purposes only. Inclusion of the names of the products or companies does not indicate a claim of ownership by IGI Global of the trademark or registered trademark.

Library of Congress Cataloging-in-Publication Data

Names: Information Resources Management Association, editor.

Title: Research anthology on advancements in quantum technology /
Information Resources Management Association, editor.

Description: Hershey, PA : Engineering Science Reference, [2021] |

“One-volume reference collection of reprinted IGI Global book chapters and journal articles”--Preface. | Includes bibliographical references and index. | Summary: “This reference book will empower computer scientists, engineers, professionals, researchers, students, and practitioners with an advanced understanding of critical issues and advancements within quantum technology”-- Provided by publisher.

Identifiers: LCCN 2021014368 (print) | LCCN 2021014369 (ebook) | ISBN 9781799885931 (h/c) | ISBN 9781799887386 (eISBN)

Subjects: LCSH: Quantum computing.

Classification: LCC QA76.889 .R47 2021 (print) | LCC QA76.889 (ebook) |
DDC 006.3/843--dc23

LC record available at <https://lcn.loc.gov/2021014368>

LC ebook record available at <https://lcn.loc.gov/2021014369>

British Cataloguing in Publication Data

A Cataloguing in Publication record for this book is available from the British Library.

The views expressed in this book are those of the authors, but not necessarily of the publisher.

For electronic access to this publication, please contact: eresources@igi-global.com.

Editor-in-Chief

Mehdi Khosrow-Pour, DBA
Information Resources Management Association, USA

Associate Editors

Steve Clarke, *University of Hull, UK*
Murray E. Jennex, *San Diego State University, USA*
Ari-Veikko Anttiroiko, *University of Tampere, Finland*

Editorial Advisory Board

Sherif Kamel, *American University in Cairo, Egypt*
In Lee, *Western Illinois University, USA*
Jerzy Kisielnicki, *Warsaw University, Poland*
Amar Gupta, *Arizona University, USA*
Craig van Slyke, *University of Central Florida, USA*
John Wang, *Montclair State University, USA*
Vishanth Weerakkody, *Brunel University, UK*

List of Contributors

Agrawal, Nishtha / <i>RCC Institute of Information Technology, India</i>	197
Aguilar, Roman Rodriguez / <i>Universidad Panamericana, Escuela de Ciencias Económicas y Empresariales, Ciudad de México, Mexico</i>	93
Amirtharajan R. / <i>Shanmugha Arts, Science, Technology, and Research Academy (Deemed), India</i>	302
Bansal, Sulabh / <i>School of Computing and Information Technology, Manipal University Jaipur, Jaipur, India</i>	22, 51
Basu, Abhishek / <i>RCC Institute of Information Technology, India</i>	127
Bhargavi, K. / <i>Siddaganga Institute of Technology, India</i>	355
Bhatia, Amandeep Singh / <i>Center for Quantum Computing, Peng Cheng Laboratory, China</i>	267
Bhattacharyya, Siddhartha / <i>RCC Institute of Information Technology, India</i>	164, 197
Cames, Olaf / <i>University of Liverpool, UK</i>	387
Chaiboonsri, Chukiat / <i>Chiang Mai University, Thailand</i>	400
Chander, Bhanu / <i>Pondicherry University, India</i>	325
Chattopadhyay, Avik / <i>University of Calcutta, India</i>	127
Das, Sunanda / <i>University Institute of Technology, India</i>	164
De, Sourav / <i>Cooch Behar Government Engineering College, India</i>	164
Dilip, Kumar / <i>Jawaharlal Nehru University, India</i>	228
Drury-Grogan, Meghann L. / <i>Fordham University, USA</i>	387
Goyal, Dinesh / <i>Suresh Gyan Vihar University, Jaipur, India</i>	111
Gupta, Amit Kumar / <i>Suresh Gyan Vihar University, Jaipur, India</i>	111
Kar, Suman Kalyan / <i>Sikkim Manipal Institute of Technology, India</i>	435
Konar, Debanjan / <i>Sikkim Manipal Institute of Technology, India</i>	435
Kumar, Sanjay / <i>NIT Jamshedpur, Jamshedpur, India</i>	289
Lekehali, Somia / <i>University of M'sila, M'Sila, Algeria</i>	447
Litvinchev, Igor / <i>Nuevo Leon State University, San Nicolás de los Garza, Mexico</i>	93
Mahdi, Fahad Parvez / <i>University of Hyogo, Kobe, Japan</i>	93
Marmolejo-Saucedo, Jose Antonio / <i>Universidad Panamericana, Facultad de Ingeniería, Ciudad de México, Mexico</i>	93
Motaghi, Hamed / <i>University of Quebec in Outaouais, Canada</i>	416
Moussaoui, Abdelouahab / <i>University of Ferhat Abbas Setif 1, El Bez, Algeria</i>	447
Pal, Pankaj / <i>RCC Institute of Information Technology, India</i>	197
Patvardhan, C. / <i>Faculty of Engineering, Dayalbagh Educational Institute (DEI), Agra, India</i>	22, 51
Paul, Surjit / <i>IIT Kharagpur, Kharagpur, India</i>	289
Pljonkin, A. P. / <i>Southern Federal University, Taganrog, Russia</i>	345

Praveenkumar, Padmapriya / <i>Shanmugha Arts, Science, Technology, and Research Academy (Deemed), India</i>	302
Rathee, Manisha / <i>Jawaharlal Nehru University, India</i>	228
Rathee, Ritu / <i>Indira Gandhi Delhi Technical University for Women, India</i>	228
Roy, Subhrajit Sinha / <i>Global Institute of Management and Technology, India</i>	127
Santhiyadevi R. / <i>Shanmugha Arts, Science, Technology, and Research Academy (Deemed), India</i>	302
Sathish Babu B. / <i>RV College of Engineering, Bangalore, India</i>	355
Starcevic, Ana / <i>University of Belgrade, Serbia</i>	378
Stojanovic, Aleksandar / <i>Federal University of Ceara, Brazil</i>	378
Subramanya, K. N. / <i>RV College of Engineering, Bangalore, India</i>	355
Suman, Rajiv Ranjan / <i>NIT Jamshedpur, Jamshedpur, India</i>	289
Thakkar, Manan Dhaneshbhai / <i>U. V. Patel College of Engineering, Ganpat University, India</i>	247
Torres, Beatriz / <i>University of Quebec in Outaouais, Canada</i>	416
Valverde, Raul / <i>Concordia University, Canada</i>	416
Vanzara, Rakesh D. / <i>U. V. Patel College of Engineering, Ganpat University, India</i>	247
Vasant, Pandian / <i>Department of Fundamental and Applied Sciences, Universiti Teknologi PETRONAS, Seri Iskandar, Malaysia</i>	93
Wannapan, Satawat / <i>Chiang Mai University, Thailand</i>	400
Watada, Junzo / <i>Universiti Teknologi Petronas, Seri Iskandar, Malaysia</i>	93
Wu, Shuyue / <i>School of Information Science & Engineering, Hunan International Economics University, Changsha, China</i>	1
Yadav, Narendra Singh / <i>JECRC University, Jaipur, India</i>	111
Zheng, Shenggen / <i>Center for Quantum Computing, Peng Cheng Laboratory, China</i>	267

Table of Contents

Preface..... X

Section 1 Algorithms and Techniques

Chapter 1

A Quantum Particle Swarm Optimization Algorithm Based on Self-Updating Mechanism 1
Shuyue Wu, School of Information Science & Engineering, Hunan International Economics University, Changsha, China

Chapter 2

An Improved Generalized Quantum-Inspired Evolutionary Algorithm for Multiple Knapsack Problem..... 22
Sulabh Bansal, School of Computing and Information Technology, Manipal University Jaipur, Jaipur, India
C. Patvardhan, Faculty of Engineering, Dayalbagh Educational Institute (DEI), Agra, India

Chapter 3

A Generalized Parallel Quantum Inspired Evolutionary Algorithm Framework for Hard Subset Selection Problems: A GPQIEA for Subset Selection..... 51
Sulabh Bansal, School of Computing and Information Technology, Manipal University Jaipur, Jaipur, India
C. Patvardhan, Department of Electrical Engineering, Dayalbagh Educational Institute, Agra, India

Chapter 4

Quantum-Behaved Bat Algorithm for Solving the Economic Load Dispatch Problem Considering a Valve-Point Effect 93
Pandian Vasant, Department of Fundamental and Applied Sciences, Universiti Teknologi PETRONAS, Seri Iskandar, Malaysia
Fahad Parvez Mahdi, University of Hyogo, Kobe, Japan
Jose Antonio Marmolejo-Saucedo, Universidad Panamericana, Facultad de Ingeniería, Ciudad de México, Mexico
Igor Litvinchev, Nuevo Leon State University, San Nicolás de los Garza, Mexico
Roman Rodriguez Aguilar, Universidad Panamericana, Escuela de Ciencias Económicas y Empresariales, Ciudad de México, Mexico
Junzo Watada, Universiti Teknologi Petronas, Seri Iskandar, Malaysia

Chapter 5

- Design and Performance Evaluation of Smart Job First Multilevel Feedback Queue (SJFMLFQ) Scheduling Algorithm With Dynamic Smart Time Quantum 111
Amit Kumar Gupta, Suresh Gyan Vihar University, Jaipur, India
Narendra Singh Yadav, JECRC University, Jaipur, India
Dinesh Goyal, Suresh Gyan Vihar University, Jaipur, India

Chapter 6

- Hardware Implementation of a Visual Image Watermarking Scheme Using Qubit/Quantum Computation Through Reversible Methodology 127
Subhrajit Sinha Roy, Global Institute of Management and Technology, India
Abhishek Basu, RCC Institute of Information Technology, India
Avik Chattopadhyay, University of Calcutta, India

Chapter 7

- True Color Image Segmentation Using Quantum-Induced Modified-Genetic-Algorithm-Based FCM Algorithm 164
Sumanda Das, University Institute of Technology, India
Sourav De, Cooch Behar Government Engineering College, India
Siddhartha Bhattacharyya, RCC Institute of Information Technology, India

Chapter 8

- Grayscale Image Segmentation With Quantum-Inspired Multilayer Self-Organizing Neural Network Architecture Endorsed by Context Sensitive Thresholding 197
Pankaj Pal, RCC Institute of Information Technology, India
Siddhartha Bhattacharyya, RCC Institute of Information Technology, India
Nishtha Agrawal, RCC Institute of Information Technology, India

Chapter 9

- DNA Fragment Assembly Using Quantum-Inspired Genetic Algorithm..... 228
Manisha Rathee, Jawaharlal Nehru University, India
Kumar Dilip, Jawaharlal Nehru University, India
Ritu Rathee, Indira Gandhi Delhi Technical University for Women, India

Section 2

Cryptography, Encryption, and Security

Chapter 10

- Quantum Internet and E-Governance: A Futuristic Perspective..... 247
Manan Dhaneshbhai Thakkar, U. V. Patel College of Engineering, Ganpat University, India
Rakesh D. Vanzara, U. V. Patel College of Engineering, Ganpat University, India

Chapter 11

- Post-Quantum Cryptography and Quantum Cloning..... 267
Amandeep Singh Bhatia, Center for Quantum Computing, Peng Cheng Laboratory, China
Shenggen Zheng, Center for Quantum Computing, Peng Cheng Laboratory, China

Chapter 12

- A Quantum Secure Entity Authentication Protocol Design for Network Security 289
Surjit Paul, IIT Kharagpur, Kharagpur, India
Sanjay Kumar, NIT Jamshedpur, Jamshedpur, India
Rajiv Ranjan Suman, NIT Jamshedpur, Jamshedpur, India

Chapter 13

- Medical Data Are Safe: An Encrypted Quantum Approach..... 302
Padmapriya Praveenkumar, Shanmugha Arts, Science, Technology, and Research Academy (Deemed), India
Santhiyadevi R., Shanmugha Arts, Science, Technology, and Research Academy (Deemed), India
Amirtharajan R., Shanmugha Arts, Science, Technology, and Research Academy (Deemed), India

Chapter 14

- Quantum Cryptography Key Distribution: Quantum Computing..... 325
Bhanu Chander, Pondicherry University, India

Chapter 15

- Vulnerability of the Synchronization Process in the Quantum Key Distribution System 345
A. P. Pljonkin, Southern Federal University, Taganrog, Russia

Chapter 16

- Optimal Parameter Prediction for Secure Quantum Key Distribution Using Quantum Machine Learning Models 355
Sathish Babu B., RV College of Engineering, Bangalore, India
K. Bhargavi, Siddaganga Institute of Technology, India
K. N. Subramanya, RV College of Engineering, Bangalore, India

Section 3

Industry Applications of Quantum Technology

Chapter 17

- Quantum Cognition and Its Influence on Decrease of Global Stress Level Related With Job Improvement Strategies: Quantum Brain and Global Stress 378
Aleksandar Stojanovic, Federal University of Ceara, Brazil
Ana Starcevic, University of Belgrade, Serbia

Chapter 18

- Complex Action Methodology for Enterprise Systems (CAMES): A System to Contextualize the Behavioral Management Issue as Quantum Mechanical Variable..... 387
Olaf Cames, University of Liverpool, UK
Meghann L. Drury-Grogan, Fordham University, USA

Chapter 19

Multi-Process Analysis and Portfolio Optimization Based on Quantum Mechanics (QM) Under Risk Management in ASEAN Exchanges: A Case Study of Answering to the E-Commerce and E-Business Direction 400
Chukiat Chaiboonsri, Chiang Mai University, Thailand
Satawat Wannapan, Chiang Mai University, Thailand

Chapter 20

A Quantum NeuroIS Data Analytics Architecture for the Usability Evaluation of Learning Management Systems 416
Raul Valverde, Concordia University, Canada
Beatriz Torres, University of Quebec in Outaouais, Canada
Hamed Motaghi, University of Quebec in Outaouais, Canada

Chapter 21

An Efficient Handwritten Character Recognition Using Quantum Multilayer Neural Network (QMLNN) Architecture: Quantum Multilayer Neural Network 435
Debanjan Konar, Sikkim Manipal Institute of Technology, India
Suman Kalyan Kar, Sikkim Manipal Institute of Technology, India

Chapter 22

Quantum Local Binary Pattern for Medical Edge Detection 447
Somia Lekehali, University of M'sila, M'Sila, Algeria
Abdelouahab Moussaoui, University of Ferhat Abbas Setif 1, El Bez, Algeria

Index..... 466

Preface

Quantum technology can create many improvements in everyday technology with multi-industry applications that are both widespread and diverse. It is the latest way to create computing power, increase secure communications, and surpass the capabilities of modern supercomputers. With the quick rate to solve problems, quantum technology goes beyond the human hand and older methods of computing to perform algorithms at an impressive rate. With new speeds, new problem-solving capabilities, and new technologies, quantum technology will forever change the face of computing. The latest tools, technologies, and applications of quantum technology are an essential discussion for both modern computing and the future of technology.

Thus, the *Research Anthology on Advancements in Quantum Technology* seeks to fill the void for an all-encompassing and comprehensive reference book covering the emerging research, concepts, and theories for preventing, identifying, and mitigating the spread of fake news both within a human and technological context. This one-volume reference collection of reprinted IGI Global book chapters and journal articles that have been handpicked by the editor and editorial team of this research anthology on this topic will empower computer scientists, engineers, professionals, researchers, students, and practitioners with an advanced understanding of critical issues and advancements within quantum technology.

The *Research Anthology on Advancements in Quantum Technology* is organized into three sections that provide comprehensive coverage of important topics. The sections are:

1. Algorithms and Techniques;
2. Cryptography, Encryption, and Security; and
3. Industry Applications of Quantum Technology.

The following paragraphs provide a summary of what to expect from this invaluable reference tool.

Section 1, “Algorithms and Techniques,” opens this comprehensive reference work with research on the methods and algorithms used in quantum technology. The opening chapter for this reference book, “A Quantum Particle Swarm Optimization Algorithm Based on Self-Updating Mechanism,” by Prof. Shuyue Wu of Hunan International Economics University, Changsha, China, describes the quantum behavior particle swarm (QPSO) algorithm and the importance of the aging mechanism. The following chapter, “An Improved Generalized Quantum-Inspired Evolutionary Algorithm for Multiple Knapsack Problem,” by Prof. Sulabh Bansal of Manipal University Jaipur, Jaipur, India and Prof. C. Patvardhan of Dayalbagh Educational Institute (DEI), Agra, India, describes how the 0/1 multiple knapsack problem (MKP), a generalization of popular 0/1 knapsack problem, is NP-hard and harder than the simple knapsack problem. Next, “A Generalized Parallel Quantum Inspired Evolutionary Algorithm Framework for Hard Subset Selection Problems: A GPQIEA for Subset Selection” by Prof. Sulabh Bansal of Manipal

Preface

University Jaipur, India and Prof. C. Patvardhan of Dayalbagh Educational Institute (DEI), Agra, India discusses the generalized parallel QIEA framework designed for the solution of subset selection problems. Another chapter, “Quantum-Behaved Bat Algorithm for Solving the Economic Load Dispatch Problem Considering a Valve-Point Effect,” by Profs. Pandian Vasant and Junzo Watada of Universiti Teknologi Petronas, Malaysia; Prof. Fahad Parvez Mahdi of the University of Hyogo, Kobe, Japan; Profs. Jose Antonio Marmolejo-Saucedo and Roman Rodriguez Aguilar of Universidad Panamericana, Mexico; and Prof. Igor Litvinchev of Nuevo Leon State University, Mexico, proposes a quantum-behaved bat algorithm (QBA) to solve a nonlinear economic load dispatch (ELD) problem. The chapter “Design and Performance Evaluation of Smart Job First Multilevel Feedback Queue (SJFMLFQ) Scheduling Algorithm with Dynamic Smart Time Quantum” by Prof. Amit Kumar Gupta of Suresh Gyan Vihar University, Jaipur, India; Prof. Narendra Singh Yadav of JECRC University, Jaipur, India; and Prof. Dinesh Goyal of Suresh Gyan Vihar University, Jaipur, India utilizes the multilevel feedback queue scheduling (MLFQ) algorithm and discusses the results. The following chapter, “Hardware Implementation of a Visual Image Watermarking Scheme Using Qubit/Quantum Computation Through Reversible Methodology,” by Prof. Abhishek Basu of the RCC Institute of Information Technology, India; Prof. Subhrajit Sinha Roy of the Global Institute of Management and Technology, India; and Prof. Avik Chattopadhyay of the University of Calcutta, India, introduces a hardware implementation of an LSB replacement-based digital image watermarking algorithm. Next, “True Color Image Segmentation Using Quantum-Induced Modified-Genetic-Algorithm-Based FCM Algorithm” by Prof. Siddhartha Bhattacharyya of the RCC Institute of Information Technology, India; Prof. Sourav De of Cooch Behar Government Engineering College, India; and Prof. Sunanda Das of the University Institute of Technology, India, proposes a quantum-induced modified-genetic-algorithm-based FCM clustering approach for true color image segmentation. “Grayscale Image Segmentation With Quantum-Inspired Multilayer Self-Organizing Neural Network Architecture Endorsed by Context Sensitive Thresholding” by Profs. Siddhartha Bhattacharyya, Pankaj Pal, and Nishtha Agrawal of the RCC Institute of Information Technology, India proposes a grayscale image segmentation method endorsed by context-sensitive thresholding technique. This section concludes with “DNA Fragment Assembly Using Quantum-Inspired Genetic Algorithm” by Profs. Manisha Rathee and Kumar Dilip of Jawaharlal Nehru University, India and Prof. Ritu Rathee of Indira Gandhi Delhi Technical University for Women, India, which proposes a quantum-inspired genetic algorithm-based DNA fragment assembly (QGFA) approach to perform the de novo assembly of DNA fragments using overlap-layout-consensus approach.

Section 2, “Cryptography, Encryption, and Security,” presents extensive coverage and case studies on the latest findings on quantum technology for security and privacy applications. This section begins with “Quantum Internet and E-Governance: A Futuristic Perspective” by Profs. Manan Dhaneshbhai Thakkar and Rakesh D. Vanzara of Ganpat University, India. It provides details on evolution of quantum cryptography, components involved to design network architecture for quantum internet, quantum key exchange mechanism, and functionality wise stages for quantum internet. The next chapter, “Post-Quantum Cryptography and Quantum Cloning,” by Profs. Amandeep Singh Bhatia and Shenggen Zheng of the Center for Quantum Computing, Peng Cheng Laboratory, China, gives an outline of major developments in privacy protectors to reply to the forthcoming threats caused by quantum systems. The chapter “A Quantum Secure Entity Authentication Protocol Design for Network Security” by Prof. Surjit Paul of IIT Kharagpur, Kharagpur, India and Profs. Sanjay Kumar and Rajiv Ranjan Suman of NIT Jamshedpur, Jamshedpur, India shows the design of a proposed quantum secure entity authentication protocol based

on the challenge response method. Another chapter, “Medical Data Are Safe: An Encrypted Quantum Approach,” by Profs. Padmapriya Praveenkumar, Santhiyadevi R., and Amirtharajan R. of Shanmugha Arts, Science, Technology, and Research Academy (Deemed), India, proposes a quantum-assisted encryption scheme by making use of quantum gates, chaotic maps, and hash function to provide reversibility, ergodicity, and integrity, respectively. Next, “Quantum Cryptography Key Distribution: Quantum Computing” by Prof. Bhanu Chander of Pondicherry University, India describes the contemporary state of classical cryptography along with the fundamentals of quantum cryptography, quantum protocol key distribution, implementation criteria, quantum protocol suite, quantum resistant cryptography, and large-scale quantum key challenges. “Vulnerability of the Synchronization Process in the Quantum Key Distribution System” by Prof. A. P. Pljonkin of Southern Federal University, Taganrog, Russia presents the results of experimental studies, which prove the existence of a vulnerability in the process of synchronization of the quantum key distribution system. The final chapter in this section, “Optimal Parameter Prediction for Secure Quantum Key Distribution Using Quantum Machine Learning Models,” by Prof. K. Bhargavi of Siddaganga Institute of Technology, India and Profs. Sathish Babu B. and K. N. Subramanya of RV College of Engineering, Bangalore, India, discusses some of the quantum machine learning models with their architecture, advantages, and disadvantages.

Section 3, “Industry Applications of Quantum Technology,” reveals the latest research on where and how quantum technology is being implemented and utilized. This last section starts with the chapter “Quantum Cognition and Its Influence on Decrease of Global Stress Level Related With Job Improvement Strategies: Quantum Brain and Global Stress” by Prof. Ana Starcevic of the University of Belgrade, Serbia and Prof. Aleksandar Stojanovic of Federal University of Ceara, Brazil and explores how quantum theory is used to insert models of cognition that target to be more innovative than models based on traditional classical probability theory, which includes cognitive modeling phenomena in science. The following chapter, “Complex Action Methodology for Enterprise Systems (CAMES): A System to Contextualize the Behavioral Management Issue as Quantum Mechanical Variable,” by Prof. Olaf Comes of the University of Liverpool, UK and Prof. Meghann L. Drury-Grogan of Fordham University, USA utilizes the conceptual framework of quantum mechanics in action science field studies for bias-free behavioral data collection and quantification. Next, “Multi-Process Analysis and Portfolio Optimization Based on Quantum Mechanics (QM) Under Risk Management in ASEAN Exchanges: A Case Study of Answering to the E-Commerce and E-Business Direction” by Profs. Chukiat Chaiboonsri and Satawat Wannapan of Chiang Mai University, Thailand attempts to classify, predict, and manage the financial time-series trends of the large stock prices of significant companies in the development of e-commerce and e-business in the ASEAN countries. The chapter “A Quantum NeuroIS Data Analytics Architecture for the Usability Evaluation of Learning Management Systems” by Prof. Raul Valverde of Concordia University, Canada and Profs. Beatriz Torres and Hamed Motaghi of University of Quebec in Outaouais, Canada proposes an architecture based on a NeuroIS that collects data by using EEG from users and then use the collected data to perform analytics by using a quantum consciousness model proposed for computer anxiety measurements for the usability testing of a LMS. Following is the chapter “An Efficient Handwritten Character Recognition Using Quantum Multilayer Neural Network (QMLNN) Architecture: Quantum Multilayer Neural Network” by Profs. Debanjan Konar and Suman Kalyan Kar of Sikkim Manipal Institute of Technology, India, which proposes a quantum multi-layer neural network (QMLNN) architecture suitable for handwritten character recognition in real time, assisted by quantum backpropagation of errors calculated from the quantum-inspired fuzziness measure of network output

Preface

states. This reference book closes with “Quantum Local Binary Pattern for Medical Edge Detection” by Prof. Somia Lekehali of the University of M’sila, M’Sila, Algeria and Prof. Abdelouahab Moussaoui of University of Ferhat Abbas Setif 1, El Bez, Algeria, which propose a new procedure to extract the texture from images called the quantum local binary pattern (QuLBP).

Although the primary organization of the contents in this work is based on its three sections offering a progression of coverage of the important concepts, methodologies, technologies, applications, social issues, and emerging trends, the reader can also identify specific contents by utilizing the extensive indexing system listed at the end. As a comprehensive collection of research on the latest findings related to quantum computing and science, the *Research Anthology on Advancements in Quantum Technology* provides computer scientists, security analysts, data scientists, engineers, professionals, researchers, students, practitioners, academicians, and all audiences with a complete understanding of the implementations and uses of quantum technology. Given the need for computing, as it has become more ingrained in daily functions, quantum technology has become a critical exploration that this extensive book investigates and addresses with the most pertinent research on the technologies, security applications, benefits and challenges, and overall outlook for quantum technology.

Section 1

Algorithms and Techniques

Chapter 1

A Quantum Particle Swarm Optimization Algorithm Based on Self-Updating Mechanism

Shuyue Wu

School of Information Science & Engineering, Hunan International Economics University, Changsha, China

ABSTRACT

The living mechanism has limited life in nature; it will age and die with time. This article describes that during the progressive process, the aging mechanism is very important to keep a swarm diverse. In the quantum behavior particle swarm (QPSO) algorithm, the particles are aged and the algorithm is prematurely convergent, the self-renewal mechanism of life is introduced into QPSO algorithm, and a leading particle and challengers are introduced. When the population particles are aged and the leading power of leading particle is exhausted, a challenger particle becomes the new leader particle through the competition update mechanism, group evolution is completed and the group diversity is maintained, and the global convergence of the algorithm is proven. Next in the article, twelve Clement2009 benchmark functions are used in the experimental test, both the comparison and analysis of results of the proposed method and classical improved QPSO algorithms are given, and the simulation results show strong global finding ability of the proposed algorithm. Especially in the seven multi-model test functions, the comprehensive performance is optimal.

1. INTRODUCTION

The Particle Swarm Optimization (PSO) was proposed by Kennedy et al in the breeding behavior of simulated birds and fish in 1995 (Kennedy et al.,1995). In the evolution of the algorithm, the group shares the optimal position information (A. Manju, et al.,2014). Under the guidance of the swarm optimal position information and its own optimal information, the self-speed and position are updated by searching the multi-dimensional solution space (Zhang et al.,2016; Wu et al.,2016), and the candidate space solution is continuously followed and compared (Hao et al., 2016). And finally, the optimal solu-

DOI: 10.4018/978-1-7998-8593-1.ch001

tion or local optimal solution of the problem are found. In particle swarm algorithm, there are the characteristics of simple evolutionary equation, good searching ability and fast convergence speed. Particle swarm algorithm has been successfully applied in many aspects since it has been put forward. But the PSO algorithm itself is not a global optimization algorithm (Van Den Bergh, 2001), many scholars have done a lot of research work (Fang et al., 2010), they also put forward some improvement methods, and some improvement effects have been achieved (Chen et al., 2013; Campos et al., 2014). On the basis of deeply studying the evolution process of social intelligent groups, Sun et al. analyzed the mechanism of particle swarm optimization algorithm, the quantum theory was introduced to PSO algorithm, and they proposed a quantum search algorithm with global search ability (Quantum-behaved Particle Swarm Optimization, QPSO) (Sun et al., 2004; Sun et al., 2012). In QPSO algorithm, there are the characteristics of simple calculation, easy programming, less control parameters, and it has attracted the attention and research of many scholars in the related fields at home and abroad. The average value is calculated by QPSO optimal algorithms, Xi et al. introduced the nonlinear weight coefficient according to the merits of the particle, and the optimization ability of the algorithm was improved (Xi et al., 2008). Sun et al. gave the particle behavior analysis and parameter selection method of QPSO algorithm (Sun et al., 2012). In the QPSO algorithm, the mutation operator is introduced to improve the global search ability of the algorithm (Fang et al., 2009). At the same time, the QPSO algorithm is also applied to many practical problems. Omkar et al. applied the QPSO algorithm to the multi-objective optimization problem of combinatorial structure (Omkar et al., 2009). Indiral et al. applied the QPSO algorithm to association rule mining (Indiral et al., 2014), At the same time, the algorithm also has been applied in the portfolio selection problem (Farzi et al., 2013).

In the group intelligence algorithm, there is always the problem of how to balance the convergence speed and the global optimization ability. Aging is the inevitable life course in the individual group of life groups. Agglomeration of particles in the group and substitution of new particles can be beneficial to the group evolutionary structure, the diversity of groups can be enhanced. QPSO algorithm is a typical swarm intelligence algorithm, the phenomenon of aging also exists in the late evolution, particles are easy to fall into the local optimal. The leader particle and the challenger particle mechanism are introduced in our article, the group self-renewal is achieved. QPSO algorithm is used to improve the diversity of the population and jump out of the local optimal area. Base on the leadership and life cycle, update rules are studied in the process of particle aging. An improved quantum particle swarm optimization algorithm (QPSO is put forward with Self-renewal mechanism (SMQPSO).

2. QUANTUM PARTICLE SWARM OPTIMIZATION (QPSO)

In the PSO algorithm, the global best position (P_g), the individual best position (P_i), the velocity information V_i of the particle, and the position information X_i are used. PSO evolution equation:

$$v_{id}(t+1) = v_{id}(t) + c_1 r_1 (p_{id}(t) - x_{id}(t)) + c_2 r_2 (P_{gd}(t) - x_{id}(t)) \quad (1)$$

$$x_{id}(t+1) = v_{id}(t+1) + x_{id}(t) \quad (2)$$

A Quantum Particle Swarm Optimization Algorithm Based on Self-Updating Mechanism

Quantum Particle Swarm Optimization (QPSO): The running track of PSO algorithm particles were analyzed by Clerc (Clerc et al., 2002), he pointed out that in the PSO algorithm, if each particle can converge to its local attraction $P_i = (P_{i1}, P_{i2}, \dots, P_{iD})$, then PSO algorithm may converge. Among them:

$$p_{id}(t) = \frac{c_1 r_{1d}(t) P_{id}(t) + c_2 r_{2d}(t) P_{gd}(t)}{c_1 r_{1d}(t) + c_2 r_{2d}(t)}, 1 \leq d \leq D \quad (3)$$

and set

$$\phi_d(t) = \frac{c_1 r_{1d}(t)}{c_1 r_{1d}(t) + c_2 r_{2d}(t)}, 1 \leq d \leq D \quad (4)$$

In Formula (3) and (4), t is the current iteration number in algorithm, $r_{1d}(t)$ and $r_{2d}(t)$ is a random number between $[0, 1]$, P_i is the current optimal position of the particle, P_g is global optimal position for groups.

In the PSO algorithm, the learning factor c_1, c_2 is usually set to the equal value, so the formula (4) can be rewritten as:

$$\phi_d(t) = \frac{r_{1d}(t)}{r_{1d}(t) + r_{2d}(t)}, 1 \leq d \leq D \quad (5)$$

It can be seen that $\phi_d(t)$ is uniformly distributed random number between $[0, 1]$, the formula (3) is rewritten as:

$$p'_{id}(t) = \phi_d(t) P_{id}(t) + [1 - \phi_d(t)] P_{gd}(t), \quad \phi_d(t) \sim U[0, 1] \quad (6)$$

As can be seen from the above equation, p'_i is located in super rectangle by point P_i and point P_g for vertices, it varies with the change of point P_i and P_g point. In fact, when the particles converge to their local attraction, their own optimum position, the local attraction point and global optimal position will converge to the same point, so it makes PSO algorithm converge. From the perspective of dynamics analysis, the particles in the search process has p' point attractor in the PSO algorithm, with the continuous reduction of the particle velocity, it is close to p' point, and it is finally dropped to p' points. Thus, throughout the execution of the algorithm, there is some form of potential field to attract groups of particles at p' point, so that the population of particles maintained aggregation. However, in classical PSO system, the search process is implemented in the form of particles orbit, while the particle speed is limited, so in the search process, the search space of the particles is limited to a limited search space, which cannot cover the entire feasible search space. General PSO algorithm is not guaranteed to converge to a global optimal solution in the probability.

Assuming PSO system is a quantum system, in the quantum space, velocity and position of the particles can not be determined at the same time, the state of each particle is determined by the wave function ψ , $|\psi|^2$ is the probability density function of particle position. By analysis of PSO particle convergence system (Clerc et al., 2002), it is assumed in the t -th iteration, particle i is in D -dimensional space of movement, the potential well of the particles in the j -th dimension is for $p'_{ij}(t)$, the i particle wave function can be obtained at the $t + 1$ iteration:

$$\psi[x_{ij}(t+1)] = \frac{1}{\sqrt{L_{ij}(t)}} \exp\left[-\frac{|x_{ij}(t+1) - p_{ij}(t)|}{L_{ij}(t)}\right] \quad (7)$$

Thus, the probability density function Q can be obtained as:

$$Q[x_{ij}(t+1)] = |\psi[x_{ij}(t+1)]|^2 = \frac{1}{L_{ij}(t)} \exp\left[-2\frac{|x_{ij}(t+1) - p_{ij}(t)|}{L_{ij}(t)}\right] \quad (8)$$

Probability distribution function F is as:

$$F[x_{ij}(t+1)] = \exp\left[-2\frac{|x_{ij}(t+1) - p_{ij}(t)|}{L_{ij}(t)}\right] \quad (9)$$

By application of the Monte Carlo method, j -dimensional position of the particle i can be obtained in the $t + 1$ iteration:

$$x_{ij}(t+1) = p'_{i,j}(t) \pm \frac{L_{ij}(t)}{2} \ln\left[\frac{1}{u_{ij}(t)}\right], u_{ij}(t) \sim U[0,1] \quad (10)$$

Value $L_{ij}(t)$ is determined by the following formula (11):

$$L_{ij}(t) = 2a |M_j(t) - x_{ij}(t)| \quad (11)$$

wherein M is called the optimum average position, it is also referred to as m_{best} , it is obtained from the following equation (12):

$$M(t) = (m_1(t), m_2(t), \dots, m_D(t)) = \left(\frac{1}{N} \sum_{i=1}^N P_{i1}(t), \frac{1}{N} \sum_{i=1}^N P_{i2}(t), \dots, \frac{1}{N} \sum_{i=1}^N P_{iD}(t)\right) \quad (12)$$

where, N is the size of population, P_i is the i -th particle best position itself. Thus, the update equation (13) can be obtained in the location of particles:

A Quantum Particle Swarm Optimization Algorithm Based on Self-Updating Mechanism

$$x_{ij}(t+1) = p'_{ij}(t) \pm \alpha \cdot |M_{ij}(t) - x_{ij}(t)| \cdot \ln \left[\frac{1}{u_{ij}(t)} \right], u_{ij}(t) \sim U[0,1] \quad (13)$$

where, α is called compression expansion factor, it is used to adjust the convergence speed of the particles.

The current updated position P_i of the particle and the global best position in P_g updated manner are identical with the best updated way of the basic PSO algorithm, namely

$$P_i(t+1) = \begin{cases} P_i(t), & f(P_i) \geq f(X_i(t+1)) \\ X_i(t+1), & f(P_i) < f(X_i(t+1)) \end{cases} \quad (14)$$

$$P_g(t+1) = \arg \min_{P_i} f(P_i(t+1)), 1 \leq i \leq N$$

Here, the PSO algorithm in particle position update formula (13) is for quantum-behaved particle swarm optimization (Quantum-behaved Particle Swarm Optimization, QPSO) (Sun et al., 2004; Sun et al., 2012).

3. A QPSO ALGORITHM WITH SELF-UPDATING MECHANISM

3.1. Particle Evolution Analysis in QPSO Algorithm

In order to study the evolutionary iterative process of each particle in QPSO algorithm, the concept of relative evolution velocity is proposed. The relative evolution rate of individual particles can be quantified by equation (15).

$$\Delta f_i = (f_i - f_{p_i}) / f_i \quad (15)$$

where f_i is the current fitness function value of the i -th particle, f_{p_i} is the optimal fitness function value (minimization problem) of the i -th individual particle, and if the value of Δf is close to 0 or equal to 0, it means that the particle evolution is basically stopped, the population particles may fall into the local area. This paper uses the CEC2005 benchmark standard test function (Suganthan et al., 2005), in these test function, $f_1 \sim f_5$ are for the single-peak problem function, $f_6 \sim f_{12}$ are multi-peak function. Figure 1 shows the particle evolution process of f_1 function by using QPSO algorithm under the condition, Group particles are 20, the dimension of the variable is 10 and the number of iterations is 10 000 times. Different colors represent different particles. Figure 2 shows the particle evolution process of f_6 by using the QPSO algorithm under the condition that the population particle is 40 and the dimension of the variable is 30 and the number of iterations is 10 000 times.

Figure 1. Optimize Particle Evolution of f_1 Function in using QPSO Algorithm

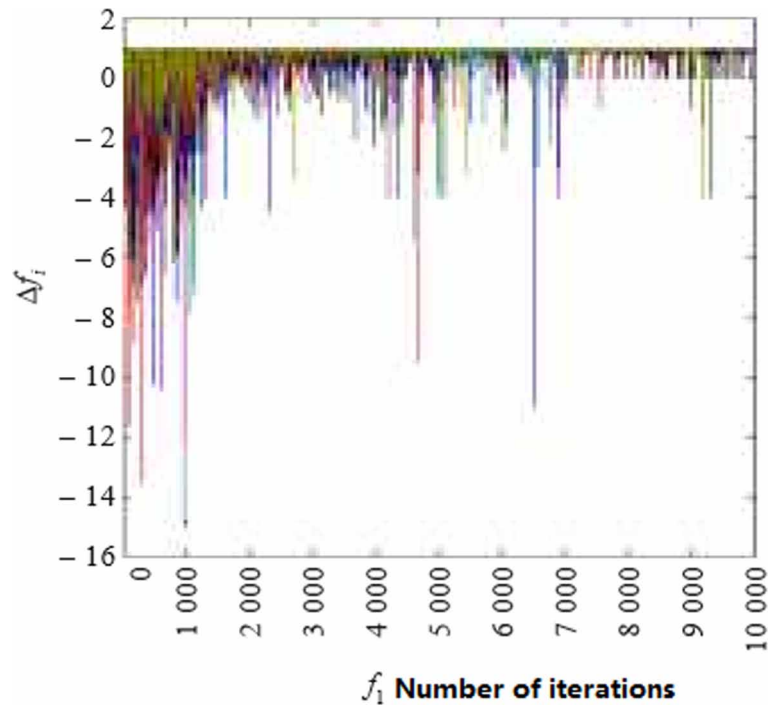
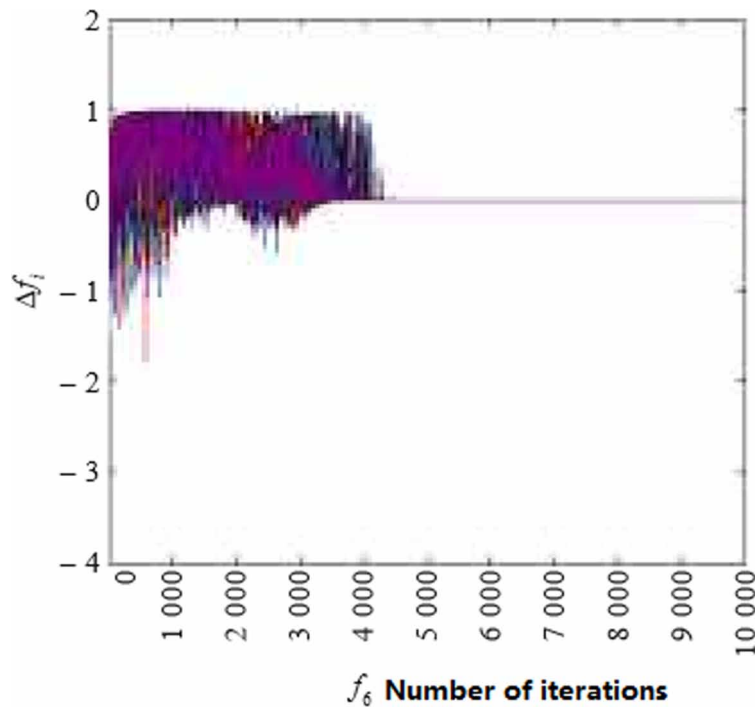


Figure 2. Optimize Particle Evolution of f_6 Function in using QPSO Algorithm



From the evolution process of particle population in Figure 1, it can be seen that for the f_1 test function, the values of each particle Δf change greatly in the early stage of evolution, and the population can be in the better evolution state. At the later stage of evolution, each particle Δf begins to gather, the evolution rate of the population particles is gradually decreased, and to some extent, it stays in the local optimal region. For the f_6 test function in Figure 2, since the multimodal function is transformed, the optimization is more difficult. Before the number of iterations is 3 500, the population has better evolutionary performance, but after 5000 iterations, the population particles Δf are rapidly clustered near the value of 0, which it is no longer changes during subsequent iterations, that is, the particles have all gathered near the smaller region and which are searched only in the neighborhood of the solution. It is easy to know that once the algorithm is localized in the search process, it is often difficult to jump out of the local optimal solution region and continue the search for the global optimal solution. From the analysis of Figure 1 and Figure 2, it can be seen that the QPSO algorithm is easy to search in the local region at the later stage of evolution, and it is necessary to increase the global search ability of the group through certain updating mechanism.

3.2. A QPSO Algorithmic Thinking with Self-Updating Mechanism

In the QPSO algorithm, the evolution of particles is achieved by iterative equations (3) (12) (13). The updating of the population particles depends on the particle information of its own optimal (P_i) and global optimal (P_g), and the particles are guided by P_i and P_g to optimize the solution space. In this search mechanism, when the population particles are attracted to a local optimal range, P_i and P_g are not updated and the diversity of the population decreases as the number of iterations increases due to the attraction of P_i and P_g . It is difficult for the population to jump out of the local optimal range, and it is difficult to optimize the performance of the algorithm in a wider range.

In the SMQPSO algorithm, in order to increase the diversity of population particles, population particles are prevented into the local optimal for the long-term, we introduce the leading particle (Leading Particle) with the life cycle, it replaces P_g in the basic QPSO algorithm, it is known as the P_{leader} . Unlike the direct introduction of the mutation operator strategy in Fang et al. (2009), the leader particle of this paper needs to continuously evaluate the leader's power in the iterative process, it is used to determine whether the current leader particle can continue to guide the group to optimize, it is used to determine whether the leader particle needs to be updated; at the same time, the concept of life cycle is also introduced for the individual's own optimal P_i , which is referred to as $P_{i,l}$, under certain conditions, if the individual particles can not be optimized, it also need to be updated. Thus, for the SMQPSO algorithm, the evolution equation (3) (12) (13) is modified as follows:

$$p'_{i_SL_j}(t) = \frac{c_1 r_{1d}(t) P_{i_l_j}(t) + c_2 r_{2d}(t) P_{leader_j}(t)}{c_1 r_{1d}(t) + c_2 r_{2d}(t)}, 1 \leq d \leq D \quad (16)$$

$$M(t) = (m_1(t), m_2(t), \dots, m_D(t)) \\ = \left(\frac{1}{N} \sum_{i=1}^N P_{i_l_1}(t), \frac{1}{N} \sum_{i=1}^N P_{i_l_2}(t), \dots, \frac{1}{N} \sum_{i=1}^N P_{i_l_D}(t) \right) \quad (17)$$

$$x_{ij}(t+1) = p'_{i_sl_j}(t) \pm \alpha \cdot |M_{ij}(t) - x_{ij}(t)| \cdot \ln \left[\frac{1}{u_{ij}(t)} \right], u_{ij}(t) \sim U[0,1] \quad (18)$$

3.3. Particle Life Cycle

In the SMQPSO algorithm, the particle's life time is important for the performance of the algorithm. In the SMQPSO algorithm, the evolution time of particles in the evolutionary process adopts the concept of dynamic survival time. By measuring the leading power of the particles in the past and present performance, it can judge whether the particles can continue to guide the group or its own evolution through leadership, and it can determine whether the particles need to be updated.

Particle leadership is accumulated through the evolution of groups in the evolution of groups or individuals. For P_{leader} , there are four cases in the evolution of the guided population: (1) to guide the evolution of the group and the evolution of the individual; (2) to guide the evolution of the group, while the individual does not evolve; (3) to guide the evolution of the individual, and the group does not evolve; (4) groups and individuals do not evolve. For P_{i_l} , there are two cases in guiding individual evolution: (1) guiding personal evolution; (2) failing to guide individual evolution. For the minimization problem, the leadership of the particle can be expressed by equation (19) (20) (21).

$$\Delta_{P_i}(t) = f(P_i(t)) - f(P_i(t-1)), \quad t = 1, 2, \dots, l \quad (19)$$

$$\sum_{i=1}^N \Delta_{P_i}(t) = \sum_{i=1}^N f(P_i(t)) - \sum_{i=1}^N f(P_i(t-1)), \quad t = 1, 2, \dots, l \quad (20)$$

$$\Delta_{P_g}(t) = f(P_g(t)) - f(P_g(t-1)), \quad t = 1, 2, \dots, l \quad (21)$$

Among them, $\Delta_{P_i}(t)$ represents the leadership of individual particles to guide their evolution, and $\sum_{i=1}^N \Delta_{P_i}(t)$ represents the leadership of Pleader's guided group evolution, $\Delta_{P_g}(t)$ represents the individual dominant evolutionary power, l represents particle life cycle. In this paper, $Power_{leader}$ is used to represent P_{leader} 's leadership, and $Power_{i_l}$ represents the leadership of the i -th particle in the population, and the leadership of the particle is analyzed as follows:

1. When $\sum_{i=1}^N \Delta_{P_i}(t) < 0$ and $\Delta_{P_g}(t) < 0$, it indicates that P_{leader} 's leadership is strong, and it can lead groups and optimal individuals to evolve simultaneously, then $Power_{leader} = Power_{leader} + \delta_1$.
2. When $\sum_{i=1}^N \Delta_{P_i}(t) > 0$ and $\Delta_{P_g}(t) < 0$, it shows that P_{leader} 's leadership is strong and can lead to the evolution of the optimal individual, but it cannot lead the evolution of the group, then $Power_{leader} = Power_{leader} + \delta_2$.

A Quantum Particle Swarm Optimization Algorithm Based on Self-Updating Mechanism

3. When $\sum_{i=1}^N \Delta_{P_i}(t) < 0$ and $\Delta_{P_g}(t) > 0$, the leadership of the P_{leader} is generally able to guide the evolution of the group, but it cannot lead the optimal individual evolution, then $\text{Power}_{\text{leader}} = \text{Power}_{\text{leader}} + \delta_3$.
4. When $\sum_{i=1}^N \Delta_{P_i}(t) > 0$ and $\Delta_{P_g}(t) > 0$, it is indicating that the leadership of P_{leader} is poor, it can not guide the evolution of the group and the optimal individual evolution, then $\text{Power}_{\text{leader}} = \text{Power}_{\text{leader}} + \delta_4$.
5. When $\Delta_{P_i}(t) < 0$, it means that P_{i-1} is strong, then $\text{Power}_{i-1} = \text{Power}_{i-1} + \zeta_1$.
6. When $\Delta_{P_i}(t) > 0$, it indicates that P_{i-1} leadership is poor, then $\text{Power}_{i-1} = \text{Power}_{i-1} + \zeta_2$.

In the SMQPSO algorithm evolution process, the cumulative leadership determines whether to update the particles.

3.4. Update Leading Particle

In the evolutionary process, the leadership of the particle changes with the dynamic changes of the evolution process. Leadership continues to increase when lead particles evolve in a round of iterative evolution, and leadership continues to decline when leading particles do not have the ability to lead groups to evolve. The leadership of the leading particles are calculated by judging the evolutionary results of each round. When the leadership of the leadership particles are in the exhaustion of energy, it means that the group particles are into the local optimal, leader particles have no ability to continue to lead the group to optimize. In this case, there must be new particles as the leading particle to guide group optimization, the new particles are called the potential leadership particles ($P_{\text{candidate}}$), we need to further determine whether the potential leadership of particles is as a leading particle to guide group optimization.

In order to ensure the integrity of the leading particle structure and consider the computational complexity factor, in the paper, $P_{\text{candidate}}$ is generated in the way of initialization for each dimension of the P_{leader} in accordance with a certain probability (pro). A random number (rnd^j) is generated in (0, 1) in the evenly distributed manner. If $\text{rnd}^j < \text{pro}$, the j -dimensional values corresponding to the P_{leader} particles are reinitialized in the solution space (Lower, Uper), if no one-dimensional meets the conditions of initialization, one-dimension in P_{leader} is randomly specified to do initialization, resulting $P_{\text{candidate}}$. The specific process as shown here:

Set the particle to D dimension, count variable count initial value is 0

```

For j = 1 to D
  If  $\text{rnd}^j < \text{pro}$ 
     $P_{\text{candidate}}^j = \text{random}(\text{Lower}^j, \text{Uper}^j)$ 
    count = count + 1
  Else
     $P_{\text{candidate}}^j = P_{\text{leader}}^j$ 
  End if
End for
If count == 0

```


$J = \text{random}(1, D)$
 $P_{\text{candidate}}^j = \text{random}(\text{Lower}^j, \text{Uper}^j)$
 End if

Since the leader particle is not updated in every round of evolution, in the most extreme case, each round of evolutionary groups cannot find a better value, the number of times which the leader particle is updated and the number of evolution iterations m is the same, that is, after m evolution, the leader particle calculation is updated for m times, the time complexity is $O(m)$.

Similarly, after the leadership of the individual guide particle $P_{i,j}$ is consumed, an individual guide candidate particle $P_{i,j,\text{candidate}}$ is also required, and the process is the same as the $P_{\text{candidate}}$ generation process. $P_{\text{candidate}}$ and $P_{i,j,\text{candidate}}$ are also required to evaluate their leadership and to guide the group to find a better solution to the problem.

If $f(P_{\text{candidate}}) < f(P_{\text{leader}})$, indicating that the group leader candidate $P_{\text{candidate}}$ is appropriate, then $P_{\text{leader}} = P_{\text{candidate}}$; otherwise, it is inappropriate to continue using the original P_{leader} to guide the current iterative evolution.

If $f(P_{i,j,\text{candidate}}) < f(P_{i,j})$, indicating that the individual leader candidate $P_{i,j,\text{candidate}}$ is appropriate, then $P_{i,j} = P_{i,j,\text{candidate}}$; Conversely, it is not appropriate to continue using the original $P_{i,j}$ to guide the current iterative evolution.

SMQPSO algorithm design:

1. Initialization parameter settings: the number of groups; expansion shrinkage factor α range; algorithm iteration times; lead the particle generation process parameters ($\text{Pro}, \delta_1, \delta_2, \delta_3, \delta_4, \zeta_1, \zeta_2$); initial solution X_i is randomly generated, and to set $P_i = X_i$, and the number of groups is calculated., and to calculate the global optimal value P_g ; to initialize the settings $P_{\text{leader}} = P_g$ and $P_{i,j} = P_i$.
2. Calculate the local attractor $P_{i,\text{SL}}^*$ according to Equation (16).
3. Calculate the average optimal value M according to Equation (17).
4. Calculate the particle update value X^{t+1}_i according to equation (18).
5. Calculate the leadership of P_{leader} and $P_{i,j}$ according to Equations (19) (20) (21).
6. Calculate the cumulative leadership of P_{leader} and $P_{i,j}$ and determine if it needs to be updated. If you want to update, to use the procedure which is shown in the specific process
7. return to 2) until the end of the cycle condition.

4. CONVERGENCE ANALYSIS OF SMQPSO ALGORITHM

4.1. Global Convergence Criteria for Search Algorithm

In the analysis of the convergence of SMQPSO algorithm, we use t as the number of iterations, S is a subset of the solution space, and z is the point in the solution space. According to the convergence criterion of Solis and Wets proposed random search algorithm (Solis F., et al.,1981), the stochastic algorithm should satisfy hypothesis 1:

Hypothesis 1: $f(D(z, \tau)) \leq f(z)$, and if $\tau \in S$ then

$$f(D(z, \tau)) \leq f(\tau) \tag{22}$$

where D denotes a specific algorithm and τ denotes a vector of sample space.

The global convergence of any algorithm means that the sequence $\{f(z_t)\}_{t=1}^{\infty}$ should converge to the lower bound of the function f in S . In order to avoid the ills of the function (the minimum point is at the point of discontinuity) so that the global optimal solution can not be searched, the search target becomes the next bound ψ , then it can be close to the lower bound without traversing every point in S . The acceptable area is defined for the algorithm:

$$R_\varepsilon = \{z \in S | f(z) < \psi + \varepsilon\} \tag{23}$$

where $\varepsilon > 0$. If the algorithm finds the point in R_ε , then the algorithm finds an acceptable point with an error of ε . Thus, for the minimization problem, the global convergence algorithm should satisfy hypothesis 2.

Hypothesis 2: For any Borel subset A of S , if its measure $v[A] > 0$, there is

$$\prod_{k=0}^{\infty} (1 - \mu_k[A]) = 0$$

where $\mu_k[A]$ is the probability of A obtained by the measure μ_k . This means that for a subset of any A of position measures v , if the random sampling method is used, the probability that it will miss the set A must be zero. Since $R_\varepsilon \subset S$, the probability of obtaining points in the acceptable area is certainly nonzero. Based on the above analysis, we can get the following theorem:

Theorem 1: Suppose that the objective function f is a measurable function, S is a subset of measurable spaces, satisfying hypothesis 1, letting $\{z_t\}_{t=1}^{\infty}$ be the solution sequence which are generated by the algorithm, then

$$\lim_{k \rightarrow \infty} P[z_k \in R_\varepsilon] = 1 \tag{24}$$

where $P[z_k \in R_\varepsilon]$ is the probability of the solution $z_k \in R_\varepsilon$ which are generated by the step t algorithm.

4.2. The Global Convergence Proof of SMQPSO Algorithm

In the process of convergence of SMQPSO algorithm, this paper studies it in the framework of global random search algorithm and proves the conclusion of theorem 1.

Lemma 1: SMQPSO algorithm satisfies hypothesis 1.

Proof: From the evolution equation of the SMQPSO algorithm, we can conclude that the sequence $\{P_g\}_{i=1}^t$ is the optimal sequence of all the particles in the population from the beginning to the t -th iteration step. According to the evolutionary process analysis of SMQPSO algorithm, P_g^t is the optimal value of the t -th iteration, and the description of the function D in the SMQPSO algorithm

can be defined as P'_g , which is monotonic (the minimization problem is monotonically decreasing), so the SMQPSO algorithm satisfies the hypothesis 1.

Lemma 2: SMQPSO algorithm satisfies hypothesis 2.

Proof: In the SMQPSO algorithm, in any one iteration step t , the probability density function of the j -th dimension of i particles is as follows:

$$Q(X_{i,j,t}) = \frac{1}{L_{i,j,t}} \exp\left(-2\left|X_{i,j,t} - P'_{i,j,t}\right|/L_{i,j,t}\right) \quad (25)$$

The probability density function of particle i can be expressed as follows:

$$Q(X_{i,t}) = \prod_{j=1}^D \frac{1}{L_{i,j,t}} \exp\left(-2\left|X_{i,j,t} - P'_{i,j,t}\right|/L_{i,j,t}\right) \quad (26)$$

Define $\mu_{i,t}$ is the probability measure corresponding to $Q(X_{i,t})$. For any Borel subset A of S , when $v[A] > 0$ is satisfied, there are as follows:

$$\mu_{i,t}[A] = \int_A Q(X_{i,t}) dX_{i,t} \quad (27)$$

$$M_{i,t} = R^D \supset S \quad (28)$$

where $M_{i,t}$ is $\mu_{i,t}$ is supported in the sample space, and $A \supset M_{i,t}$. So it can be as follows:

$$0 < \mu_{i,t}[A] < 1 \quad (29)$$

The support of the particles is:

$$M_t = \bigcup_{i=1}^s M_{i,t} = R^D \supset S \quad (30)$$

where M_t is the support of the distribution μ_t , and the probability A of which is generated by μ_t can be calculated from the following equation.

$$\mu_t[A] = 1 - \prod_{i=1}^s (1 - \mu_{i,t}[A]) \quad (31)$$

By equation (29), we can get:

$$0 < \mu_t[A] < 1, \quad t = 1, 2, \dots \quad (32)$$

So available:

$$\prod_{i=1}^S (1 - \mu_{i,t}[A]) = 0 \quad (33)$$

This indicates that the SMQPSO algorithm satisfies hypothesis 2. Proof is completed.

5. SIMULATION ANALYSIS OF SMQPSO ALGORITHM

5.1. Analysis of Particle Leadership Parameters

In the SMQPSO algorithm, the the particle leadership parameters ($\delta_1, \delta_2, \delta_3, \delta_4, \zeta_1, \zeta_2$) have important influence on the algorithm. In this paper, the parameters are studied by different parameter combinations. The test function uses the CEC2005 benchmark test function (Suganthan P., et al.,2005), where f_1 to f_5 are single-peak functions and f_6 to f_{12} are multimodal functions. In the algorithm, the other parameters are set as follows: the contraction expansion factor α decreases from 1.0 linear to 0.5, the dimension of the problem is 30, the maximum number of iterations corresponding to the algorithm is 20 000, the number of particles is 40, and the solution of each problem is random to run independently 50 times, pro value is $1/D$.

Table 1 gives the average and standard deviation of the target test function values when the leadership parameters are different. In the value of leadership parameters,for the different cases of P_{leader} particle leadership, δ_1, δ_2 and δ_3 are different values (2, 1, 0) respectively. For δ_4 , we consider two kinds of values, namely -1 and -2, respectively. When P_{leader} cannot lead the group, the δ_4 value-2 can quickly consume the P_{leader} 's pre-accumulated leadership to achieve the purpose of quickly updating the P_{leader} , and when the leadership is exhausted, the particle's life cycle is over. For the individual particle leadership ζ_1, ζ_2 , we studied the case of (2, -1), (2, $-\infty$) and (3, -1), where $-\infty$ indicates that when the particle cannot lead the individual to seek, it goes directly into the particle update step, no longer consider the accumulation of early leadership.

From the simulation data in Table 1, it can be concluded that different combinations of leadership parameters have an effect on the performance of the algorithm. For the unimodal function ($f_1 \sim f_5$), the optimization problem is relatively simple and the probability of particles falling into local optimum is small. When the leading particles fall into the local optimum, it quickly reduces its leadership, allowing the new particles to replace it as soon as possible, leading the group to continue to optimize. For the multimodal function ($f_6 \sim f_{12}$), the optimization problem is relatively complex. In the optimization process, the particles tend to fall into the local optimum, and the leading particles accumulate relatively more leadership, and the smaller lead drop velocity will be conducive to maintaining the optimal structure of the group, and the optimal value is ultimately found.

Table 1. Mean and variance of test functions for SMQPSO algorithm under different leadership parameters

		$\delta 1, \delta 2, \delta 3, \delta 4, \zeta 1, \zeta 2$				
		(2,1, 0,-1, 2,-1)	(2,1,0,-1,2,-∞)	(2,1,0,-1,3,-1)	(2,1,0,-2,2,-1)	(2,1,0,-2,3,-1)
f1	Average	1.772 7E-27	1.804 8E-27	1.791 1E-27	1.778 2E-27	1.731 5E-27
	variance	1.275 0E-30	3.024 3E-30	1.825 6E-30	6.340 8E-30	2.075 8E-30
f2	Average	2.328 8E-08	1.693 5E-11	3.334 9E-13	2.567 1E-12	1.316 4E-12
	variance	4.752 8E-10	3.446 1E-13	6.682 3E-15	2.519 3E-14	2.125 5E-14
f3	Average	1.081 6E+07	9.356 0E+06	1.131 1E+07	1.097 1E+07	1.127 1E+07
	variance	1.821 4E+04	1.943 8E+04	6.431 7E+03	8.404 0E+04	5.204 3E+04
f4	Average	7.140 7	6.747 6	5.956 4	6.172 3	5.394 9
	variance	0.131 3	0.123 1	0.017 2	0.080 7	0.275 0
f5	Average	2.067 7E+03	1.912 7E+03	1.977 2E+03	1.823 9E+03	2.111 5E+03
	variance	19.123 4	5.135 9	22.110 7	9.355 1	14.721 5
f6	Average	32.513 6	25.709 5	27.483 9	29.880 1	30.732 6
	variance	0.354 7	1.071 2	0.938 6	0.567 1	0.277 7
f7	Average	0.013 1	0.014 4	0.017 4	0.015 9	0.015 9
	variance	1.183 5E-04	9.417 0E-05	1.543 8E-04	1.754 9E-04	5.770 7E-04
f8	Average	6.252 7E-15	5.826 4E-15	6.323 8E-15	6.110 6E-15	6.110 6E-15
	variance	1.740 1E-17	2.610 1E-17	5.655 3E-17	2.030 1E-17	5.220 3E-17
f9	Average	0	0	0	0	0
	variance	0	0	0	0	0
f10	Average	82.903 7	83.799 7	86.652 2	82.467 6	81.613 4
	variance	0.061 1	0.059 3	0.280 4	0.252 5	0.329 9
f11	Average	25.737 3	25.489 4	26.043 4	25.536 5	25.447 5
	variance	0.034 4	0.077 8	0.001 0	0.031 4	0.038 4
f12	Average	5.797 0E+03	6.001 3E+03	6.138 4E+03	6.089 1E+03	6.474 1E+03
	variance	11.596 6	32.252 1	21.466 7	41.642 0	56.809 8

5.2. Simulation Results and Discussion

Table 2 and Table 3 show the simulation results of the SMQPSO algorithm which are presented in this paper and other typical improved QPSO algorithms. The comparison of these algorithms mainly has a fixed contraction expansion factor QPSO (BQPSO) algorithm, standard QPSO (QPSO) algorithm, the QPSO (LCQPSO) algorithm for local search strategy, self-learning QPSO (SQPSO) algorithm, enhanced QPSO (QLQPSO) algorithm, optimum attraction point QPSO (GQPSO), mixed attracting point QPSO (HQPSO) algorithm, linear weighting coefficient QPSO (WQPSO) algorithm and nonlinear weight QPSO (UQPSO, DQPSO) algorithm (Fang W.,2008; Sheng X., et al.,2015). In all the algorithms, the number of problems is 30, the maximum number of iterations is 20 000, the number of particles is 40, and the solution of each problem is run independently for 50 rounds. The other parameters are the same as the original reference.

A Quantum Particle Swarm Optimization Algorithm Based on Self-Updating Mechanism

Table 2. The average optimal value and variance of SMQPSO and BQPSO, QPSO, LCQPSO, SQPSO and QLQPSO after 50 rounds

		BQPSO	QPSO	LCQPSO	SQPSO	QLQPSO	SMQPSO
f1	Average	3.985 2E-27	1.745 2E-27	1.960 7E-27	1.770 9E-27	2.052 2E-27	1.804 8E-27
	variance	2.030 2E-29	3.989 9E-29	1.923 0E-29	3.299 0E-30	6.415 8E-30	3.024 3E-30
f2	Average	1.549 2E-14	1.574 5E-15	5.239 4E-08	1.272 4E-13	1.169 6E-21	1.693 5E-11
	variance	3.150 8E-16	7.652 6E-16	1.068 2E-09	3.259 4E-15	8.756 9E-24	3.446 1E-13
f3	Average	1.595 1E+06	1.035 9E+06	1.812 2E+06	1.287 6E+06	1.313 7E+06	9.356 0E+06
	variance	2.241 1E+04	6.355 0E+04	9.239 7E+02	4.173 2E+03	1.693 4E+04	1.943 8E+04
f4	Average	0.008 4	0.507 8	3.644 4	1.769 9	9.104 3E-05	6.747 6
	variance	1.074 2E-04	0.072 0	0.050 1	0.022 6	1.716 5E-06	0.123 1
f5	Average	4.171 5E+03	4.058 7E+03	2.225 5E+03	2.225 4E+03	3.381 2E+03	1.912 7E+03
	variance	17.200 2	1.574 6E+02	3.940 4	11.070 8	16.762 3	5.135 9
f6	Average	25.589 3	31.077 4	46.783 8	24.620 2	33.895 2	25.709 5
	variance	0.191 6	0.942 9	0.7740 8	1.226 9	0.422 7	1.071 2
f7	Average	0.021 5	0.018 1	0.013 6	0.015 1	0.018 8	0.014 4
	variance	2.386 0E-04	0.001 9	7.225 4E-05	3.093 1E-04	3.846 5E-04	9.417 0E-05
f8	Average	6.679 1E-15	6.465 9E-15	6.039 6E-15	6.110 6E-15	6.536 9E-15	5.826 4E-15
	variance	8.700 5E-18	1.969 6E-16	2.175 1E-17	2.030 1E-17	1.160 0E-17	2.610 1E-17
f9	Average	17.698 6	38.717 3	18.835 7	18.996 9	30.846 7	0
	variance	0.051 3	2.349 5	0.003 0	0.024 9	0.363 9 1.	0
f10	Average	1.066 5E+02	1.711 5E+02	1.005 0E+02	59.142 1	359 4E+02	83.799 7
	variance	1.016 2	7.538 4	0.772 5	0.770 1	0.588 4	0.059 3
f11	Average	12.987 6	24.096 7	26.742 7	20.489 7	25.363 7	25.489 4
	variance	0.052 4	0.668 5	0.005 9	0.085 0	0.375 2	0.077 8
f12	Average	2.220 9E+04	3.459 5E+04	2.083 0E+04	1.747 4E+04	1.711 8E+04	6.001 3E+03
	variance	2.188 4E+02	4.805 4E+03	3.556 7E+02	3.138 2E+02	1.957 8E+02	32.252 1

A comparison of the results in Table 2 and Table 3 shows that SMQPSO has achieved a good value in the test function Schwefel 's Problem 2.6 with Global Optimum on the Bounds function (f_5), Shifted Rotated Griewank's Function without Bounds function (f_7), Shifted Rotated Ackley' s function (f_8) Shifted Rastrigin 's function (f_9), Shifted Schwefel' s Problem 1.2 function (f_{12}), and it has been the first in the f_5 , f_8 , f_9 test function, it is the largest of all the test algorithms. In other test functions, SMQPSO also achieved similar simulation results with other algorithms. BQPSO algorithm, QPSO algorithm, LCQPSO algorithm, GQPSO algorithm, HQPSO algorithm, UQPSO algorithm, WQPSO algorithm made an optimal value respectively in Shifted Rotated Weierstrass function (f_{11}), Shifted Rotated High Conditioned Elliptic function (f_3), f_7 , Shifted Sphere function (f_1), Shifted Rotated Rastrigin 's function (f_{10}), Shifted Rosenbrock function (f_6), f_{12} . The QLQPSO algorithm achieves a quadratic optimal value in the Shifted Schwefel's Problem 1.2 function (f_2), Shifted Schwefel 's Problem 1.2 with Noise in Fitness function (f_4).

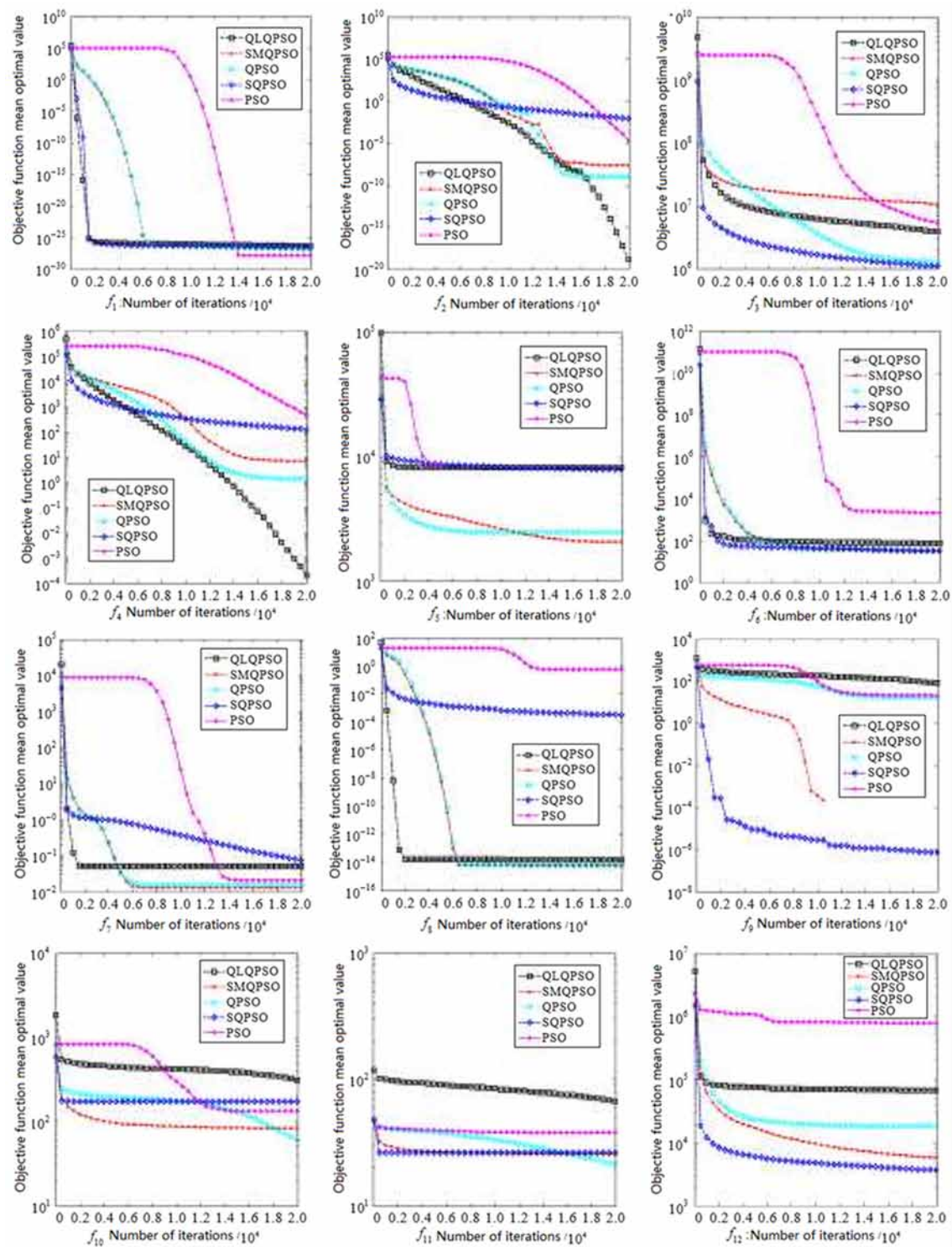
Table 3. The average optimal value and variance of SMQPSO and GQPSO, HPSO, UQPSO, DQPSO and WQPSO after 50 rounds

		GQPSO	HQPSO	UQPSO	DQPSO	WQPSO	SMQPSO
f1	Average	0	9.276 0E-28	1.472 4E-28	1.41	6.593 1E-27	1.804 8E-27
	variance	0	3.239 1E-31	2.952 5E-31	0.0051	9.351 0E-30	3.024 3E-30
f2	Average	3.948 0E-11	2.736 9E-17	1.755 3E-10	8.0528	0.008 8	1.693 5E-11
	variance	8.057 1E-13	5.585 6E-19	3.582 2E-12	0.0437	1.444 3E-04	3.446 1E-13
f3	Average	4.145 9E+06	1.855 7E+06	1.369 7E+06	2.852 2E+06	1.038 9E+06	9.356 0E+06
	variance	8.870 8E+04	1.407 4E+04	3.781 7E+03	8.516 0E+03	4.594 8E+03	1.943 8E+04
f4	Average	5.482 9E+03	1.4933	1.7893	16.2515	1.250 7E+02	6.747 6
	variance	2.103 9E+02	0.0036	0.039	0.0759	0.582 0	0.123 1
f5	Average	5.914 8E+03	2.675 9E+03	2.728 8E+03	2.336 4E+03	8.560 0E+03	1.912 7E+03
	variance	3.6594	15.2394	5.5376	18.3328	32.586 3	5.135 9
f6	Average	24.6203	41.0812	23.7312	2.954 4E+02	37.842 5	25.7095
	variance	0.4317	0.4295	1.0461	3.4583	1.041 8	1.071 2
f7	Average	0.0301	0.0174	0.0177	1.0782	0.082 4	0.014 4
	variance	4.149 3E-04	3.963 4E-04	2.407 5E-04	9.685 3E-05	2.113 1E-04	9.417 0E-05
f8	Average	4.7739	0.4079	6.608 0E-15	6.252 7E-15	3.706 4E-04	5.826 4E-15
	variance	0.0974	0.0083	1.015 0E-17	1.740 1E-17	2.774 1E-06	2.610 1E-17
f9	Average	56.4393	24.6288	17.9173	12.027	5.458 0E-07	0
	variance	0.1209	0.0751	0.0161	0.0233	1.001 4E-08	0
f10	Average	1.113 8E+02	50.8278	58.501	54.0265	1.714 6E+02	83.799 7
	variance	0.5603	0.7238	0.4753	0.4369	1.042 4	0.059 3
f11	Average	25.2661	15.0969	17.0333	17.1813	26.482 6	25.489 4
	variance	0.0371	0.0324	0.1028	0.2637	2.144 0E-04	0.077 8
f12	Average	6.863 7E+04	3.227 8E+04	1.992 5E+04	2.427 5E+04	2.999 6E+03	6.001 3E+03
	variance	1.102 4E+0	4.294 8E+02	31.4028	1.650 0E+02	42.854 2	32.252 1

Figure 3 shows the evolution curves of the QPSO algorithm, PSO algorithm, SMQPSO algorithm, QLQPSO algorithm and SQPSO algorithm for 20 000 iterations. It can be seen from the convergence curve that the SMQPSO algorithm and the PSO algorithm can achieve faster convergence rate in 12 test functions. Compared with the QPSO algorithm, the convergence rate can be approximated in the test function. The convergence rate in f_9 , f_{10} and f_{11} is better than that of QPSO. Compared with other QPSO algorithm, although it cannot obtain obvious advantages in all the test functions, the convergence performance is stable and the comprehensive performance is good. The SMQPSO algorithm with self-updating mechanism can improve the ability of jumping out of local search and improve the overall performance of the algorithm.

A Quantum Particle Swarm Optimization Algorithm Based on Self-Updating Mechanism

Figure 3. Comparison of Convergence Curve of Objective Function Value in Different Algorithm Optimization Test Function



Analysis of Variance (ANOVA) is also known as “variance analysis” or “F test”, it is used for two or more samples of the difference between the two significant test. In order to better compare the overall performance of the test algorithm, the ANOVA test method (Day R., et al.,1989) is used in this paper to study the overall performance of each improved algorithm, which the significance level of the ANOVA test method is set to 0.05. All algorithms are based on the results of the test to determine whether the test is reliable and effective. Table 4 gives the sorting results for each of the 12 test functions. Table 5 gives the sorting results for the seven test functions specifically for the multi-peak problem (f6 ~ f12). From the sorted values in Table 4, the SQPSO algorithm has a sorted value of 49, and the overall performance of the 12 test functions is optimal. The UQPSO algorithm and the SMQPSO operator are followed by the 56, 57, respectively. For the seven multi-peak problems, the proposed SMQPSO algorithm in this paper has the sort value 25, and the performance is optimal in all algorithms. The comparison of these values shows that the QPSO algorithm with self-updating mechanism increases the diversity of the test function in the optimization of the test function, and it exhibits strong optimization characteristics, especially in the multi-peak problem.

Table 4. Performance comparison tables for different algorithms to optimize 12 test functions

Algorithm	f1	f2	f3	f4	f5	f6	f7	f8	f9	f10	f11	f12	Sort value
BQPSO	9	4	6	2	9	4	8	8	4	7	1	7	69
QPSO	4	3	1	3	8	6	6	5	10	10	6	10	72
LCQPSO	7	9	7	7	2	10	1	2	6	6	11	6	74
SQPSO	5	5	3	5	3	2	3	3	7	4	5	4	49
QLQPSO	8	1	4	1	7	7	7	6	9	9	8	3	70
GQPSO	1	7	10	11	10	3	9	11	11	8	7	11	99
HQPSO	3	2	8	4	5	9	4	10	8	1	2	9	65
UQPSO	2	8	5	6	6	1	5	7	5	3	3	5	56
DQPSO	11	11	9	9	4	11	11	4	3	2	4	8	87
WQPSO	10	10	2	10	11	8	10	9	2	11	10	1	94
SMQPSO	6	6	11	8	1	5	2	1	1	5	9	2	57

A Quantum Particle Swarm Optimization Algorithm Based on Self-Updating Mechanism

Table 5. Performance comparison tables for different algorithms to optimize seven multimodal functions

Algorithm	f6	f7	f8	f9	f10	f11	f12	Sort value
BQPSO	4	8	8	4	7	1	7	39
QPSO	6	6	5	10	10	6	10	53
LCQPSO	10	1	2	6	6	11	6	42
SQPSO	2	3	3	7	4	5	4	28
QLQPSO	7	7	6	9	9	8	3	49
GQPSO	3	9	11	11	8	7	11	60
HQPSO	9	4	10	8	1	2	9	43
UQPSO	1	5	7	5	3	3	5	29
DQPSO	11	11	4	3	2	4	8	43
WQPSO	8	10	9	2	11	10	1	51
SMQPSO	5	2	1	1	5	9	2	25

6. CONCLUSION

The evolutionary equation of QPSO algorithm is analyzed, and the phenomenon of aging and death is studied in the evolution of life in nature. In the process of QPSO evolution, the self-renewal mechanism is introduced, and the concept of leader particle and challenger particle is put forward. The leadership of the leader particle is calculated by the current particle performance, and the method of leadership calculation is analyzed in different states. When the leadership is exhausted, the challenge mechanism is used to determine whether the leader particle needs to be updated and the execution of the entire algorithm is given. The QPSO algorithm with self-updating mechanism fully preserves the diversity of the group evolution. In the simulation comparison using the CEC2005 test function and several other improved algorithms, the QPSO algorithm with self-updating mechanism can achieve better results in many test functions. The SMQPSO algorithm can improve the overall performance of the QPSO algorithm, especially in the multi-peak test, and other functions can achieve similar results with other methods.

ACKNOWLEDGMENT

This work is sponsored by the Scientific Research Project (NO. 14A084) of Hunan Provincial Education Department, China.

REFERENCES

Campos, M., Krohling, R., & Enriquez, I. (2014). Bare bone particle swarm optimization with scale matrix adaption. *IEEE Transactions on Cybernetics*, 44(9), 1567–1578. doi:10.1109/TCYB.2013.2290223 PMID:25137686

- Chen, W., Zhang, J., Lin, Y., Chen, N., Zhan, Z.-H., Chung, H. S.-H., ... Shi, Y.-H. (2013). Particle swarm optimization with an aging leader and challengers. *IEEE Transactions on Evolutionary Computation*, 17(2), 241–258. doi:10.1109/TEVC.2011.2173577
- Clerc, M., & Kennedy, J. (2002). The particle swarm: Explosion, stability and convergence in a multi-dimensional complex space. *IEEE Transactions on Evolutionary Computation*, 6(1), 58–73. doi:10.1109/4235.985692
- Day, R., & Quinn, G. (1989). Comparisons of treatments after an analysis of variance in ecology. *Ecological Monographs*, 59(4), 433–463. doi:10.2307/1943075
- Fang, W. (2008). *Swarm intelligence and its application In the optimal design of digital filters*. Wuxi: Jiangnan University.
- Fang, W., Sun, J., Ding, Y., Wu, X., & Xu, W. (2010). A review of Quantum-behaved Particle Swarm Optimization. *IETE Technical Review*, 27(4), 336–348. doi:10.4103/0256-4602.64601
- Fang, W., Sun, J., & Xu, W. (2009). Analysis of odd operators on quantum-behaved particle swarm optimization algorithm. *Mathematics and Natural Computation*, 5(2), 487–496. doi:10.1142/S179300570900143X
- Farzi, S., Shavazi, A., & Pandari, A. (2013). Using quantum-behaved Particle swarm optimization for portfolio selection problem. *The International Arab Journal of Information Technology*, 10(2), 111–119.
- Indiral, K., Kanmani, S., & Jagan, R. (2014). An evolutionary quantum behaved particle swarm optimization for mining association rules. *International Journal of Scientific & Engineering Research*, 5(5), 379–388.
- Ji, H., Yi, F., & (2016). An Improved Cooperative QPSO Algorithm with Adaptive Mutation Based on Entire Search History. *Tien Tzu Hsueh Pao*, 44(12). doi:10.3969/j.issn.0372-2112.2016.12.013
- Kennedy, J., & Eberhart, R. (1995). Particle swarm optimization. In *Proceedings of IEEE International Conference on Neural Networks*, Perth, WA. (pp. 1942-1948). IEEE. 10.1109/ICNN.1995.488968
- Manju, A., & Nigam, M. J. (2014, June). Applications of quantum inspired computational intelligence: A survey. *Artificial Intelligence Review*, 42(1), 79–156. doi:10.1007/10462-012-9330-6
- Nan, W., Song, F.-M., & (2016). Universal Quantum Computer: Theory, Organization and Implementation. *Chinese Journal of Computers*, 39(12). doi:10.11897/SPJ.1016.2016.02429
- Omkar, S., Khandelwal, R., Ananth, T., Narayana Naik, G., & Gopalakrishnan, S. (2009). Quantum behaved Particle Swarm Optimization (QPSO) for multi-objective design optimization of composite structures. *Expert Systems with Applications*, 36(8), 11312–11322. doi:10.1016/j.eswa.2009.03.006
- Sheng, X., Xi, M., Sun, J., & Xu, W. (2015). Quantum-behaved particle swarm optimization with novel adaptive strategies. *Journal of Algorithms & Computational Technology*, 9(2), 143–161. doi:10.1260/1748-3018.9.2.143
- Solis, F., & Wets, R. (1981). Minimization by random search techniques. *Mathematics of Operations Research*, 6(1), 19–30. doi:10.1287/moor.6.1.19

A Quantum Particle Swarm Optimization Algorithm Based on Self-Updating Mechanism

Suganthan, P., Hansen, N., & Liang, J. (2005). *Problem definitions and evaluation criteria for the CEC 2005 special session on real-parameter optimization*. Singapore: Nanyang Technological University.

Sun, J., Fang, W., Xu, W., & (2012). Quantum-behaved particle swarm optimization analysis of individual particle behavior and parameter selection. *Evolutionary Computation*, 20(3), 349–393. doi:10.1162/EVCO_a_00049 PMID:21905841

Sun, J., Xu, W., & Feng, B. (2004). A global search strategy of quantum behaved particle swarm optimization. In *Proceedings of the 2004 IEEE Conference on Cybernetics and Intelligent Systems*, Singapore (pp. 111-116). IEEE.

Sun, J., Xu, W., Plade, V., & (2012). Convergence analysis and improvement of quantum-behaved particle swarm optimization. *Information Sciences*, 193, 81–103. doi:10.1016/j.ins.2012.01.005

Van Den Bergh, F. (2001). *An analysis of particle Swarm optimists*. Pretoria: University of Pretoria.

Xi, J., & Xu, W. (2008). An improved quantum-behaved particle swarm optimization algorithm with weighted mean best position. *Applied Chemistry and Computation*, 205(2), 751–759.

Zhang, H.-G., Mao, S.-W., & (2016). Overview of Quantum Computation Complexity Theory. *Chinese Journal of Computers*, 39(12). doi:10.11897/SPJ.1016.2016.02403

This research was previously published in the International Journal of Swarm Intelligence Research (IJSIR), 9(1); pages 1-19, copyright year 2018 by IGI Publishing (an imprint of IGI Global).

Chapter 2

An Improved Generalized Quantum-Inspired Evolutionary Algorithm for Multiple Knapsack Problem

Sulabh Bansal

School of Computing and Information Technology, Manipal University Jaipur, Jaipur, India

C. Patvardhan

Faculty of Engineering, Dayalbagh Educational Institute (DEI), Agra, India

ABSTRACT

This article describes how the 0/1 Multiple Knapsack Problem (MKP), a generalization of popular 0/1 Knapsack Problem, is NP-hard and harder than simple Knapsack Problem. Solution of MKP involves two levels of choice – one for selecting an item to be placed and the other for selecting the knapsack in which it is to be placed. Quantum Inspired Evolutionary Algorithms (QIEAs), a subclass of Evolutionary algorithms, have been shown to be effective in solving difficult problems particularly NP-hard combinatorial optimization problems. QIEAs provide a general framework which needs to be customized according to the requirements of a given problem to obtain good solutions in reasonable time. An existing QIEA for MKP (QIEA-MKP) is based on the representation where a Q-bit collapse into a binary number. But decimal numbers are required to identify the knapsack where an item is placed. The implementation based on such representation suffers from overhead of frequent conversion from binary numbers to decimal numbers and vice versa. The generalized QIEA (GQIEA) is based on a representation where a Q-bit can collapse into an integer and thus no inter conversion between binary and decimal is required. A set of carefully selected features have been incorporated in proposed GQIEA-MKP to obtain better solutions in lesser time. Comparison with QIEA-MKP shows that GQIEA-MKP outperforms it in providing better solutions in lesser time for large sized MKPs. The generalization proposed can be used with advantage in other Combinatorial Optimization problems with integer strings as solutions.

DOI: 10.4018/978-1-7998-8593-1.ch002

1. INTRODUCTION

0-1 Multiple Knapsack Problem (MKP) is a generalization of the standard 0-1 Knapsack Problem (KP) where multiple knapsacks are required to be filled instead of one.

Given a set of n items with their profits p_j and weights w_j , $j \in \{1, \dots, n\}$ and m knapsacks with capacities c_i , $i \in \{1, \dots, m\}$ the MKP is to select a subset of items to fill given m knapsacks such that the total profit is maximized and sum of weights in each knapsack i doesn't exceed its capacity c_i .

$$\text{maximize: } \sum_{i=1}^m \sum_{j=1}^n p_j x_{ij} \quad (1)$$

$$\text{subject to: } \sum_{j=1}^n w_j x_{ij} \leq c_i, \quad i \in \{1, \dots, m\}, \quad (2)$$

$$\sum_{i=1}^m x_{ij} \leq 1, \quad j \in \{1, \dots, n\}, \quad (3)$$

$$x_{ij} \in \{0,1\}, \quad \forall i \in \{1, \dots, m\}, \quad \forall j \in \{1, \dots, n\}, \quad (4)$$

where $x_{ij} = 1$ if item j is assigned to knapsack i , $x_{ij} = 0$ otherwise and coefficients p_j , w_j and c_i are positive integers.

In order to avoid any trivial case, the following assumptions are made

1. Every item has a chance to be placed at least in largest knapsack:

$$\max_{j \in N} w_j \leq \max_{i \in \{1, \dots, m\}} c_i. \quad (5)$$

2. The smallest knapsack can be filled at least by the smallest item:

$$\min_{i \in \{1, \dots, m\}} c_i \leq \min_{j \in N} w_j. \quad (6)$$

3. There is no knapsack which can be filled with all N items:

$$\sum_{j=1}^n w_j \geq c_i, \quad \forall i \in \{1, \dots, m\} \quad (7)$$

The subset sum variant of MKP having $p_j = w_j$, $j \in \{1, \dots, n\}$, is known as Multiple Subset Sum Problem (MSSP).

The MKP have several applications. An application is seen when scheduling jobs on processors where some machines are unavailable for a fixed duration or some high priority jobs are pre-assigned to processors (Diedrich & Jansen, 2009). A real-world application of MKP is the problem of cargo loading where some containers need to be chosen from a set of n containers to be loaded in m vessels with different loading capacities for the shipment of the containers (Eilon & Christofides, 1971). Another real-world problem for MSSP is mentioned in (Kellerer, Pferschy, & Pisinger, 2004, p. 287) from a company producing objects of marble.

The MKP problem is strongly NP-complete. Some approximation algorithms exist for MKP. Kellerer (Kellerer H., 1999) presented a Polynomial Time Approximation Scheme for MKP with identical capacities. Chekuri & Khanna (Chekuri & Khanna, 2006) generalized it and presented the PTAS for MKP. However, no Fully Polynomial Time Approximation Scheme is possible for MKP (Chekuri & Khanna, 2006).

Martello & Toth (Martello & Toth, Solution of the zero-one multiple knapsack problem, 1980; Martello & Toth, Knapsack Problems: Algorithms and Computer Implementations, 1990) proposed a heuristic algorithm, called MTHM, for solving the MKP. This algorithm consists of three phases as follows. During first phase, an initial feasible solution is obtained by applying the Greedy algorithm to the first knapsack; a set of remaining items is obtained, then the same procedure is applied for all knapsacks iteratively. The initial solution is improved during the second phase by swapping each pair of items assigned to different knapsack. Then a new item is inserted if possible such that the total profit is increased. Each selected item is replaced by one or more remaining items during the last phase if it enhances the profit sum. The details are available in (Martello & Toth, Knapsack Problems: Algorithms and Computer Implementations, 1990, pp. 179-181).

Quantum-Inspired Evolutionary Algorithm (QIEA) is a population based search technique where the representation of individuals and operators involved in generation of new individuals are both designed based on concepts from Quantum Computing. Various forms of QIEAs have been used to solve a variety of difficult problems (Yang, Wang, & Jiao, 2004; Patvardhan, Narayan, & Srivastav, 2007; Platel, Schliebs, & Kasabov, 2007; Sailesh Babu, Bhagwan Das, & Patvardhan, 2008; Mani & Patvardhan, 2010; Wang & Li, 2010; Yang, Wang, & Jiao, 2010; Xiao, Yan, Zhang, & Tang, 2010; Arpaia, Maisto, & Manna, 2011; Patvardhan, Prakash, & Srivastav, (ICOREM 2009), 2012). QIEA, originally proposed by Han & Kim (Han & Kim, 2002), is directly applicable in problems where a Q-bit individual represents a linear superposition of binary solutions. Alegria & Tupac (Alegria & Tupac, 2013) proposed a generalization of the QIEA (GQIEA), where a Q-bit individual is a superposition of combinatorial solutions represented as a string of non-binary integers, to improve performance in combinatorial optimization.

QIEA-MKP (Patvardhan, Bansal, & Srivastav, Balanced quantum-inspired evolutionary algorithm for multiple knapsack problem, 2014) is a hybridized QIEA to solve MKP. It is based on the popular representation used in QIEAs where Q-bit represents the superposition of binary solutions. The observation of Q-bit individuals results in binary solutions. Thus, such a representation puts an overhead of frequent conversions from binary to decimal and vice versa. A selected item can be placed only in single knapsack at a time for a solution of MKP. But the probability of an item to be selected in to different knapsacks keeps on changing during evolution. These probabilities should be normalized such that their sum remains equal to 1. QIEA-MKP doesn't normalize these probabilities in that way. GQIEA provides a solution for the issue through the use a generalized representation of Q-bits (GQ-bit) and their update operator (Alegria & Tupac, 2013).

In this paper an effective GQIEA is proposed for MKP. The representation for GQ-bit, the process for observing a GQ-bit and the process to update a GQ-bit has been defined as required for MKP. The proposed GQIEA, dubbed GQIEA-MKP, is hybridized with an existing heuristic for MKP known as MTHM (Martello & Toth, Solution of the zero-one multiple knapsack problem, 1980). Various other features like biased initialization of GQ-bit individuals, local search, mutation, re-initialization etc. have been designed and incorporated in GQIEA-MKP. GQIEA-MKP balances heuristics to promote exploitation for obtaining good solutions and several other features like mutation and re-initialization to increase randomness and power to explore unreached areas. A comparison shows on a variety of randomly generated instances of MKP that GQIEA-MKP outperforms QIEA-MKP.

The methodology adopted here to design GQIEA can be used to design similar GQIEAs to solve other combinatorial problems where solutions are represented as sequences of integers.

The rest of the paper is organized as follows. A brief description of the QIEA-MKP is given in section 2. In section 3 GQIEA_MKP is described. Computational performance of QIEA-MKP and GQIEA-MKP is presented in section 4. Conclusions are presented in section 5.

2. QIEA -MKP

The QIEA introduced in (Han & Kim, 2002) use a vector of Q-bits to represent the probabilistic state of individual. Each Q-bit is represented as $q_i = \begin{bmatrix} \alpha_i \\ \beta_i \end{bmatrix}$ where $|\alpha_i|^2$ is the probability of state being 1 and $|\beta_i|^2$ is the probability of state being 0 such that $|\alpha_i|^2 + |\beta_i|^2 = 1$. Thus, a Q-bit string with n bits represents a superposition of 2^n binary states. QIEA uses the Q-gate, for example a rotation gate to update the Q-bits as follows:

$$\begin{bmatrix} \alpha_i^{t+1} \\ \beta_i^{t+1} \end{bmatrix} = \begin{bmatrix} \cos(\Delta_i) & -\sin(\Delta_i) \\ \sin(\Delta_i) & \cos(\Delta_i) \end{bmatrix} \begin{bmatrix} \alpha_i^t \\ \beta_i^t \end{bmatrix} \quad (8)$$

where, α_i^{t+1} and β_i^{t+1} denote probabilities for i^{th} Q-bit in $(t + 1)^{\text{th}}$ iteration and Δ_i is equivalent to the step size in typical iterative algorithms in the sense that it defines the rate of movement towards the currently perceived optimum.

The implementation of QIEAs to solve MKP requires special consideration as it calls for subset allocation and selection. A solution of MKP indicates the selection status of each item and the knapsack in which it is placed. A solution consists of a string of length n of integer values ranging from 0 to m. 0 indicates that the corresponding item is not selected. Otherwise, it mentions the knapsack in which the item is placed.

To implement QIEA-MKP (Patvardhan, Bansal, & Srivastav, Balanced quantum-inspired evolutionary algorithm for multiple knapsack problem, 2014) two binary strings (arrays) are used to represent one complete solution. A binary string of length n, having one bit for each item conveying about its selection status, and another of length $(n * \log_2 m)$ contains the index in binary of knapsack in which it is packed. The integers in $\{1, \dots, m\}$ are represented by a bit string of length $\log_2 m$. A qubit individual is represented by two components of lengths n and $n * \log_2 m$ corresponding to two binary strings of solution.

Two components of population of qubit individuals after t^{th} iteration are represented using $Q1(t)$ and $Q2(t)$, $P1(t)$ and $P2(t)$ represent the first and second components of population of individual solutions, $B1(t)$ and $B2(t)$ is the set of best solutions corresponding to first and second component of each individual. The individuals of populations q_j^t is composed of $q1_j^t$ and $q2_j^t$, p_j^t is composed of $p1_j^t$ and $p2_j^t$, and b_j^t is composed of $b1_j^t$ and $b2_j^t$ for each $j \in \{1, \dots, n\}$; b have $b1$ and $b2$. In the following paragraphs a brief description of procedures implemented in QIEA-MKP is given.

Initialize (q_j^t): The first component (say $q1_j^t$) is initialized as follows. The items are considered divided in to 3 classes based on where they lie in order of preference. Qubits for items lying in first class (third class) are assigned values closer to 1 (0) so that they have high (low) probability of collapsing to value 1. Items lying in the second class require more processing for convergence to either 0 or 1, hence intermediate values between 0 and 1 are assigned to them. As a result, the hybridised algorithm starts exploiting the area or region in solution space having solutions closer to optimal with higher probability. Qubits of second component (say $q2_j^t$) are assigned the value $1/\sqrt{2}$.

Observe: The procedure collapses the first (second) component qubit individual/s to generate first (second) component of solution individual/s.

Repair: Solutions are repaired based on phase 1 of description of MTHM in (Martello & Toth, Knapsack Problems: Algorithms and Computer Implementations, 1990). Overheads add up due to conversion required for binary representation of decimal numbers used in second component of solution representation.

Update q_j^t based on b_j^t : Rotates the qubits $q1_j^t$ towards bits in $b2_j^t$ and $q2_j^t$ towards bits in $b1_j^t$ as explained earlier and defined in (Han & Kim, 2002) using the rotation angle as 0.01.

Evaluate p_j^t : Sum the profits of items set to 1 in $p1_j^t$.

3. GQIEA-MKP

A GQ-bit individual in the proposed GQIEA-MKP, inspired from (Alegria & Tupac, 2013), is represented as an array of $m+1$ real

$$GQ_i = \begin{bmatrix} \pm_0 \\ \pm_1 \\ \vdots \\ \pm_m \end{bmatrix} \tag{9}$$

where, $0 \leq \alpha_i \leq 1$ and $\sum_{i=1}^m \alpha_i = 1$. Total number of different possible states it represents is $m+1$, instead of just two. In this representation, α_0 is the probability of an item not getting selected in any of the knapsacks, α_i , for $i \in \{1, \dots, m\}$ is the probability of item being put in i^{th} knapsack. Similar to the Q-gate in the original QIEA, two GQ-gate operators: the arithmetic GQ-gate and the geometric GQ-gate have been proposed in (Alegria & Tupac, 2013). Here arithmetic GQ-gate is used to update GQ-bit individuals as described in section 3.3.

The items having a greater profit by weight ratio are considered to have higher probability of their inclusion in the optimal solution. Thus, the items in input are sorted in the decreasing order of their profit by weight ratio. This sorting is used to initialize GQ-bit individuals as explained in section 3.1 so that they can generate better solutions. The sorted input is utilized to improve repair procedure also, section 3.4, so that it provides better solutions.

A brief description of the primary operations in GQIEA-MKP and the features applied for improvement follows.

3.1. Initialize

The best solution is initialized with the good solution obtained using MTHM heuristic as described in (Martello & Toth, Solution of the zero-one multiple knapsack problem, 1980; Martello & Toth, Knapsack Problems: Algorithms and Computer Implementations, 1990).

To initialize GQ-bit individuals an array, q , of real numbers of length n is first initialized as follows. The items are considered divided in to 3 classes based on where they lie in the order of preference. The values for items lying in first class (third class) are assigned values closer to 1 (0) so that they have high (low) probability of collapsing to value 1. Items lying in the second class require more processing for convergence to either 0 or 1, hence intermediate values between 0 and 1 are assigned to them. As a result, the hybridised algorithm is expected to start exploiting the area or region in solution space having solutions closer to optimal with higher probability. The initialization of q_j^t is further done using q as in Pseudo-code in Figure 1.

Figure 1. Pseudo-code for Initialize function in GQIEA-MKP

```
Procedure Initialize( $q_j^t$ )  
1 let  $C$  be the sum of all capacities  $c_i$  and  $c_a$  be average capacity;  
2 let  $W$  be sum of weights  $w_i$  of all items and  $w_a$  be the average weight  
3 for  $i$  from 1 to  $n$  do{  
4      $\alpha_0$  of  $q_j^t[i]$  is set to  $1.0 - q[i]$ ;  
5     for  $j$  from 1 to  $m$   
6          $\alpha_j$  of  $q_j^t[i]$  is set to  $q[i] * c_j / C + (w_i - w_a) * (c_j - c_a) / (w_a * c_a)$ ;  
7 }/* for  $i$ */
```

Since a knapsack with larger capacity can hold more items, the probability of an item being put into a particular knapsack is considered to be proportional to the weight of the knapsack divided by the sum of weights of all knapsacks. The probability of an item also depends on the relation between weight of an item and the capacity of knapsack. Initially, lighter items have higher probability to be placed in smaller knapsacks and heavier items have higher probability to be placed in larger knapsacks. This is reflected in steps 5 and 6 in Figure 1.

The GQ-bit component of i^{th} item corresponding to j^{th} knapsack is set to $q[i] * c_j / C + (w_i - w_a) * (c_j - c_a) / (w_a * c_a)$, where $q[i]$ is the value of Q-bit assigned to i^{th} item based on above method, c_j is the capacity of j^{th} knapsack, C is the sum total of capacities of all knapsacks, w_i is the weight of i^{th} item, w_a is the average weight of an item, c_a is the average capacity of a knapsack.

3.2. Observe

The procedure is described in Pseudo-code of Figure 2. To understand the approach, consider a 3 state

GQ-bit system $\begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \end{bmatrix}$. An integer, p , need to be generated ranging between 0 and 2 to define the state of

an item in the solution. if $(\alpha_0 + \alpha_1 + \alpha_2)$ is not equal to 1 then it indicates an error. Otherwise a random variable r_1 is generated and p is assigned the value as follows

$$p = \begin{cases} 0, & r_1 < \alpha_0 \\ 1, & \alpha_0 < r_1 < \alpha_0 + \alpha_1 \\ 2, & \alpha_0 + \alpha_1 < r_1 < 1 \end{cases}$$

This idea extends to the $m+1$ GQ-bit system naturally when there are m knapsacks.

Figure 2. Pseudo-code for Observe function in GQIEA-MKP

```

Procedure Observe( $q_j^t$ ) //return  $p_j^t$ 
1  for i from 1 to n do{
2      let r be a random number;  $p_j^t[i]=0$ ;  $N=0.0$ ;
3      for j from 1 to m
4           $N=N + \alpha_j$  of  $q_j^t[i]$ ;
5          if( $r < N$ ){  $p_j^t[i]=j$ ; break;}
6      }//*for j*//
7  }//* for i*//
    
```

3.3 Update

q_j^t based on b_j^t : The procedure is described in pseudo-code in Figure 3. Let the j^{th} GQ-bit of a GQ-bit individual represent a superposition of $m+1$ states $\{s_0, s_2, \dots, s_m\}$. If the state s_ϕ was found in j^{th} position of the best individual b_j^t of the generation, the new values of α_1 are determined according to the arithmetic GQ-gate as defined in equation (10), where Δd is a parameter of the algorithm. Each GQ-bit is

then normalized to ensure that $\sum_{i=1}^r \pm_i = 1$ as shown in step 5 in Figure 3.

$$\alpha_i = \begin{cases} \alpha_i + \Delta d & \text{if } i = \phi \\ \alpha_i & \text{if } i \neq \phi \end{cases} \quad (10)$$

Figure 3. Pseudo-code for Update in GQIEA-MKP

```

Procedure Update(  $q_j^t$  based on  $b_j^t$  ) //
1  let  $p_j^t$  is solution observed using  $q_j^t$ ;
2  for i from 1 to n do{
3      if(  $b_j^t$  is better than  $p_j^t$  ) {  $\Delta=0.1$ ;  $d=1.0 - \alpha_{b_j^t[i]}$  of  $q_j^t[i]$ ; }
4      for j from 1 to m{
5          if(  $j < > b_j^t[i]$  )  $q_j^t[i] = q_j^t[i] * (d - \Delta/d)$ ;
6          else  $q_j^t[i] = q_j^t[i] + \Delta$ ;
7      } // *for j* //
8  } // *for i* //
    
```

3.4. Improved Repair Function

In GQIEA-MKP, the repair function is modified to improve the quality of solutions while making them feasible based on the phase 1 of MTHM heuristic as described in (Martello & Toth, Knapsack Problems: Algorithms and Computer Implementations, 1990). This improves the speed of convergence. As explained earlier the items are sorted in order of their preference to include them into a knapsack. So, in each repair step, items having low preference (closest to the end in the sorted order) are removed and items having high preference (closest to the beginning in the sorted order) are added as necessary. The knapsacks are assumed to be sorted in order of their increasing capacity and that's the order in which they are considered when items are added into knapsacks (see Figure 4).

Figure 4. Pseudo-code for Repair function in GQIEA-MKP

```

Procedure Repair(x)
1  let  $R_i, \forall i \in \{1, \dots, m\}$  be residue in knapsack i;
2  for i from 1 to m{
3      while ( $R_i < 0$ ) {
4          let u be item of lowest preference in sorted input.
5          remove u from knapsack i;  $R_i = R_i + w_u$ ;
6      } // *while* //
7  } // *for i* //
8  for j from 1 to n {
9      let k be knapsack of minimum capacity such that  $R_i \geq w_j$  )
          {  $x_{kj} \leftarrow 1$ ;  $R_k = R_k - w_j$ ; }
10 } // *for j* //
    
```

3.5. Improving the Local Best Solutions

The local best solutions are further improved in two stages based on the phases 2 and 3 of MTHM heuristic (Martello & Toth, Solution of the zero-one multiple knapsack problem, 1980; Martello & Toth, Knapsack Problems: Algorithms and Computer Implementations, 1990). In first stage, Improve1, it tries to exchange every pair of items assigned to different knapsacks along with inserting a new item so that total profit is increased. In second stage, Improve2, every selected item (starting from last in the sorted order) is tried to be replaced by one of the remaining items so that the total profit sum is increased. The pseudo-codes of these procedures are given in Figure 5 and Figure. 6.

Figure 5. Pseudo-code for Improve1

```

Procedure Improve1(x)
1  let  $R_i \leftarrow c_i - \sum_{j=1}^n w_j x_{ij}, \forall i \in \{1, \dots, m\}$ ;
2  for each pair  $i$  and  $j$  in  $\{1, \dots, n\}$  {
3    if  $(\exists u, v \text{ in } \{1, \dots, m\} | x_{ui} = 1 \text{ and } x_{vj} = 1 \text{ and } (R_u \geq w_j - w_i) \text{ and } (R_v \geq w_i - w_j))$ {
4      if  $(\exists k \in \{1, \dots, n\} | (R_u \geq w_j + w_k - w_i) \text{ or } (R_v \geq w_i + w_k - w_j))$ {
5        let  $k = (\min_{s \in \{1, \dots, n\}} s | (R_u \geq w_j + w_s - w_i) \text{ or } (R_v \geq w_i + w_s - w_j))$ 
6        if  $((R_u \geq w_j + w_s - w_i) \{ x_{ui} \leftarrow 0; x_{vj} \leftarrow 0; x_{uj} \leftarrow 1; x_{vi} \leftarrow 1; x_{uk} \leftarrow 1; \}$ 
7        else  $\{ x_{ui} \leftarrow 0; x_{vj} \leftarrow 0; x_{uj} \leftarrow 1; x_{vi} \leftarrow 1; x_{vk} \leftarrow 1; \}$ 
8      }/* if*/
9    }/* if*/
10 }/*for pair  $i$  and  $j$ */

```

Figure 6. Pseudo-code for Improve2

```

Procedure Improve2(x)
1  let  $R_i \leftarrow c_i - \sum_{j=1}^n w_j x_{ij}, \forall i \in \{1, \dots, m\}$ ;
2  for  $\forall i \in \{1, \dots, n\}$ {
3    if  $(\exists u \in \{1, \dots, m\} | x_{ui} = 1)$ {
4      for  $\forall j \in \{1, \dots, n\} | x_{vj} = 0 \forall v \in \{1, \dots, m\}$  {
5        if  $(R_u + w_i - w_j \geq 0) P_j \leftarrow p_j - p_i$ ; else  $P_j \leftarrow 0$ ;
6      }/* for  $j$ */
7      let  $P_k = \max_{v \in \{1, \dots, n\}} P_j$ ;
8      if  $(P_k > 0) \{ x_{ui} \leftarrow 0; x_{uk} \leftarrow 1; R_u \leftarrow R_u + w_i - w_k; \}$ 
9    }/*If  $u$  */
10 }/*for  $i$  */

```

3.6. Mutation of Solutions Appearing to be Stuck in Local Optimum

The proposed GQIEA-MKP have a the tendency of getting stuck in local optima due several heuristic based deterministic features discussed above in sections 3.1, 3.4 and 3.5. To combat this tendency, the generated solution is mutated such that randomly selected 2-3 bits in the solution vector are changed to 0, when it is close to global best solution (Hamming distance is less than 2) found so far it. The partial solution is improved using ImproveStage1. This operator improves diversity with small computational effort. It helps to explore the solution space around a current solution such that an optimal in vicinity is not missed. This improves the chances of finding optimal in case it is in vicinity of the converging solution.

3.7. Re-Initialization of GQ-Bit Individuals

After a sequence of generations a GQ-bit individual converges such that all solutions generated from it are same. No new solutions can be generated using such individuals. Thus, when a GQ-bit individual generates same solution for more than 3 times out of 5, it is reset as in initialization. It increases the diversity of solutions explored through the Q-bit individuals with small computational effort.

3.8 Faster Local Exploitation of GQ-Bit Individuals Before Global Exploration

The evolution steps of a basic QIEA are executed with the specialized local search procedure for some iteration to update some of the GQ-bit individuals. The steps listed in the following are performed on half of the GQ-bit individuals for small number of times (empirically set as 15 for this work).

- Make
- Repair
- Improve1
- Improve2
- Update

The execution of these steps will exploit intensively the area represented by the initial GQ-bit individuals. This execution may solve some of the easier instances earlier. The resulting GQ-bit individuals favour the smaller region in search space around better solutions.

The features and steps explained above are put together to design the proposed GQIEA-MKP. The Pseudo-code of the GQIEA-MKP is given in Figure 7. In the pseudo-code; t refers to the current iteration, population of GQ-bit individuals after t^{th} iteration is represented using $Q(t)$, $P(t)$ represent the population of individual solutions, $B(t)$ is the population of best solutions corresponding to each GQ-bit individual, c_i is the capacity of the i^{th} knapsack. Individuals represented by $Q(t)$ are referred to as q_j^t , individuals in $P(t)$ are referred to as p_j^t , similarly individuals in $B(t)$ are referred to as b_j^t for each $j \in n$; b refers to global best solution found so far. Some other functions used are as follows:

HamDistance (p_j^s , b): Hamming distance is returned as number of places in two strings having different bits.

Figure 7. Pseudo-code for GQIEA-MKP

```

Improved GQIEA-MKP
1  SortGreedy the Input;
2   $t \leftarrow 0$ ;  $b \leftarrow 0$ ;
3  Initialize Q-bit Individuals  $Q(t)$ ;
4  Initialize  $b$ 
5  Observe  $P(t)$  from  $Q(t)$ ;
6  Repair ( $P(t)$ );
7  Initialize  $B(T)$  as  $P(T)$ ;
8  for each  $j \in \{1, \dots, n/4\}$  {
9    Observe  $p_j^t$  from  $q_j^t$ ;
10   Repair ( $p_j^t$ );
11   Improve1 ( $p_j^t$ );
12   Improve2 ( $p_j^t$ );
13   if ( $p_j^t$  is better than  $b_j^t$ )  $b_j^t \leftarrow p_j^t$ ;
14 }
15 while ( $t < \text{MaxIterations}$ ) {
16    $t \leftarrow t+1$ ;  $\text{cnt}_j \leftarrow 0$ ;
17   for  $r$  from 0 to  $\eta_1$  do{
18     for  $s$  from 0 to  $\eta_2$  do{
19       Observe  $P(s)$  from  $Q(t)$ ;
20       Repair( $P(s)$ );
21       for each  $j \in \{1, \dots, n\}$  {
22         if (HamDistance( $p_j^s, b$ ) < 2) {Mutate( $p_j^s$ );Improve1( $p_j^s$ );}
23       }/**for  $j^*$ */
24       for each  $j \in \{1, \dots, n\}$ 
25         if ( $p_j^s$  better than  $p_j^t$ )  $p_j^t \leftarrow p_j^s$ ; else if ( $p_j^s$  equal  $p_j^t$ )  $\text{cnt}_j \leftarrow \text{cnt}_j + 1$ ;
26       } /**for  $s^*$ */
27       if( $\text{cnt}_j > 3$ ){
28         ReInitialize( $q_j^t$ ) for each  $j \in \{1, \dots, n\}$ ;
29       }/**if  $\text{cnt}_j^*$ */
30       for  $j \in \{1, \dots, n\}$  Improve2( $p_j^t$ ) ;
31       for each  $j \in \{1, \dots, n\}$  if ( $p_j^t$  is better than  $b_j^t$ )  $b_j^t \leftarrow p_j^t$ ;
32       for each  $j \in \{1, \dots, n\}$  if ( $b_j^t$  is better than  $b$ )  $b \leftarrow b_j^t$  ;
33       for each  $j \in \{1, \dots, n\}$  Update  $q_j^t$  based on  $b_j^t$  ;
34     } /**for  $r^*$ */
35     for each  $j \in \{1, \dots, n\}$  Update  $q_j^t$  based on  $b$ ;
36   } /**while*/

```

4. RESULTS AND DISCUSSION

The experiments are done on Intel® Xeon® Processor E5645 (12M Cache, 2.40 GHz, 5.86 GT/s Intel® QPI). The machine uses Red Hat Linux Enterprise 6.

An Improved Generalized Quantum-Inspired Evolutionary Algorithm for Multiple Knapsack Problem

The solutions converged for most of the problem instances considered here within 10 iterations hence maxIterations is set to 10. Empirically, η_1 and η_2 are set to 5 and population size is set to 10.

The performance is observed on randomly generated instances having elements 1000, 5000 and 10000 with number of knapsacks as 2, 5 and 10. These instances are randomly generated, using the generator of instances available at the Pisinger's home page i.e. <http://www.diku.dk/~pisinger/codes.html>. Two types of instances have been generated, first the strongly correlated where weights w_j are distributed in $[1, R]$ and profits p_j are calculated as $p_j = w_j + R/10$ and second is Uncorrelated where weights w_j and profits p_j are independently distributed in $[1, R]$. Such instances correspond to a real-life situation where the return is proportional to the investment plus some fixed charge for each project.

Two different cases of capacities are considered: similar and dissimilar.

In case of similar capacities the first $m-1$ capacities $c_i, \hat{i} \in \{1, \dots, m-1\}$ are distributed in the range

$$\left[0.4 \sum_{j=1}^n w_j / m, 0.6 \sum_{j=1}^n w_j / m \right] \quad \forall i \in \{1, \dots, m-1\} \quad (11)$$

In case of dissimilar capacities the first $m-i$ capacities c_i are distributed in the range

$$\left[0, 0.5 \sum_{j=1}^n w_j - \sum_{k=1}^{i-1} c_k \right] \quad \forall i \in \{1, \dots, m-1\} \quad (12)$$

The last capacity c_m is chosen as

$$c_m = 0.5 \sum_{j=1}^n w_j - \sum_{i=1}^{m-1} c_i \quad (13)$$

Table 1. Details of Instances generated in four different classes.

n_m_s	STRCORRDISS			STRCORRSIM			UNCORRDISS			UNCORRSIM		
	Optimal	Capacity	Heuristic	Optimal	Capacity	Heuristic	Optimal	Capacity	Heuristic	Optimal	Capacity	Heuristic
1000_2_1	258384	251354	258290	258384	251354	258383	391675	256767	391653	391675	256767	391653
1000_2_2	260485	253465	260483	260485	253465	260452	409026	250741	408994	409026	250741	408990
1000_2_3	258942	251912	258721	258942	251912	258940	406439	248256	406426	406439	248256	406413
1000_2_4	255726	248626	255725	255726	248626	255681	408580	248569	408564	408580	248569	408564
1000_2_5	265225	258235	265074	265225	258235	265213	415860	254070	415846	415860	254070	415835
5000_2_1	1311854	1276724	1311854	1311854	1276724	1311752	2003828	1262124	2003806	2003828	1262124	2003821
5000_2_2	1311739	1276659	1311656	1311739	1276659	1311703	2045748	1253440	2045737	2045748	1253440	2045737
5000_2_3	1287821	1252561	1287755	1287821	1252561	1287821	2019647	1250828	2019633	2019647	1250828	2019630
5000_2_4	1298230	1262920	1298230	1298230	1262920	1298230	2034403	1265161	2034400	2034403	1265161	2034387
5000_2_5	1315856	1280766	1315807	1315856	1280766	1315856	2026015	1271477	2025987	2026015	1271477	2025987
10000_2_1	2607305	2536995	2607147	2607305	2536995	2607281	4040310	2536030	4040301	4040310	2536030	4040301
10000_2_2	2584205	2513685	2584015	2584205	2513685	2584205	4067232	2531903	4067224	4067232	2531903	4067221

continues on following page

An Improved Generalized Quantum-Inspired Evolutionary Algorithm for Multiple Knapsack Problem

Table 1. Continued

n_m_s	STRCORRDISS			STRCORRSIM			UNCORRDISS			UNCORRSIM		
	Optimal	Capacity	Heuristic	Optimal	Capacity	Heuristic	Optimal	Capacity	Heuristic	Optimal	Capacity	Heuristic
10000_2_3	2587728	2517308	2587728	2587728	2517308	2587637	4037917	2510003	4037911	4037917	2510003	4037906
10000_2_4	2601537	2531107	2601537	2601537	2531107	2601537	4054712	2506649	4054704	4054712	2506649	4054700
10000_2_5	2619338	2549058	2619333	2619338	2549058	2619338	4029938	2533368	4029933	4029938	2533368	4029915
1000_5_1	258384	251354	258125	258384	251354	258224	391675	256767	391627	391675	256767	391605
1000_5_2	260485	253465	260231	260485	253465	260270	409026	250741	408994	409026	250741	408922
1000_5_3	258942	251912	258652	258942	251912	258907	406439	248256	406377	406439	248256	406364
1000_5_4	255726	248626	255711	255726	248626	255438	408580	248569	408552	408580	248569	408484
1000_5_5	265225	258235	264857	265225	258235	265157	415860	254070	415835	415860	254070	415823
5000_5_1	1311854	1276724	1311710	1311854	1276724	1311745	2003828	1262124	2003805	2003828	1262124	2003805
5000_5_2	1311739	1276659	1311656	1311739	1276659	1311729	2045748	1253440	2045725	2045748	1253440	2045714
5000_5_3	1287821	1252561	1287411	1287821	1252561	1287811	2019647	1250828	2019630	2019647	1250828	2019605
5000_5_4	1298230	1262920	1297988	1298230	1262920	1298152	2034403	1265161	2034387	2034403	1265161	2034366
5000_5_5	1315856	1280766	1315466	1315856	1280766	1315614	2026015	1271477	2025962	2026015	1271477	2025962
10000_5_1	2607305	2536995	2606951	2607305	2536995	2607295	4040310	2536030	4040263	4040310	2536030	4040288
10000_5_2	2584205	2513685	2583961	2584205	2513685	2584194	4067232	2531903	4067211	4067232	2531903	4067206
10000_5_3	2587728	2517308	2587616	2587728	2517308	2587724	4037917	2510003	4037886	4037917	2510003	4037911
10000_5_4	2601537	2531107	2601523	2601537	2531107	2601439	4054712	2506649	4054695	4054712	2506649	4054689
10000_5_5	2619338	2549058	2619087	2619338	2549058	2619328	4029938	2533368	4029927	4029938	2533368	4029920
1000_10_1	258383	251354	258126	258384	251354	258091	409602	253519	409452	391675	256767	391526
1000_10_2	260485	253465	259936	260485	253465	260447	401741	255797	401615	409026	250741	408876
1000_10_3	258942	251912	258347	258942	251912	258449	406439	248256	406360	406439	248256	406256
1000_10_4	255726	248626	255370	255726	248626	254850	403660	256177	403617	408580	248569	408441
1000_10_5	265225	258235	264857	265225	258235	265087	406072	256221	405983	415860	254070	415706
5000_10_1	1311854	1276724	1311262	1311854	1276724	1311535	2024918	1275798	2024879	2003828	1262124	2003772
5000_10_2	1311739	1276659	1311569	1311739	1276659	1311710	2045748	1253440	2045696	2045748	1253440	2045621
5000_10_3	1287821	1252561	1287411	1287821	1252561	1287749	2019647	1250828	2019607	2019647	1250828	2019576
5000_10_4	1298230	1262920	1297988	1298230	1262920	1297908	2034403	1265161	2034373	2034403	1265161	2034333
5000_10_5	1304030	1268840	1303896	1315856	1280766	1315633	2026015	1271477	2025962	2026015	1271477	2025927
10000_10_1	2607305	2536995	2607178	2607305	2536995	2607256	4040310	2536030	4040253	4040310	2536030	4040263
10000_10_2	2584205	2513685	2584132	2584205	2513685	2583550	4067232	2531903	4067187	4067232	2531903	4067179
10000_10_3	2587728	2517308	2587616	2587728	2517308	2587570	4061148	2509396	4061129	4037917	2510003	4037853
10000_10_4	2601537	2531107	2601011	2601537	2531107	2601507	4035606	2513796	4035592	4054712	2506649	4054669
10000_10_5	2619338	2549058	2619179	2619338	2549058	2619318	4029938	2533368	4029914	4029938	2533368	4029889

45 instances are generated using code available in (Pisinger D.) in each of the three classes of instances namely Strongly Correlated instances with dissimilar capacities (STRCORRDISS), Strongly Correlated instances with similar capacities (STRCORRSIM), Uncorrelated instances with dissimilar capacities (UNCORRDISS) and Uncorrelated instance with similar capacities (UNCORRSIM). The Optimal profit (found using the Mulknaps algorithm of (Pisinger D., 1999) available at (Pisinger D.)), total capacity constraint (actually distributed in multiple knapsacks) and the value obtained using heuristic has been

An Improved Generalized Quantum-Inspired Evolutionary Algorithm for Multiple Knapsack Problem

reported for all of these instances in Table 1. The number of knapsacks (m) in these instances is 2, 5 or 10, total number of items (n) is 1000, 5000 or 10,000 and 5 different instances have been generated for each combination (total combinations 9) which are distinguished using the seed value as 1 to 5. The instances in each class have been distinguished using acronym n_m_s where n is the number of elements, m is the number of knapsacks and the s refers to seed.

The experiments have been performed using QIEA-MKP of (Patvardhan, Bansal, & Srivastav, Balanced quantum-inspired evolutionary algorithm for multiple knapsack problem, 2014) and proposed GQIEA-MKP. For both of these cases the tests have been done using population size of 20 and 100. Tables 2 to 5 compares the results obtained using QIEA-MKP and GQIEA-MKP. The best value obtained and the difference of best value from the average value over 30 runs has been shown in same column separated using pipe '|'. The average time taken to reach the best solution over 30 runs and average FES (Function Evaluations) has been shown in same column similarly. The largest best value provided by any of the four implementations of algorithms that is GQIEA_MKP(100), GQIEA_MKP(20) QIEA_MKP(100) and QIEA_MKP(20) in the table is darkened. The algorithm is made to terminate before the fixed maximum number of iterations (MAXIterations), when the optimal solution is found.

Table 2. Comparison of results obtained for strongly correlated instances having dissimilar capacities using QIEA-MKP and GQIEA-MKP with population sizes of 20 and 100. The values obtained using optimal values and heuristic are shown as reference. Best value and difference between best and average is shown for QIEAs. Time to reach best solution in seconds and Function Evaluations (FES) are given.

n_m_s	QIEA-MKP(20)		QIEA-MKP(100)		GQIEA-MKP(20)		GQIEA_MKP(100)	
	Best Best-Avg	T(sec) FES	Best Best-Avg	T(sec) FES	Best Best-Avg	T(sec) FES	Best Best-Avg	T(sec) FES
1000_2_1	258384 2.1	3.336 56.1	258384 0.27	12.636 222.37	258384 1.9	0.45 54	258384 0.5	2.024 215.2
1000_2_2	260485 1.8	0.652 4.87	260485 1	18.396 162	260485 0	0.246 2.2	260485 0	0.249 2.2
1000_2_3	258942 6.8	5.43 47.7	258942 3.3	23.303 211.53	258942 0	0.311 3.8	258942 0	0.315 3.8
1000_2_4	255725 0	0.045 0	255725 0	0.044 0	255726 0	0.077 3.3	255726 0	0.079 3.3
1000_2_5	265225 3.5	3.924 63.53	265225 0.9	14.33 240.27	265225 1.6	0.62 54.3	265225 0.2	3.807 309.5
5000_2_1	1311854 0	1.075 0	1311854 0	1.04 0	1311854 0	0.088 0	1311854 0	0.062 0
5000_2_2	1311679 20	122.914 12.6	1311679 16.03	1681.838 181.77	1311739 0	11.17 1	1311739 0	11.186 1
5000_2_3	128779 110	414.583 68.77	1287800 9.4	1732.235 295.7	1287821 0	16.33 2.2	1287821 0	16.343 2.2
5000_2_4	1298230 0	7.94 0	1298230 0	7.704 0	1298230 0	6.713 0	1298230 0	6.722 0
5000_2_5	1315835 23	184.401 32.63	1315836 15.4	1673.487 311.37	1315856 2	52.578 40.5	1315856 0	63.868 38.4
10000_2_1	2607248 27	1050.292 63.47	2607255 19.3	4416.376 283.17	2607305 1	211.426 29.6	2607305 0	1014.753 128.3
10000_2_2	2584146 25	2284.621 75.53	2584153 20.47	8888.503 313.57	2584205 1	863.77 42	2584205 0	3020.713 148.6
10000_2_3	2587728 0	86.604 0	2587728 0	84.957 0	2587728 0	77.947 0	2587728 0	78.008 0
10000_2_4	2601537 0	4.31 0	2601537 0	4.229 0	2601537 0	0.193 0	2601537 0	0.214 0
10000_2_5	2619333 0	4.308 0	2619333 0	4.202 0	2619338 2	227.629 29.1	2619338 0	955.099 128.1
1000_5_1	2583799.1	9.876 55.93	2583827.7	51.308 302.27	2583834.1	1.803 59.2	2583840.4	6.626 219.9
1000_5_2	2604759.2	9.542 56.43	2604763.2	44.469 272.83	2604805.2	0.921 63.2	2604844.7	3.762 52.4
1000_5_3	2589318.2	10.168 54.43	2589325.43	49.137 274.9	2589426.3	1.696 61.8	2589420.9	8.082 279.5
1000_5_4	2557153.8	1.458 6.9	2557163.67	16.344 90.03	2557264	2.286 57.9	2557261.2	11.3 277.2
1000_5_5	2652021 4.2	5.548 60.6	2652131 3.2	29.861 754.9	26521918.1	0.384 63.1	2652237.9	1.845 316
5000_5_1	1311797 29	526.492 66	1311797 17.6	2194.247 282.27	1311849 11	42.019 69	1311853 5	158.319 269.3

continues on following page

Table 2. Continued

n_m_s	QIEA-MKP(20)		QIEA-MKP(100)		GQIEA-MKP(20)		GQIEA_MKP(100)	
	Best Best-Avg	T(sec) FES	Best Best-Avg	T(sec) FES	Best Best-Avg	T(sec) FES	Best Best-Avg	T(sec) FES
5000_5_2	131169022	534.489 53.53	1311693 14.3	2620.31 271.97	1311734 10	14.669 60.8	1311739 7	78.675 291.7
5000_5_3	128777018	500.59 60.9	1287779 17.43	2245.453 281.83	1287816 16	89.544 73.4	1287820 9	302.204 259.2
5000_5_4	1298162 23	823.385 69.3	1298174 23.03	3268.562 284.3	1298230 7	117.392 51.5	1298230 1	553.283 242
5000_5_5	1315789 21	540.043 67.27	1315814 28.57	2258.925 292.57	1315854 13	52.204 59.8	1315856 7	243.346 287.7
10000_5_1	2607139 32	6226.748 65.83	2607144 19.7	28216.31 304.9	2607299 18	1611.487 54.9	2607304 8	7463.16 250.6
10000_5_2	2584135 28	5753.947 58.93	2584145 24.63	25850.299 272.03	2584195 4	3716.762 48.9	2584195 0	16264.166 220.9
10000_5_3	2587616 0	47.905 0	2587616 0	47.328 0	2587726 12	1619.371 71.4	2587728 2	6238.245 292.7
10000_5_4	2601523 0	64.643 0	2601523 0	66.757 0	2601529 5	137.361 5	2601535 9	1560.024 92.7
10000_5_5	2619168 28	5726.428 63.03	2619208 46.27	26414.639 278.4	2619335 5	2139.161 56.7	2619338 4	10443.43 270.8
1000_10_1	258363 15.6	14.848 54.9	258366 8.17	80.653 302.93	258297 55.4	0.433 76.3	258292 21.4	1.782 331.1
1000_10_2	260473 8.5	15.916 61.7	260475 5.5	72.851 288	260280 275.8	0.044 4	260455 217.7	0.193 40
1000_10_3	258921 17.8	15.081 55.97	258922 10.97	69.641 262	258904 49.5	0.488 81.1	258914 17.7	1.532 295.2
1000_10_4	255703 31.6	16.588 59.93	255696 15.27	77.615 285.3	255564 30.5	0.224 46.8	255686 83.1	1.198 270.8
1000_10_5	265175 30.2	15.081 649.47	265184 22.53	61.724 1835.87	265023 125.1	0.021 2	265132 69.4	0.033 3
5000_10_1	1311808 28	517.081 55.7	1311808 14.53	2865.905 312.9	1311739 57	12.586 63.8	1311738 33	34.544 316.2
5000_10_2	1311656 26	710.891 65.6	1311666 21.7	2947.104 276.6	1311703 46	13.563 42.9	1311701 25	32.528 232.7
5000_10_3	1287772 25	582.302 58.5	1287777 19.13	2848.431 292.3	1287800 122	4.376 14.4	1287798 45	25.507 179.6
5000_10_4	1298148 21	780.136 59.17	1298160 19.13	3590.579 274.13	1298198 55	13.906 55.4	1298206 23	90.309 349.5
5000_10_5	1303954 24	353.441 330.83	1303967 24.3	1676.855 1012.77	1303964 59	0.323 2	1303996 62	0.383 3
10000_10_1	2607178 0	125.391 0	2607178 0	127.033 0	2607293 13	794.163 62.9	2607305 11	3916.469 328.5
10000_10_2	2584132 0	85.966 0	2584132 0	87.271 0	2584176 35	110.651 4.8	2584200 48	291.331 11.5
10000_10_3	2587616 0	51.587 0	2587616 0	52.461 0	2587712 17	275.129 49.9	2587716 7	1505.956 294.8
10000_10_4	2601396 38	6129.751 66.4	2601398 21.63	27199.691 290.7	2601507 20	190.081 68.1	2601513 9	916.235 378.1
10000_10_5	2619260 32	5851.741 65.33	2619265 18.97	24789.69 273.9	2619326 18	451.893 71.8	2619327 7	1724.228 305.9

For strongly correlated instances having dissimilar capacities the results are as follows

- GQIEA_MKP(100) provides largest best value for 38 out of 45 instances.
- GQIEA_MKP(20) provides largest best value for 25 out of 45 instances.
- QIEA_MKP(100) provide largest best value in 13 instances
- while QIEA_MKP(20) provide only for 7 instances.
- However, Out of 45 instances for 7 instances all four algorithms provide same best value, for 6 instances only QIEA_MKP(100) provides largest best value, for 11 instances only two versions of GQIEA provide largest best value, for 2 instances only GQIEA_MKP(20) provides largest best value while for 19 instances only GQIEA_MKP(100) provides largest best value.
- Where all four types of instances provide same largest value, versions of GQIEAs are more consistent with better average values and significantly faster.
- In the instances for which both GQIEAs provide same best value, GQIEA_MKP(100) provides better average value or takes less time on an average.
- In the instances for which GQIEA_MKP(20) provides largest best value, GQIEA_MKP(100) provides better average value.

An Improved Generalized Quantum-Inspired Evolutionary Algorithm for Multiple Knapsack Problem

Table 3. Comparison of results obtained for strongly correlated instances having similar capacities using QIEA-MKP and GQIEA-MKP with population sizes of 20 and 100. The values obtained using optimal values and heuristic are shown as reference. Best value and difference between best and average is shown for QIEAs. Time to reach best solution in seconds and Function Evaluations (FES) are given.

n_m_s	QIEA-MKP(20)		QIEA-MKP(100)		GQIEA-MKP(20)		GQIEA-MKP(100)	
	Best (Best-Avg)	Time sec (FES)	Best (Best-Avg)	Time sec (FES)	Best (Best-Avg)	Time sec (FES)	Best (Best-Avg)	Time sec (FES)
1000_2_1	2583840.93	0.4993.3	2583840.87	5.24842.6	2583840	1.66925.2	2583840	7.1311105
1000_2_2	2604851.11	5.30345	26048518.4	22.298184.77	2604850	1.64625.1	2604850	7.2531106.2
1000_2_3	2589400	0.0870	2589421.8	4.50237.87	2589420	0.1712	2589420	0.17312
1000_2_4	2557166.67	6.009151.33	255726110.3	30.5021256.83	2557260	0.1864.3	2557260	0.194.3
1000_2_5	2652249.1	6.311152.73	26522518.7	22.696185.63	2652250	3.083151.6	2652250	6.9351140.6
5000_2_1	1311764110.3	236.73123.63	13117648.13	1679.7771163	13118545.2	284.461599.5	13118540	1782.7581262.3
5000_2_2	13117030	1.1250	13117030	1.130	13117390	245.13928.9	13117390	910.884109.9
5000_2_3	12878210	7.3170	12878210	7.3330	12878210	6.3610	12878210	6.3760
5000_2_4	12982300	8.2630	12982300	8.280	12982300	7.3070	12982300	7.3240
5000_2_5	13158560	1.0350	13158560	1.0390	13158560	0.050	13158560	0.060
10000_2_1	26072810	4.650	26072810	4.6550	26072956.8	3465.05152.6	26072952	16114.3881247.2
10000_2_2	25842050	4.1660	25842050	4.1890	25842050	0.1870	25842050	0.2120
10000_2_3	25876370	9.5090	25876370	9.6720	25877281	2140.47438	25877280	6873.6951115.8
10000_2_4	26015370	4.1630	26015370	4.2260	26015370	0.1890	26015370	0.2120
10000_2_5	26193380	4.1560	26193380	4.270	26193380	0.1870	26193380	0.2110
1000_5_1	2583844.3	8.451148.23	2583840.03	35.9971203.63	2583840	2.21328.3	2583840	8.313107.6
1000_5_2	2604854.4	8.98150.67	2604850.2	45.8821257.8	2604850	3.3640.3	2604850	10.1221119.4
1000_5_3	25894215.1	9.157152.63	25894210.9	49.5691283.9	2589421.5	4.218159.3	2589420	15.741219.6
1000_5_4	25572519.2	9.397152.23	25572619.67	26.3271145.1	25572615.2	2.20434.7	2557260	13.1311201.7
1000_5_5	26522518.1	7.55843	26522511.77	46.2251263.63	2652250	2.512133.9	2652250	9.0851121.4
5000_5_1	1311814111.07	669.911153.77	1311824110.57	2912.9241228.43	13118547	104.071112	13118541.6	1242.5161159.4
5000_5_2	13117290	10.6660	13117290	10.6990	13117390.9	416.223144.7	13117390	1048.5341115.2
5000_5_3	12878110	14.7750	12878110	14.810	128782114.1	281.31628.7	12878210.1	1776.9581176.5
5000_5_4	129819017.3	647.247152.23	129820018.67	29751236.83	12982302	292.907135.7	12982300	659.457174.7
5000_5_5	131582613.7	671.82154.57	1315836115.57	2960.6671236.7	13158464.9	384.526144.5	13158460	1559.4621181.8
10000_5_1	26072950	88.1680	26072950	88.8690	26073050	161.40711.6	26073050	161.60711.6
10000_5_2	25841940	40.2560	25841940	41.6230	25842056.3	4038.2151489.2	25842052.3	14592.941200.3
10000_5_3	25877240	64.1090	25877240	65.5480	25877280	984.901112	25877280	1045.213113.4
10000_5_4	26014487.1	1564.415117.1	2601457113.07	14911.2231159.73	26015270	697.854110.2	26015270	803.027111.2
10000_5_5	26193280	52.6110	26193280	54.1810	26193383	3126.132145.6	26193380	11391.5081163.8
1000_10_1	2583828.37	15.043153.1	25838418.2	54.2731192.77	2583841.7	4.58157.7	2583840.1	16.6241205.9
1000_10_2	260485110.97	17.905163.3	26048215.97	75.5121267.67	2604851	3.797165.1	2604850	14.9591241.7
1000_10_3	25893213.2	15.558155.13	25893210.03	60.4751215.3	25894212.3	4.4162.4	25894210.1	16.2311217.7
1000_10_4	25571617.93	15.818155.3	25571615.37	72.4631255.1	25572316.7	3.602169.5	2557160	12.9191237.7
1000_10_5	26522410	14.499151.67	26521913.93	57.0671204.53	26522513.3	4.5191173.8	2652250.5	16.5371229.9
5000_10_1	1311814114.7	890.522156.27	1311824117.7	3571.7981229.3	13118440	271.441134.2	13118546	2078.94111609.3
5000_10_2	13117100	14.5420	13117100	14.4340	13117390.3	359.14150.6	13117390	1133.5921156.9

continues on following page

Table 3. Continued

n_m_s	QIEA-MKP(20)		QIEA-MKP(100)		GQIEA-MKP(20)		GQIEA-MKP(100)	
	Best (Best-Avg)	Time sec (FES)	Best (Best-Avg)	Time sec (FES)	Best (Best-Avg)	Time sec (FES)	Best (Best-Avg)	Time sec (FES)
5000_10_3	128779121	897.482156.87	1287801121.37	3479.0351221.83	12878210	339.068147.4	12878210	825.371115.5
5000_10_4	1298190111.7	1027.679165.63	1298200115.03	3856.2341250.7	129823012.3	285.63147.5	12982300	1229.7781213.1
5000_10_5	1315816115.7	906.021156.87	131581618.67	4033.5641258.6	131585609	302.421135.6	131585608	1544.4151673.9
10000_10_1	260725610	71.15410	260725610	71.4410	2607305111.5	4001.6341188.4	260730516	12893.3231399.1
10000_10_2	2584125120.7	6884.654163.27	2584125111.33	29960.6231273.13	258420514.8	3588.6761171	258420512	16402.3871522.2
10000_10_3	2587658127.3	6785.086161.53	2587658121.43	28702.9741263.77	258771810	2886.294153.9	258772414.4	9550.7441173.2
10000_10_4	260150710	108.15610	260150710	107.10110	260152710	2082.553133.1	260152710	7356.1171109.8
10000_10_5	261931810	99.0410	261931810	98.67410	261933818.3	2217.3641142.83	261933813.3	13319.071693.9

For strongly correlated instances having similar capacities the results are as follows

- GQIEA_MKP(100) provides largest best value for 44 out of 45 instances.
- GQIEA_MKP(20) provides largest best value for 42 out of 45 instances.
- QIEA_MKP(100) provide largest best value in 17 instances
- while QIEA_MKP(20) provide only for 11 instances.
- However, Out of 45 instances for 11 instances all four algorithms provide same best value, for 6 instances QIEA_MKP(100), GQIEA_MKP(20) and GQIEA_MKP(100) provide same largest best value, for 25 instances only two versions of GQIEA provide largest best value, for 1 instance only GQIEA_MKP(20) provides largest best value while for 2 instances only GQIEA_MKP(100) provides largest best value.
- Where all four types of instances provide same largest value, versions of GQIEAs are more consistent with better average values and significantly faster.
- In the instances where both GQIEA_MKP(20) and GQIEA_MKP(100) provide same best value, for 22 instances GQIEA_MKP(100) provide better average value. But the time required by GQIEA_MKP(100) is typically more than GQIEA_MKP(20).

Table 4. Comparison of results obtained for uncorrelated instances having dissimilar capacities using QIEA-MKP and GQIEA-MKP with population sizes of 20 and 100. The values obtained using optimal values and heuristic are shown as reference. Best value and difference between best and average is shown for QIEAs. Time to reach best solution in seconds and Function Evaluations (FES) are given.

n_m_s	QIEA-MKP(20)		QIEA-MKP(100)		GQIEA-MKP(20)		GQIEA-MKP(100)	
	Best (Best-Avg)	Time sec (FES)	Best (Best-Avg)	Time sec (FES)	Best (Best-Avg)	Time sec (FES)	Best (Best-Avg)	Time sec (FES)
1000_2_1	39165612.8	0.2812.43	391675117.1	8.8721158.6	39167519.1	1.26211465.3	39167512.7	6.63219226.2
1000_2_2	40902219.4	3.865145.4	40902311.5	8.9391171.6	40901713.6	0.3461397.8	40901712.4	0.635198
1000_2_3	40643919.8	1.358117.4	40643915.9	8.0071184.57	40643817.8	0.4241906.3	40643913.6	4.08119130.9
1000_2_4	408580111.3	2.829133.3	40858012.1	11.9181257.73	40858010	0.241158.5	40858010	0.436179

continues on following page

An Improved Generalized Quantum-Inspired Evolutionary Algorithm for Multiple Knapsack Problem

Table 4. Continued

n_m_s	QIEA-MKP(20)		QIEA-MKP(100)		GQIEA-MKP(20)		GQIEA-MKP(100)	
	Best (Best-Avg)	Time sec (FES)	Best (Best-Avg)	Time sec (FES)	Best (Best-Avg)	Time sec (FES)	Best (Best-Avg)	Time sec (FES)
1000_2_5	4158556.4	1.78121.23	4158564.7	7.7331162	41585316.3	0.1691555.6	41586019.9	0.7031838.2
5000_2_1	200381215	28.149111.87	200382119	310.9761206.4	200382612	15.7651158.2	200382713	105.88913275.3
5000_2_2	204573710	1.74410	204573710	1.21110	204574614	4.4161233.5	204574610	5.934195.1
5000_2_3	201963310	1.27910	201964016	110.026172.47	201964011	6.905134.9	201964716	43.5612267.2
5000_2_4	203440010	0.98310	203440010	1.16310	203440010	0.06710	203440010	0.07910
5000_2_5	202598710	1.17610	202599114	52.449134.83	202601316	41.99811758.7	202601313	240.168112345.4
10000_2_1	404030110	3.9610	404030211	30.69413.73	404030513	131.69811520.2	404030513	415.4641327.7
10000_2_2	406722410	4.77810	406722410	6.68610	406722913	138.03811745.3	406723011	458.54715723.9
10000_2_3	403791110	4.21910	403791110	4.25210	403791510	81.58511151.8	403791510	144.65511010.6
10000_2_4	405470410	5.03610	405470410	4.11210	405470612	7.007114.3	405470610	754.76316359.3
10000_2_5	402993310	6.3410	402993310	4.20210	402993612	112.16811868.3	402993512	135.27812398.1
1000_5_1	39164918.9	3.207118.57	39165917.2	25.6081278.7	391661120.5	0.326170	39166418.5	1.5941336.8
1000_5_2	409016119.1	3.073117.43	40901119.7	13.671146.77	409013115.6	0.03717.5	409013113	0.7731193.9
1000_5_3	406425119.6	8.74153.77	40642518.6	19.4241218.87	406420131.8	0.2041136.7	406421120.1	1.58411336.8
1000_5_4	40855311	0.30710.87	408580126.1	2.762128.93	40856417.2	0.051112.8	40856411.2	0.9441231.1
1000_5_5	41583510	0.15510	41584316.8	5.453159.93	41583510	0.00510	41583711.8	0.086118.5
5000_5_1	200380510	2.91310	200380510	2.27510	200382115	7.304152.3	200382516	50.7091341.1
5000_5_2	204572510	2.3210	204572510	2.31310	204573717	3.978131.5	204573713	30.3561244.3
5000_5_3	201963010	2.17810	201963010	2.1710	201963313	1.22916.2	201963010	0.19210
5000_5_4	203438710	2.14210	203438811	25.208110.63	203438710	0.11410	203438710	0.14410
5000_5_5	2025977114	30.312110.37	2025979114	223.411182.87	2026001111	13.04149.9	202600016	86.0261317.9
10000_5_1	404026310	10.14710	4040274110	520.58143.07	404030118	68.847140	404030212	566.8731323.6
10000_5_2	406721110	10.54210	406721110	9.52810	406722115	50.505140.9	406722414	287.3641241.6
10000_5_3	403788610	8.56310	403789619	355.441140.6	403790313	59.19411954.2	403790713	185.64116010.6
10000_5_4	405469510	8.65910	405469510	8.65610	405469510	0.53710	405470317	56.0812199.4
10000_5_5	402992710	10.29610	402992710	9.25210	402993114	8.48315.8	402993313	141.3891111.6
1000_10_1	409556124	15.534152.83	409563115.7	52.8661288.37	40945210	0.01210	409484124.6	0.257171.6
1000_10_2	401691141.3	13.203145.17	401692121.9	41.3321226.4	401641122.4	0.083117.1	401636113.4	1.0251232.3
1000_10_3	406408120.7	10.877138.37	406410111.9	29.0281164.37	40636010	0.0110	40636010	0.02310
1000_10_4	40361710	0.27410	40361710	0.17510	40361710	0.0110	40361710	0.02210
1000_10_5	406064124.1	13.141146.77	40605616	38.721220.23	40598310	0.00710	40599016.3	0.01910.2
5000_10_1	202487910	7.29610	202488112	39.34817.4	202487910	0.39210	202488314	2.389122
5000_10_2	204569711	8.59210.67	2045713116	129.461126.8	204569610	0.28210	204569812	4.361133.9
5000_10_3	201960710	4.4310	201961416	197.319142.4	201960710	0.25510	201960710	0.31710
5000_10_4	203438318	66.036113.37	203438718	1097.0981249.23	203437310	0.13810	203437310	0.20110
5000_10_5	202596614	8.04410.7	2025985122	50.36719.57	202596210	0.46910	2025977112	26.8981179.8
10000_10_1	404025310	19.93810	404025411	19.96810	404026616	36.842144.6	404026914	227.8581279.8
10000_10_2	406718710	18.61810	406718811	189.68118.8	4067205112	24.698152	4067211111	142.3841311.3
10000_10_3	406112910	17.7810	406112910	17.38610	406112910	0.83210	406112910	1.110
10000_10_4	403559210	17.8910	403559210	17.49510	403559210	0.9810	403559210	1.26410
10000_10_5	402991410	18.30310	402991410	17.84410	402991410	1.38210	402991410	1.65110

An Improved Generalized Quantum-Inspired Evolutionary Algorithm for Multiple Knapsack Problem

For uncorrelated instances having dissimilar capacities the results are as follows

- GQIEA_MKP(100) provides largest best value for 30 out of 45 instances.
- GQIEA_MKP(20) provides largest best value for 14 out of 45 instances.
- QIEA_MKP(100) provide largest best value in 19 instances
- while QIEA_MKP(20) provide only for 9 instances.
- However, Out of 45 instances
 - for 5 instances all four algorithms provide same best value,
 - for 1 instance QIEA_MKP(100), GQIEA_MKP(20) and GQIEA_MKP(100) provide same largest best value,
 - for 2 instance QIEA_MKP(20), QIEA_MKP(100) and GQIEA_MKP(100) provide same largest best value,
 - for 7 instances only GQIEA_MKP(20) and GQIEA_MKP(100) provide largest best value,
 - for 1 instance only QIEA_MKP(20) provide largest best value,
 - for 10 instance only QIEA_MKP(100) provide largest best value,
 - for 3 instances only GQIEA_MKP(20) provides largest best value
 - while for 16 instances only GQIEA_MKP(100) provides largest best value.
- Where all four types of instances provide same largest value, versions of GQIEAs are more consistent with better average values and significantly faster.
- The instances where both GQIEA_MKP(20) and GQIEA_MKP(100) provide same best value, for 22 instances GQIEA_MKP(100) provide better average value. But the time required by GQIEA_MKP(100) is typically more than GQIEA_MKP(20).

Table 5. Comparison of results obtained for uncorrelated instances having similar capacities using QIEA-MKP and GQIEA-MKP with population sizes of 20 and 100. The values obtained using optimal values and heuristic are shown as reference. Best value and difference between best and average is shown for QIEAs. Time to reach best solution in seconds and Function Evaluations (FES) are given.

n_m_s	QIEA-MKP(20)		QIEA-MKP(100)		GQIEA-MKP(20)		GQIEA-MKP(100)	
	Best (Best-Avg)	Time sec (FES)	Best (Best-Avg)	Time sec (FES)	Best (Best-Avg)	Time sec (FES)	Best (Best-Avg)	Time sec (FES)
1000_2_1	39166117.2	0.47618.8	39166317.13	4.9361102.5	391675 16.7	1.20711677	391675 11.3	5.4949285.2
1000_2_2	40901019.83	2.512145.13	409022111.3	12.981246.3	40902217.8	0.9341664.5	409023 3.4	3.76911117.2
1000_2_3	40642218.17	0.4819	40642419.37	4.399193.03	406439 16.7	1.11411904.7	406439 3.1	5.11417475.4
1000_2_4	408580 14.8	0.22913.83	408580 13.9	2.202146.03	408580 0.9	0.96211673.5	408580 0	3.32413341
1000_2_5	415850112.7	1.017119.7	41584715.73	9.3521195.17	415856111.5	0.83111524.3	415860 5	2.96412907.3
5000_2_1	200382110	1.25610	200382110	1.22410	200382110	0.33910	2003825 3.6	34.87211799.2
5000_2_2	204573710	1.14710	204574113.87	13.63619.23	2045746 3.3	35.4412231.8	2045746 0.6	178.761111601.7
5000_2_3	201963010	1.03810	201963010	1.01110	201964211.9	41.62611549.9	2019647 14.6	195.26916047.4
5000_2_4	203438710	1.11610	203438710	1.08110	2034402 3.7	36.69112276.6	20344000.3	180.495111105.4
5000_2_5	202598911.93	4.85312.6	202599517.37	38.198126.07	2026014 5.6	51.02912533.5	2026014 3.1	278.746118965.5
10000_2_1	404030110	4.02610	404030110	3.91310	404030512.8	83.0041740.1	4040309 11.1	1411.442116011.1
10000_2_2	406722110	4.810	406722110	4.65910	4067230 1.8	193.0912398.2	4067230 11.1	829.24218990.8

continues on following page

An Improved Generalized Quantum-Inspired Evolutionary Algorithm for Multiple Knapsack Problem

Table 4. Continued

n_m_s	QIEA-MKP(20)		QIEA-MKP(100)		GQIEA-MKP(20)		GQIEA-MKP(100)	
	Best (Best-Avg)	Time sec (FES)	Best (Best-Avg)	Time sec (FES)	Best (Best-Avg)	Time sec (FES)	Best (Best-Avg)	Time sec (FES)
10000_2_3	40379060	5.3120	40379060	5.1450	403791511.6	217.68111763.6	40379160.9	1270.973112146.7
10000_2_4	40547000	4.9350	40547000	4.7790	40547093.3	206.1262381.7	40547101	994.818114873.8
10000_2_5	40299150	4.3150	40299150	4.2030	402993512.2	267.2152377.1	40299351.1	1106.81216426
1000_5_1	391632124.4	1.18911.73	391639125.77	18.3151199.37	391643117.2	0.27626.1	391653115.5	1.3211129.6
1000_5_2	408978133.33	5.554154.8	408979120.13	27.3631281.57	409000151.5	1.09611405.4	40899025.8	7.39117024.2
1000_5_3	406379114.5	0.33612.67	406389120.4	13.9031152.2	406381115.3	0.1741298.8	406403127.7	4.98319641.4
1000_5_4	408516124.3	3.084131.23	408533121.83	28.011299.67	408543125.7	0.255124.8	408564125	2.64312632.6
1000_5_5	4158230	0.0890	4158240.97	0.42713.7	4158230	0.0080	415843116.7	0.01412.9
5000_5_1	20038050	2.3530	20038050	2.2970	20038050	0.3460	20038050	0.3740
5000_5_2	20457140	2.1940	20457140	2.1410	2045735116.4	7.8931187.5	204573611	67.9291170.9
5000_5_3	201961610	19.06916.67	201961910.53	350.5671140.73	2019623112.9	14.0071631	201962516.5	140.69812108.7
5000_5_4	20343660	2.2940	203436811.87	16.30815.77	203437215.2	7.7011280.1	2034387117	134.33914952.6
5000_5_5	202597017.2	21.87617.17	2025978114.63	140.097152.1	2025984116	16.235130.6	202598319.3	117.9581220.3
10000_5_1	40402880	9.4810	40402880	9.2180	404029516.3	2.84110.7	404029515.9	208.45611267.3
10000_5_2	40672060	9.3440	40672060	9.1010	40672060	1.2240	406720912.7	28.326112.7
10000_5_3	403791110	9.4830	403791110	9.2210	403791110	1.3560	403791110	1.4160
10000_5_4	40546890	9.4030	40546890	9.2020	40546916.1	30.143113.8	405469212.6	114.524153
10000_5_5	40299200	10.1150	40299200	9.9460	402992211.8	1.9190	40299200	1.9770
1000_10_1	3915260	0.1760	391550121.9	10.954161.13	391596150.7	0.31130.1	391598127.8	2.3151478.3
1000_10_2	4088760	0.1810	408897120.1	2.163110.67	408922129.2	0.4071177.1	408935126.5	3.0191279.3
1000_10_3	406270113.53	0.76913.17	406277118.2	17.718197.2	406351162	1.1111133.3	406346131	4.70716120.6
1000_10_4	4084410	0.1810	4084410	0.1760	408481122.3	0.198119.6	408504125.2	3.68413892.3
1000_10_5	415733126	0.1790	415771158.9	6132.27	415816160.8	0.6551622.3	415789120.7	2.2941439.2
5000_10_1	20037720	4.5970	20037720	4.4460	20037720	0.4240	2003787112.3	45.888194.8
5000_10_2	2045662132.8	157.481130.67	2045663124.03	1367.0271282.53	2045693116.9	15.94412.5	2045701112.9	91.6451234
5000_10_3	20195760	4.5760	20195760	4.4270	201958013.6	0.3960	201958616.8	43.2321107.1
5000_10_4	20343330	4.5360	20343330	4.3860	2034367122.2	21.0021930.7	2034373122	76.4081238.8
5000_10_5	20259270	4.6910	2025949121.13	73.826114.37	2025980134.2	22.314181.6	2025980121.6	103.61312638.8
10000_10_1	40402630	18.9250	40402630	18.3090	404027315.5	84.604139.3	4040288115.8	501.6611238.6
10000_10_2	40671790	19.2130	40671790	18.580	406718313.6	8.18913.5	4067192110	212.00511738.4
10000_10_3	40378530	18.9320	403785511.9	284.767113.07	4037890114.1	100.294150.8	4037902113.3	5171268.3
10000_10_4	40546690	18.6080	40546690	18.1690	405468319.9	86.143147.3	405468513.9	633.41812627.2
10000_10_5	40298890	18.460	40298890	18.2980	4029916112.3	87.074139.8	402991411.3	298.1421138.2

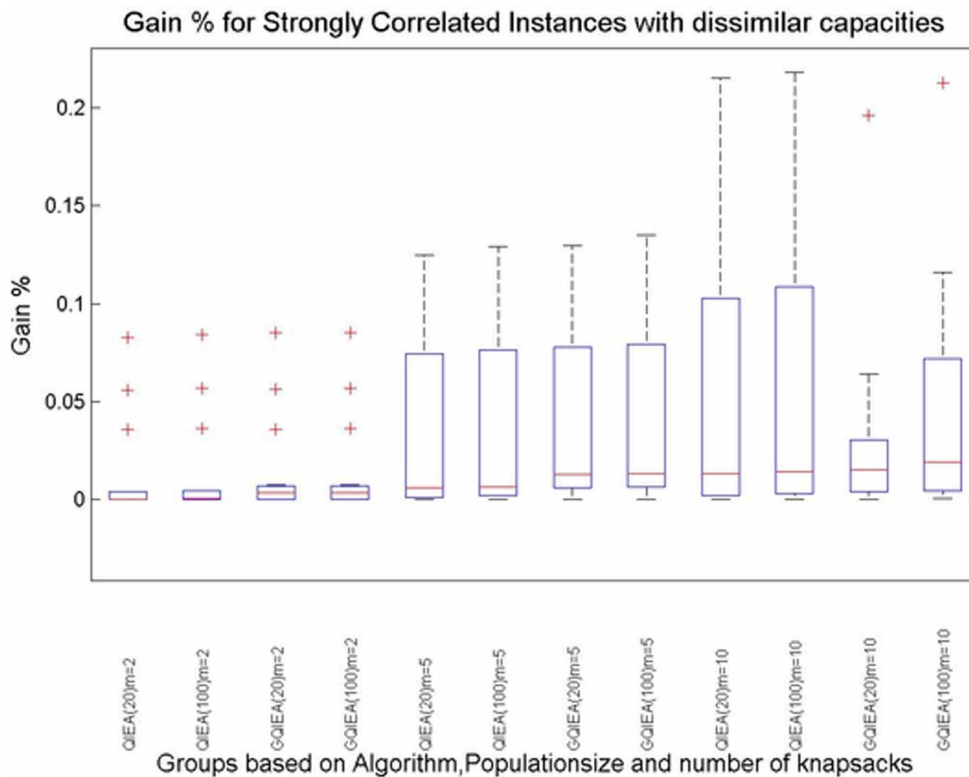
For uncorrelated instances having similar capacities the results are as follows

- GQIEA_MKP(100) provides largest best value for 38 out of 45 instances.
- GQIEA_MKP(20) provides largest best value for 18 out of 45 instances.
- QIEA_MKP(100) provide largest best value in 3 instances
- while QIEA_MKP(20) provide only for 3 instances.

- However, Out of 45 instances
 - for 3 instances all four algorithms provide same best value,
 - for 9 instances only GQIEA_MKP(20) and GQIEA_MKP(100) provide largest best value,
 - for 7 instance only QIEA_MKP(20) provide largest best value,
 - while for 26 instances only GQIEA_MKP(100) provides largest best value.
- Where all four types of instances provide same largest value, versions of GQIEAs are more consistent with better average values and significantly faster.
- The instances 12 instances where both GQIEA_MKP(20) and GQIEA_MKP(100) provide same best value, for 8 instances GQIEA_MKP(100) provide better average value. But the time required by GQIEA_MKP(100) is typically more than GQIEA_MKP(20).

Gain % in best solution and average solution obtained using applied approach over the values obtained from heuristic are calculated to elucidate the comparison. They are used to compare different algorithms using box plots in Figures 8 to 11 when instances grouped on the basis of same number of knapsacks and Figures 16 and 17 when instances are grouped on the basis of number of elements.

Figure 8. Boxplots for gain % in observed profit values over the heuristic values using different strategies and population size to solve Strongly Correlated Instances of MKP with dissimilar capacities grouped by number of knapsacks



An Improved Generalized Quantum-Inspired Evolutionary Algorithm for Multiple Knapsack Problem

Figure 9. Boxplots for gain % in observed profit values over the heuristic values using different strategies and population size to solve Uncorrelated Instances of MKP with dissimilar capacities grouped by number of knapsacks

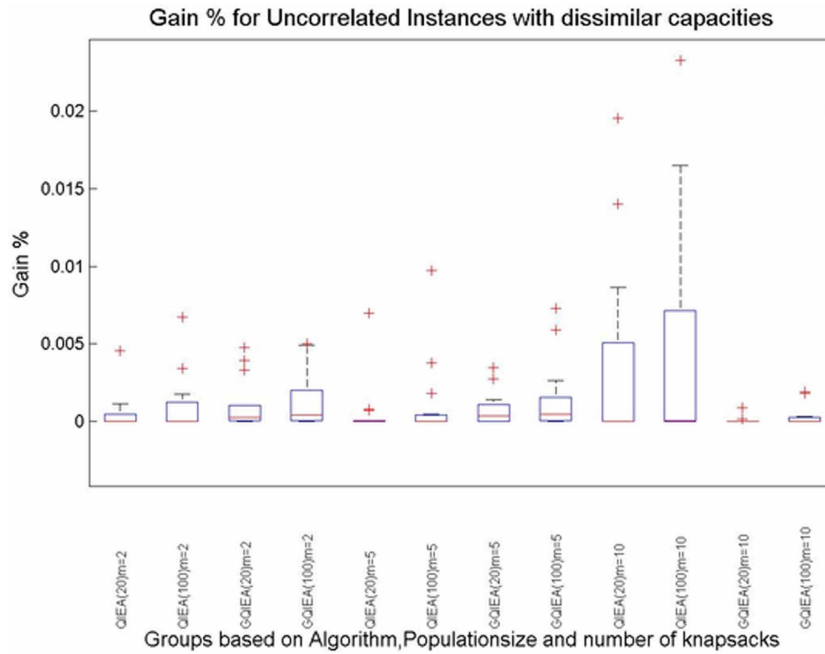


Figure 10. Boxplots for gain % in observed profit values over the heuristic values using different strategies and population size to solve Strongly correlated Instances of MKP with similar capacities grouped by number of knapsacks

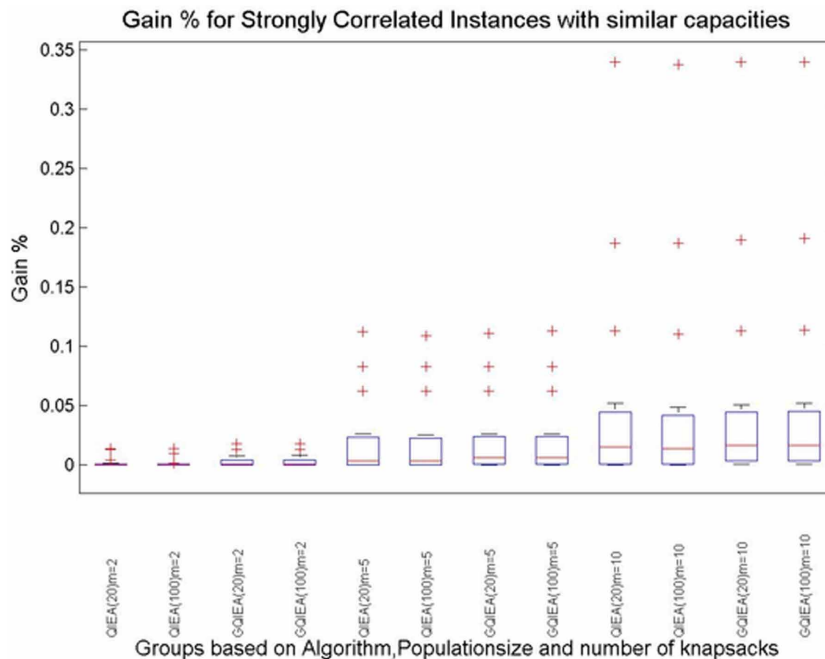


Figure 11. Boxplots for gain % in observed profit values over the heuristic values using different strategies and population size to solve Uncorrelated Instances of MKP with similar capacities grouped by number of knapsacks

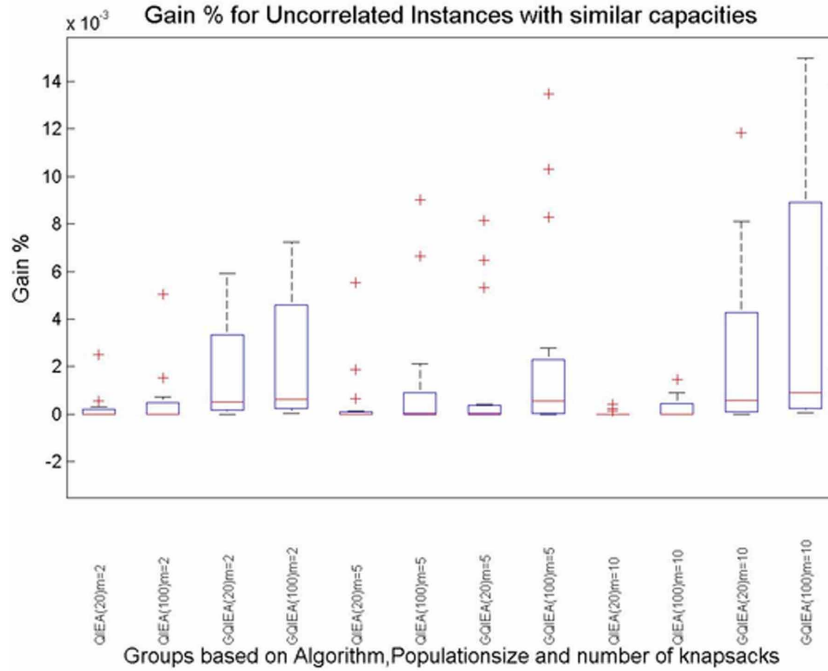
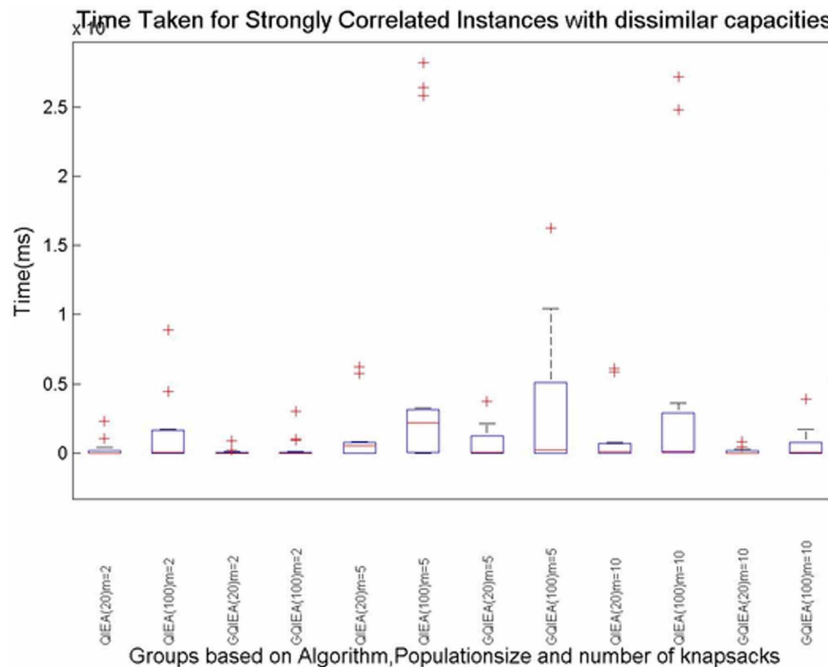


Figure 12. Boxplots for time taken using different strategies and population size to solve Strongly correlated Instances of MKP with dissimilar capacities grouped by number of knapsacks



An Improved Generalized Quantum-Inspired Evolutionary Algorithm for Multiple Knapsack Problem

Figure 13. Boxplots for time taken using different strategies and population size to solve Uncorrelated Instances of MKP with dissimilar capacities having grouped by number of knapsacks

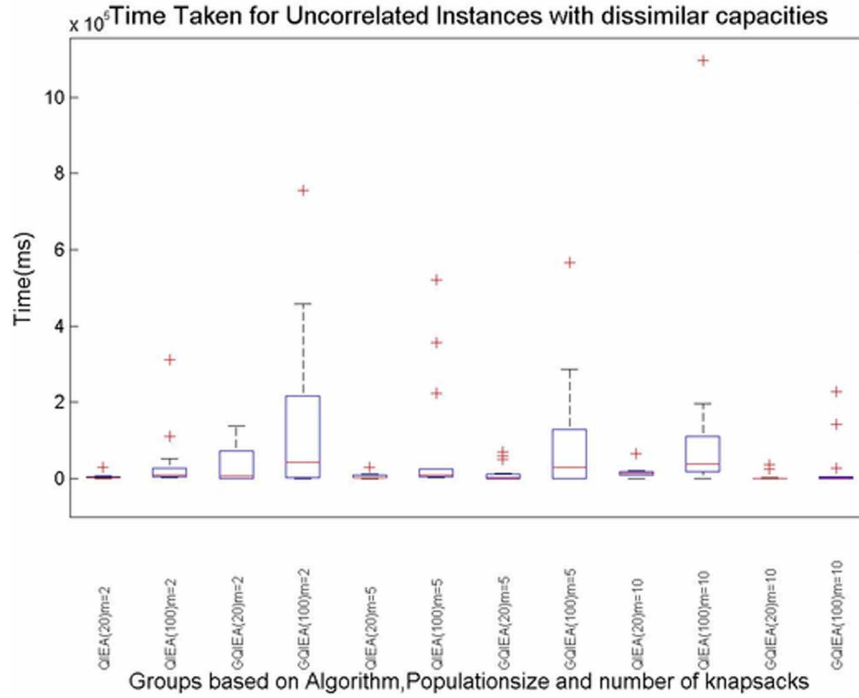


Figure 14. Boxplots for time taken using different strategies and population size to solve Strongly correlated Instances of MKP with similar capacities grouped by number of knapsacks

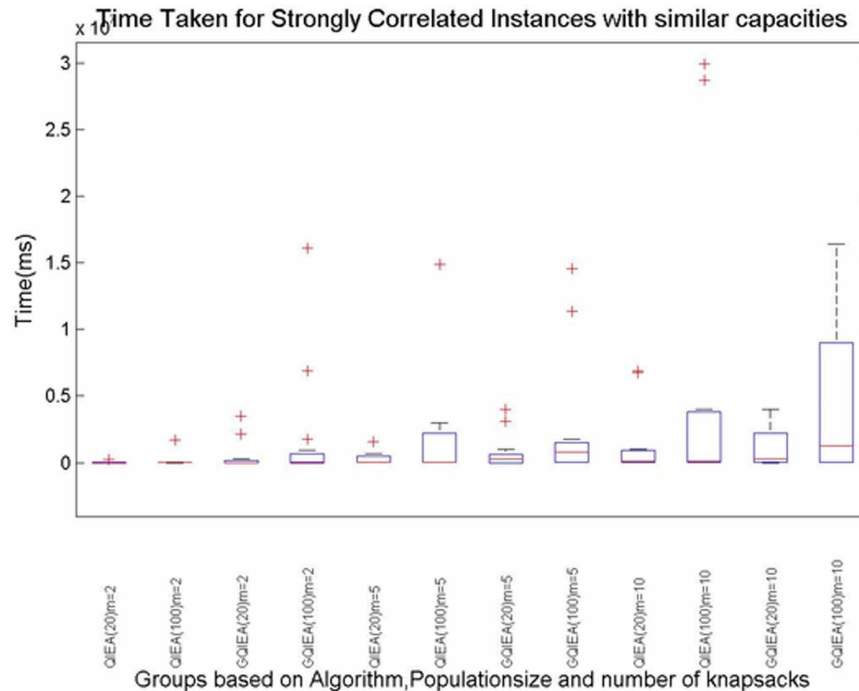


Figure 15. Boxplots for time taken using different strategies and population size to solve Uncorrelated Instances of MKP with similar capacities grouped by number of knapsacks

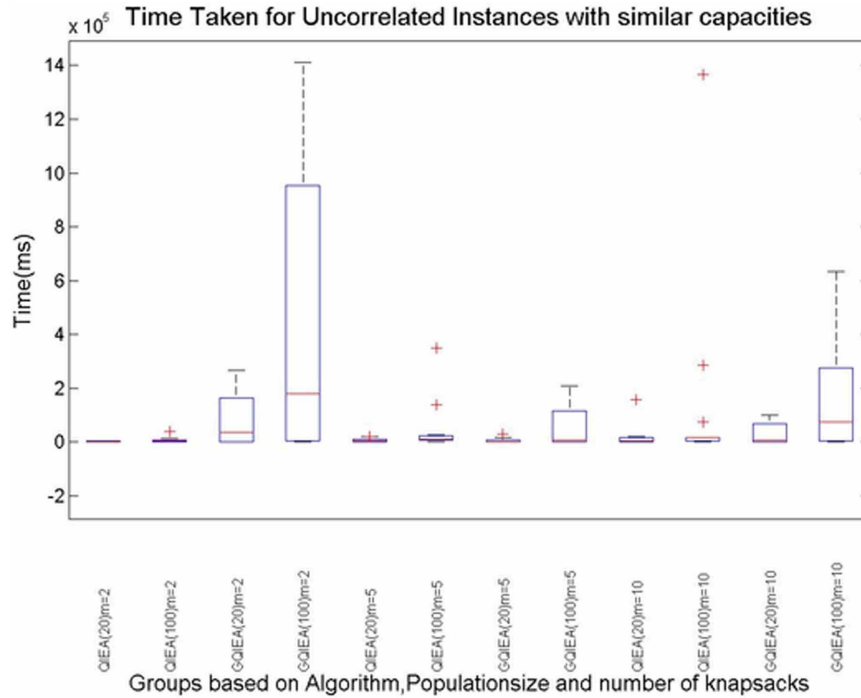


Figure 16. Boxplots for gain % in observed profit values over the heuristic values using different strategies and population size to solve Strongly Correlated Instances of MKP with dissimilar capacities grouped by size of problem

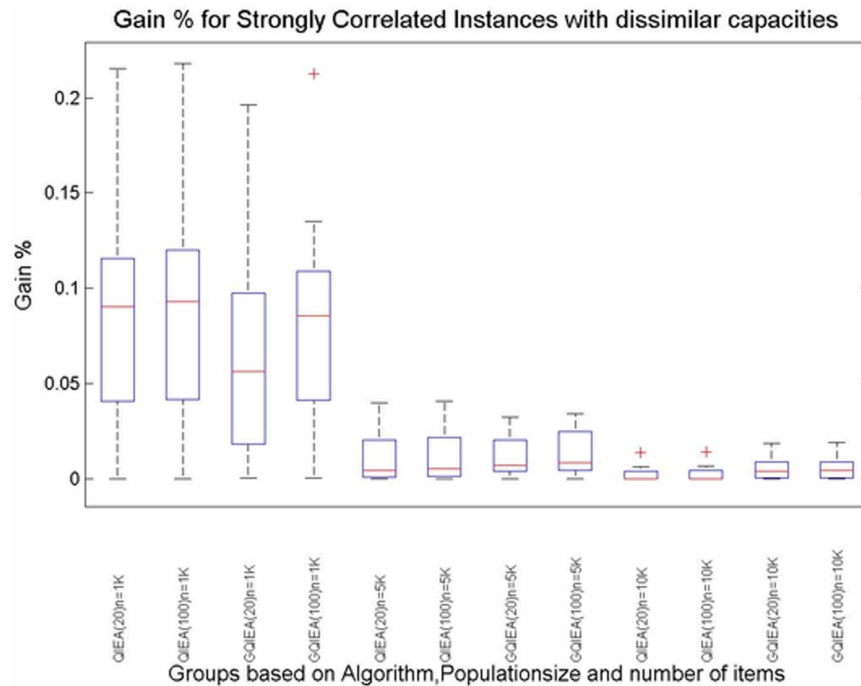
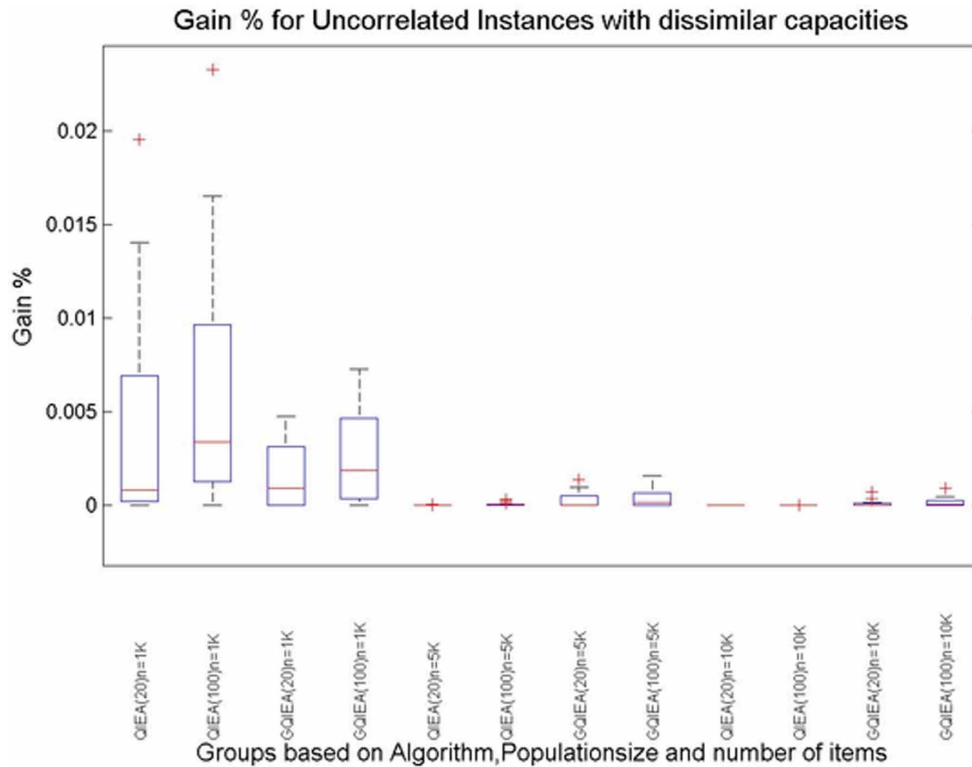


Figure 17. Boxplots for gain % in observed profit values over the heuristic values using different strategies and population size to solve Uncorrelated Instances of MKP with dissimilar capacities grouped by size of problem



The following observations are made from the results.

- Both forms of QIEAs viz. QIEA-MKP and GQIEA-MKP studied here to solve MKP with different number of variables and knapsacks shows considerable improvement in quality of solutions obtained as compared to the solutions provided by the popular heuristic, the MTHM.
- From Figures 8 to 15 it is clear that, GQIEA-MKP have shown a significant improvement in quality of solutions and also in time taken to find good solutions as compared to QIEA-MKP for the instances having number of knapsacks up to 5. In some instances the time taken to reach the best solution by GQIEA-MKP is larger than observed in case of QIEA-MKP. It is because in these cases QIEA-MKP could bring no improvement in the quality of the initialized solutions, so best solution is the initialized solution and no time has been taken to reach the best solution. (Based on experiments conducted it is observed that even after providing time to execute to QIEA-MKP much more than GQIEA-MKP, quality of solution is not improved in these cases).
- In case of instances having higher number of knapsacks (as 10), the one with similar capacities are solved in better way by GQIEA-MKP on an average as compared to QIEA-MKP while in case of dissimilar capacities QIEA-MKP provides better solutions than GQIEA-MKP. This observation is made in Figures 8 to 13. In these figures, the group-wise averages are considered such that all instances having different sizes but same number of knapsacks are grouped together.

- To illustrate another perspective for instances having dissimilar capacities, separate grouping is formed. All instances having same size but different number of knapsacks are grouped together. The separate box plots in Figure 16 and 17 have been drawn where the instances have been grouped in this way. It is observed that irrespective of what is the number of knapsacks, GQIEA-MKP performs better than QIEA-MKP for larger sizes. It is clear from these that GQIEA-MKP performs better as compared to QIEA-MKP as size of the problem increases. Similar graphs have not been shown for other classes of instances where also the performance of GQIEA-MKP improves over QIEA-MKP as size of problem increases.

5. CONCLUSION

The GQIEA-MKP has been designed based on generalized representation in QIEA to solve MKP effectively. Due to its effective representation for MKP, GQIEA-MKP has an edge over QIEA-MKP which uses the standard representation of Q-bits and operators. The proposed GQIEA-MKP is hybridized by influencing the initialization of generalized Q-bit individuals and the local search procedure based on a known effective heuristics for MKP with an objective to improve exploitation. Apart from it some techniques viz. mutation of solutions appearing to be close to local optima, and reinitializing Q-bit individuals found incapable to generate new solutions are also induced in order to improve the power to explore the search space. Hence, the balanced capability to exploit and explore the search space is established in proposed algorithm.

The hybridized versions of generalized QIEA (GQIEA-MKP) is studied in comparison to simple QIEA (QIEA-MKP) proposed earlier in (Patvardhan, Bansal, & Srivastav, Balanced quantum-inspired evolutionary algorithm for multiple knapsack problem, 2014) to solve Multiple Knapsack Problem (MKP). The GQIEA-MKP is shown to be better choice than QIEA-MKP to solve problems having non-binary integer solutions like MKP.

REFERENCES

- Alegria, J. M., & Tupac, Y. J. (2013). A Generalized Quantum-Inspired Evolutionary Algorithm for Combinatorial Optimization Problems. In *Proceedings of the XXXII International Conference of the Chilean Computer Science Society (SCCC)*, San Pablo.
- Arpaia, P., Maisto, D., & Manna, C. (2011). A Quantum-inspired Evolutionary Algorithm with a competitive variation operator for Multiple-Fault Diagnosis. *Applied Soft Computing*, 11(8), 4655–4666. doi:10.1016/j.asoc.2011.07.017
- Blum, C., Puchinger, J., Raidl, G. R., & Roli, A. (2011). Hybrid metaheuristics in combinatorial optimization: A survey. *Applied Soft Computing*, 11(6), 4135–4151. doi:10.1016/j.asoc.2011.02.032
- Chekuri, C., & Khanna, S. (2006). A PTAS for the multiple knapsack problem. *SIAM Journal on Computing*, 35, 713–728. doi:10.1137/S0097539700382820

An Improved Generalized Quantum-Inspired Evolutionary Algorithm for Multiple Knapsack Problem

- Diedrich, F., & Jansen, K. (2009). Improved approximation algorithms for scheduling with fixed jobs. In *Proceedings of the 20th ACM-SIAM Symposium on Discrete Algorithms (SODA2009)* (pp. 675-684). 10.1137/1.9781611973068.74
- Eilon, S., & Christofides, N. (1971). The loading problem. *Management Science*, 17(5), 259–268. doi:10.1287/mnsc.17.5.259
- Han, K.-H., & Kim, J.-H. (2002, December). Quantum-Inspired Evolutionary Algorithm for a Class of Combinatorial Optimization. *IEEE Transactions on Evolutionary Computation*, 6(6), 580–593. doi:10.1109/TEVC.2002.804320
- Kellerer, H. (1999). A polynomial time approximation scheme for the multiple knapsack problem. In *Proceedings of the 2nd Workshop on Approximation Algorithms for Combinatorial Optimization Problems, LNCS* (Vol. 1671, pp. 51-62). 10.1007/978-3-540-48413-4_6
- Kellerer, H., Pferschy, U., & Pisinger, D. (2004). *Knapsack Problems*. Berlin: Springer-Verlag. doi:10.1007/978-3-540-24777-7
- Mani, A., & Patvardhan, C. (2010). A Hybrid quantum evolutionary algorithm for solving engineering optimization problems. *International Journal of Hybrid Intelligent Systems*, 7(3), 225–235. doi:10.3233/HIS-2010-0115
- Martello, S., & Toth, P. (1980). Solution of the zero-one multiple knapsack problem. *European Journal of Operational Research*, 4(4), 276–283. doi:10.1016/0377-2217(80)90112-5
- Martello, S., & Toth, P. (1990). *Knapsack Problems: Algorithms and Computer Implementations*. Chichester, UK: Wiley.
- Patvardhan, C., Bansal, S., & Srivastav, A. (2014). Balanced quantum-inspired evolutionary algorithm for multiple knapsack problem. *International Journal of Intelligent Systems and Applications*, 11(11), 1–11. doi:10.5815/ijisa.2014.11.01
- Patvardhan, C., Narayan, A., & Srivastav, A. (2007). Enhanced Quantum Evolutionary Algorithms for Difficult Knapsack Problems. In *PREMI'07 Proceedings of the 2nd international conference on Pattern recognition and machine intelligence* (pp. 252-260). Springer-Verlag Berlin.
- Patvardhan, C., Prakash, P., & Srivastav, A. (2012). A novel quantum-inspired evolutionary algorithm for the quadratic knapsack problem. *Int. J. Mathematics in Operational Research*, 4(2), 114–127. doi:10.1504/IJMOR.2012.046373
- Pisinger, D. (1999, May). An exact algorithm for large multiple knapsack problems. *European Journal of Operational Research*, 114(3), 528–541. doi:10.1016/S0377-2217(98)00120-9
- Pisinger, D. (n.d.). *David Pisinger's optimization codes*. Retrieved November 2, 2012, from <http://www.diku.dk/~pisinger/codes.html>
- Platel, M. D., Schliebs, S., & Kasabov, N. (2007). A versatile quantum-inspired evolutionary algorithm. In *Proc. of CEC* (pp. 423-430).

An Improved Generalized Quantum-Inspired Evolutionary Algorithm for Multiple Knapsack Problem

Sailesh Babu, G. S., Bhagwan Das, D., & Patvardhan, C. (2008). Real-Parameter quantum evolutionary algorithm for economic load dispatch. *IET Generation, Transmission & Distribution*, 2(1), 22–31. doi:10.1049/iet-gtd:20060495

Wang, L., & Li, L. (2010). An effective hybrid quantum-inspired evolutionary algorithm for parameter estimation of chaotic systems. *Expert Systems with Applications*, 37(2), 1279–1285. doi:10.1016/j.eswa.2009.06.013

Xiao, J., Yan, Y., Zhang, J., & Tang, Y. (2010). A quantum-inspired genetic algorithm for k-means clustering. *Expert Systems with Applications*, 37(7), 4966–4973. doi:10.1016/j.eswa.2009.12.017

Yang, S., Wang, M., & Jiao, L. (2004). A novel quantum evolutionary algorithm and its application. In *Proc of CEC* (pp. 820-826).

Yang, S., Wang, M., & Jiao, L. (2010). Quantum-inspired immune clone algorithm and multiscale Bandelet based image representation. *Pattern Recognition Letters*, 31(13), 1894–1902. doi:10.1016/j.patrec.2009.12.016

This research was previously published in the International Journal of Applied Evolutionary Computation (IJAE), 9(1); pages 17-51, copyright year 2018 by IGI Publishing (an imprint of IGI Global).

Chapter 3

A Generalized Parallel Quantum Inspired Evolutionary Algorithm Framework for Hard Subset Selection Problems: A GPQIEA for Subset Selection

Sulabh Bansal

School of Computing and Information Technology, Manipal University Jaipur, Jaipur, India

C. Patvardhan

Department of Electrical Engineering, Dayalbagh Educational Institute, Agra, India

ABSTRACT

Quantum-inspired evolutionary algorithms (QIEAs) like all evolutionary algorithms (EAs) perform well on many problems but cannot perform equally better than random for all problems due to the No Free Lunch theorem. However, a framework providing near-optimal solutions on reasonably hard instances of a large variety of problems is feasible. It has an effective general strategy for easy incorporation of domain information along with effective control on the randomness in the search process to balance the exploration and exploitation. Moreover, its effective parallel implementation is desired in the current age. Such a Generalized Parallel QIEA framework designed for the solution of Subset Selection Problems is presented here. The computational performance results demonstrate its effectiveness in the solution of different large-sized hard SSPs like the Difficult Knapsack Problem, the Quadratic Knapsack Problem and the Multiple Knapsack problem. This is the first such a generalized framework and is a major step towards creating an adaptive search framework for combinatorial optimization problems.

DOI: 10.4018/978-1-7998-8593-1.ch003

1. INTRODUCTION

Evolutionary Algorithms (EAs) are popular population- based meta-heuristic techniques inspired from the natural process of evolution which have been used with advantage in a large variety of applications (Goldberg, 1989; Mitchell, 1996; Bäck, Fogel, & Michalewicz, 1997a; Bäck, Hammel, & Schwefel, 1997b; Zhou, et al., 2011). However, slow convergence remains a huge problem especially for large problem instances. Quantum computers use quantum bits (qubits) as the smallest unit of information (Hey, 1999). Quantum Inspired Evolutionary Algorithms (QIEAs) (Quantum-Inspired Evolutionary Algorithm for a Class of Combinatorial Optimization, 2002) form a subclass of EAs. These exploit the advantages of quantum representation, superposition of states and operators to mitigate some of the limitations in EAs for better search and optimization (Zhang G., 2011). A variety of QIEAs, shown to be effective for search and optimization problems, have been developed. Conceptual comparison between EAs and QIEAs is summarized in Table 1.

Table 1. Comparison between EAs and QIEAs

	Similarities	Differences
1.	Both EAs and QIEAs work with individuals and population(s)	EA represents solutions as individuals specifying parameter values of problem being solved. QIEA utilizes Q-bit strings. A Q-bit string is a superposition of all possible solutions. Thus, individuals in EAs are particular solutions in search space while the individuals in QIEAs are probabilistic representations of the search space.
2.	Both EAs and QIEAs use operators to update individuals	Reproduction operators in EAs are applied directly on solutions while in QIEAs operators are applied on the Q-bit strings.
3.	Both evaluate solutions to measure their fitness.	In EAs a set of good solutions are selected to be used as parents for producing better children in future generations. While in QIEAs, a few good solutions are selected, these may then be used to update Q-bit strings so that solutions closer to the best solutions found are generated in subsequent iterations.
4.	Both generate new solutions in each iteration	In EAs, solutions are generated through reproductive operations on existing solutions while in QIEAs solutions are generated through observation on updated Q-bit individuals.

Although QIEAs are inspired from quantum computing, they are not meant for quantum computers. QIEA is another evolutionary algorithm for a classical computer. The basic building blocks of a typical QIEA are explained as follows:

1. **Representation:** A Q-bit is the smallest unit of information in a QIEA. A Q-bit individual is a string of Q-bits. A Q-bit is denoted as $\begin{bmatrix} \alpha_i \\ \beta_i \end{bmatrix}$, where α_i and β_i are complex numbers symbolizing its probabilistic states. Such that $|\alpha_i|^2$ and $|\beta_i|^2$ represent the probability of state being 0 and 1 respectively, and following condition is satisfied:

$$|\alpha_i|^2 + |\beta_i|^2 = 1 \tag{1}$$

Thus, a Q-bit string of length n represents a superposition of 2^n binary states and provides an extremely compact representation of entire space. Typical implementations of QIEA, represent α_i and β_i as real numbers for the sake of simplicity and without loss of generality.

2. **Observation and Fitness computation:** In QIEAs, solutions are generated using a Q-bit string, say Q , using a process called observation described as follows.

For problems having binary solutions of length n , the Q-bits of Q (say Q_i , $i \in \{1, \dots, n\}$) are observed and a binary string, P (consisting bits P_i , $i \in \{1, \dots, n\}$), representing the solution(s) of the problem under consideration is(are) generated as follows. $P_i \forall i \in \{1, \dots, n\}$, is initialized to zero. For each Q_i , $i \in \{1, \dots, n\}$, a random number, say r , between 0 and 1 is generated. P_i is set to one if r is less than $(\alpha_i)^2$ otherwise it is set to zero.

3. **Evolution Operator:** For evolution, in QIEAs the Q-bit individuals are modified in each step so to increase the probability of generating solutions closer to found good solutions. So, the Q-bits gradually converge to values close to 0 or 1, when they generate same solution upon every observation with very high probability. This solution is likely to be the (near) optimal solution given enough computation.

A popularly used Q-gate is the rotation gate, which is defined as follows:

$$\begin{bmatrix} \alpha_i^{t+1} \\ \beta_i^{t+1} \end{bmatrix} = \begin{bmatrix} \cos(\Delta\theta_i) & -\sin(\Delta\theta_i) \\ \sin(\Delta\theta_i) & \cos(\Delta\theta_i) \end{bmatrix} \begin{bmatrix} \alpha_i^t \\ \beta_i^t \end{bmatrix} \quad (2)$$

where, α_i^{t+1} and β_i^{t+1} denote values for i^{th} Q-bit in $(t + 1)^{\text{th}}$ iteration and $\Delta\theta_i$ is some small rotation angle whose value is picked from a predefined look-up table.

Several variations of Q-gate of Equation (2) have been presented in literature.

4. **Initialization:** Generally, the Q-bit individuals are initialized such that each state has equal probability of generation.

In a QIEA, a population of solutions is formed iteratively by observation as described above (either by observing a single Q-bit string several times or by observing several Q-bit strings). Based on the computed fitness values, the best solution is identified within formed population and called the global attractor. Further, the update step slightly alters the Q-bits in the string using the quantum gate such that in subsequent iterations the solutions more similar to the global attractor are generated with higher probability. This sequence of steps continues till termination criterion is satisfied. Multiple Q-bit strings can be handled in a similar fashion.

1.1. Strengths and Weaknesses of QIEAs

Search algorithms in general and EAs in particular form solutions by randomly choosing values of variables from the search space without estimating any probability distribution or without creating a

probabilistic model for the variables of the concerned problem. The algorithms that estimate the probability distribution by using selected set of solutions and further generate the solutions based on the estimate are called EDAs. Pelikan et al. (1999) discuss and classify EDAs based on the complexity of models used. QIEAs belongs to a class of Estimation of Distribution Algorithm (EDA) (Zhou & Sun, 2005; Han, 2006; Platel, Schliebs, & Kasabov, 2009; Zhang, 2011) which have most of the strengths of EAs. Being an EDA, QIEA propagates the search such that entire history of generated good solutions impacts the new solutions. A Q-bit string, which represents an estimation of distribution, is updated iteratively using a Q-gate taking feedback from generated good solutions. Thus, the update process provides appropriate direction during search.

The basic QIEA is a high-level procedure. Any attempted implementation, therefore, must be judiciously tailored to include features suited to the particular problem at hand in order to get the desired performance. Exploration refers to capability of a search algorithm to find solutions in disparate regions in search space. Exploitation refers to its capability to comprehensively search in a region around a particular good solution. The objective in any attempted implementation of QIEA is to balance exploration and exploitation thus achieving convergence to optimal or near optimal solution without requiring prohibitively large computation. This is referred to as “right-sizing the randomness” in the QIEA search. Primary strengths and weaknesses of QIEAs are listed in Table 2.

Table 2. Strengths and limitations of QIEAs

Strengths	Limitations
1. QIEAs have better representation power using Q-bits to enable use of smaller populations (ideally even a size of 1) (Han & Kim, 2003; Han K.-H., 2006). Smaller populations require lesser computation.	1. Slow convergence may result from use of small Q-bit rotations. Fast Q-bit rotations towards observed best solutions may cause the algorithm to miss a good solution completely.
2. QIEAs have an Estimation of Distribution Algorithms (EDA) style functioning with implicit determination of distributions leading to better solutions (Platel, Schliebs, & Kasabov, 2009; Zhang G., 2011).	2. Inclusion of features that promote faster convergence increases its tendency to get stuck in local optima.
3. QIEAs provide an extremely flexible framework that can be adapted for both real and parameter optimization as well as for the solution of COPs (Han, 2006; Zhang, 2011).	3. Slow convergence puts a limit on size of the problems that can be handled using QIEAs.
4. It is possible to include features appropriate for a given problem for delivering better search performance (Zhang G., 2011).	4. Implementation of QIEAs, just as other EAs, is more an art to enable balance of exploration and exploitation that is required for good search performance.
5. QIEA inherently favours exploration initially which shifts gradually towards exploitation as the search progresses. This is a desirable aspect (Han K.-H., 2006).	
6. There is a possibility of utilizing one of several termination criteria appropriate for the problem at hand (Han & Kim, 2004).	

1.2. A Brief Survey of Variations in QIEAs

QIEA implementations have to be crafted carefully to make them competitive with respect to the state-of-art algorithms for a particular problem. Many design alternatives are possible as QIEA is a loose framework. Some principles from EAs may be used for guiding particular implementations. However,

for most part, it is an art. Many variations of QIEAs exist in literature (Arpaia, Maisto, & Manna, 2011; Han, 2006; Imabeppu, Nakayama, & Ono, 2008; Han, Park, Lee, & Kim, 2001; Kim, Kim, & Han, 2006; Kliemann, Kliemann, Patvardhan, Sauerland, & Srivastav, 2013; Konar, Bhattacharya, Sharma, & Pradhan, 2017; Li, Zhang, Cheng, Jiang, & Zhao, 2005; Lu & Yu, 2013; Mahdabi, Jalili, & Abadi, 2008) (Mani & Patvardhan, 2010; Narayanan & Moore, 1996; Nowotniak & Kucharski, 2012; Patvardhan, Prakash, & Srivastav, 2012; Patvardhan, Narayan, & Srivastav, 2007; Platel, Schliebs, & Kasabov, A versatile quantum-inspired evolutionary algorithm, 2007; Qin, Zhang, Li, & Zhang, 2012; Sailesh Babu, Bhagwan Das, & Patvardhan, 2008; Tayarani-N & Akbarzadeh-T, 2008; Wang & Li, 2010) (Xiao, Yan, Zhang, & Tang, 2010; Yang, Wang, & Jiao, 2004a; Zhang & Rong, 2007; Zhang, Gheorghe, & Wu, 2008; Zhang, Li, Jin, & Hu, 2006; Zhang & Gao, 2007; Zhao, Peng, Peng, & Yu, 2006), each presenting some modifications in the basic QIEA (Han & Kim, 2002). Select QIEAs are discussed in Table 3 with improvements.

Table 3. A brief outline of modifications considered in existing QIEAs

	Modifications	Examples
1.	Modified initialization of Q-bit individuals in QIEA	Han and Kim (2004) propose a two-phase initialization of Q-bit strings in QIEA. Zhao et al. (Zhao, Peng, Peng, & Yu, 2006) propose three ways (viz., uniform, proportional and probabilistic seed) for initialization of Q-bit individuals.
2.	Modification in Termination Criteria	Han and Kim (2004) propose the convergence of Q-bits to be used in termination criteria.
3.	Modifications in Update procedure e.g. choice of attractor, different Q-gate, other learning strategies etc.	Han and Kim (2004) propose novel H_c gate to avoid local optima. H_c gate makes the probability of $ 1\rangle^{\alpha}$ $ 0\rangle^{1-\alpha}$ or $ 0\rangle^{\beta}$ $ 1\rangle^{1-\beta}$ converge to either $1-\epsilon$ or ϵ instead of 0 or 1. Zhang et al. (2010) present a comparison between six different Q-gates varying the method for calculating the values of θ . Platel et al. (2007) in their versatile QIEA (vQIEA) choose the attractor as the best solution in current generation rather than the overall best. Mahdabi et al. (2008) propose to update different Q-bits in an individual based on different attractor. Patvardhan et al. (2007; 2012) propose varying rotation angles in modified gates. Two gates are proposed such that one helps in exploration while other helps in exploitation of search space.
4.	Modifications in methods to deal with infeasible solutions	Han and Kim (2002) experimented using multiple types of penalty functions and repair procedures to deal with infeasible solutions. Zhao et al. (2006) use Q-bit values of elements as a criterion for removing elements from an infeasible solution to repair it.
5.	Modification of structure of QIEA	Platel et al. (2007) propose a structure having three layers as individual, group and global in vQIEA instead of two layers as in original QIEA. Imabeppu et al. (2008) use pair-swap method instead of migration. Mahdabi et al. (2008) use multi-measurement operator. Zhang et al. (2008) propose a membrane system-based structure in QIEA.
6.	Incorporation of genetic operator mutation	Patvardhan et al. (2012) mutate the obtained solutions, which may be chosen as an attractor.
7.	Re-initialization of Q-bits	Mahdabi et al. (2008) re-initialize the Q-bit individuals on convergence.
8.	Inclusion of domain knowledge in the search process	Patvardhan et al. (2007) sort the input items to solve Knapsack Problem (KP) instances in descending values of their profit by weight ratio. Zhao et al. (2006) propose a method where for KP the Q-bit values of items are initialized to values proportional to the profit/weight ratio. Konar et al. (2017) proposed Hybrid Quantum-Inspired Genetic Algorithm where the real-time tasks are sorted on the basis of their deadlines and computation times to use Earliest deadline First (EDF) and Shortest Computation First (SCTF) heuristics.
9.	Parallel implementation	Han et al. (2001) present a QIEA for multi-processor system. Nowotniak and Kucharski (2012) implemented a QIEA for General Purpose Graphical Processing Unit (GPGPU).

1.3. Need for Generalized Framework of QIEAs

According to the No Free Lunch theorem (Wolpert & Macready, 1997) any search algorithm like QIEA is only as good as random search when its performance is averaged over all problems. The QIEAs described in Table 3 are highly specialized in that they typically apply one or two modifications to the basic QIEA and show performance improvement on small sized instances of particular target problems. These two observations taken together motivate the design of a broader QIEA framework that is general enough to enable good results on a larger variety of complex problems by choosing the appropriate features to be brought into play. The success of the framework depends on ease of applying it to a given problem. The framework should also provide mechanisms for easy inclusion of domain knowledge where available that can be exploited to solve the problem effectively. It is well known that effective use of domain knowledge contributes immensely to effective solution of Combinatorial Optimization Problems (COPs). It should also take advantage of the multi and many core architectures available today.

A generalized QIEA framework based on the above considerations is described in this work for engineering the solution of more complex and larger problems than attempted hitherto. Several Subset Selection Problems (SSP) are solved to illustrate the utility of the proposed framework including Difficult Knapsack Problems (DKP), Quadratic Knapsack Problem (QKP) and Multiple Knapsack Problems (MKP).

The basic formulation of the optimal SSP is as follows. Let U denote some finite and discrete set of n items $\{x_1, x_2, \dots, x_n\}$, to be called the *universe*. Suppose X is a subset of U . F denotes an objective function of the form: $F: X \rightarrow \mathbb{R}$ and $G_1, G_2, G_3, \dots, G_k$ denote some constraints functions of the form $G_i: X \rightarrow \mathbb{R}$, where $i \in \{1, 2, \dots, k\}$ where \mathbb{R} is the set of real numbers and a subset X is said to be feasible if $G_i(X) \leq 0 \forall i=1, 2, \dots, k$. The optimal SSP is to find a subset X of U for which the given set of constraints is satisfied, and objective function has an optimal value (maximum or minimum). Assuming the goal is to maximize the value of F , the optimal SSP is to find a feasible subset X of U such that $F(X)$ is maximum. In mathematical notation it means, find X such that:

$$X \subseteq U \tag{3}$$

and:

$$G_i(X) \leq 0 \forall i=1, 2, \dots, k \tag{4}$$

such that:

$$F(X) \geq F(Y), \text{ for any } Y \subseteq U \tag{5}$$

The proposed framework is effectively utilized for faster solution of larger instances of listed SSPs to obtain optimal or near-optimal solutions in reasonable time. The results show that the framework can be used for a wide variety of COPs and provides an excellent tool for such problems. Such a generalized, rigorous and thorough study has been attempted for the first time.

The rest of the paper is organized as follows. The proposed framework is described in section 2. The implementation and the results of computational experiments are discussed in section 3. Conclusions are derived in section 4.

2. GENERALIZED PARALLEL QIEA (GPQIEA)

GPQIEA provides a variety of features which may be applied in judicious combination according to the requirements of a particular problem. Some of these features help in better exploitation of regions, while others increase the randomness so that disparate regions in the search space are explored. The structure of GPQIEA aids easier distribution of computing load on to different computation units if they are available.

In section 2.1, some methods for incorporating domain knowledge in a GPQIEA implementation are discussed. Other features that can be incorporated in GPQIEA are described in section 2.2.

2.1. Representation and Mechanisms to Incorporate Domain Knowledge

The known heuristics for an SSP provide a good initial solution. This is used in GPQIEA to compute priority of selecting an element in the solution. This priority is computed as a real number in the range $[0, 1]$ with 1 representing the highest priority and 0 the lowest. The methods for this are as follows:

- **A Priori Probabilities:** The items included in a heuristic solution may be assigned a higher priority of inclusion than those not included in the solution;
- **Multiple Solutions:** When multiple heuristic solutions are available for a problem, the count of the solutions where an element is included can be used to estimate its priority of inclusion with higher count resulting in higher priority of inclusion;
- **Sequential Approach of Forming a Solution:** Many heuristics and exact algorithms for SSPs build the solution in sequential manner. Starting with an empty solution, the components are added one by one into it. Otherwise, starting with all components in solution, they are removed one by one. At each step to add or remove a component a choice is made (out of many options) using a function defining its priority. The elements may be assigned decreasing (or increasing) priority of inclusion in the order they would be selected (or removed).

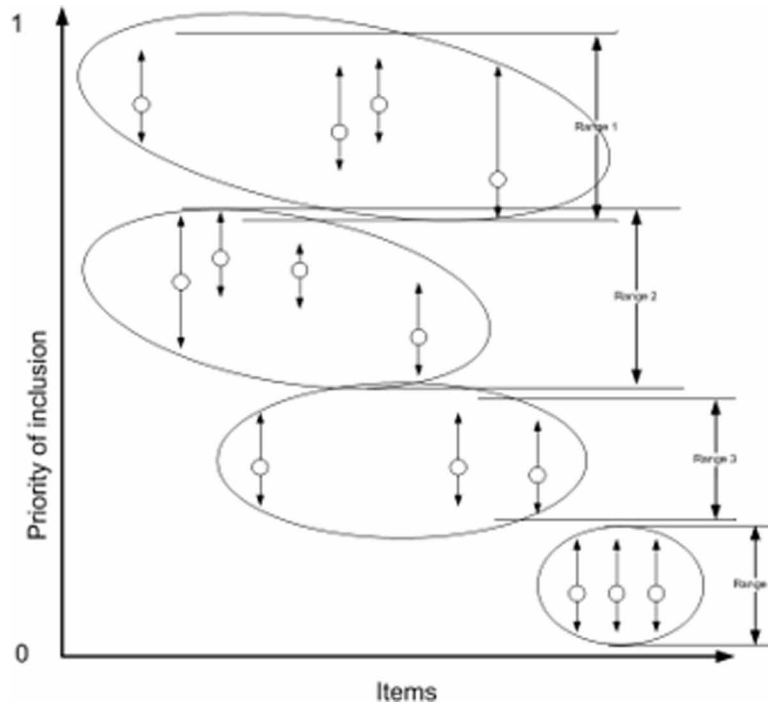
The utility of this priority assignment depends on the quality of the heuristic used. The priority order may be used to partition items into different sets, called *PriorityPockets*, based on the range of the priorities. The items may be assigned initial Q-bit values according to the *PriorityPockets* they belong to as shown in Figure 1. The initial Q-bit value of an item in GPQIEA represents the initial priority of selecting the item in the solution. The Q-bit values in descending order define a sequence of items called the *PrioritySequence*.

When there are multiple good heuristics for a problem multiple sets of *PriorityPockets*, and hence, *PrioritySequences* may be defined. Enhanced robustness and better performance are obtained by increasing the number of good and possibly diverse initial solutions in this manner. The added computational overhead due to forming *PriorityPockets* in multiple ways may be shared between multiple threads in a parallel implementation to reduce time.

Q-bit individuals in QIEAs, being EDAs, represent probability distributions. Hence, domain information represented in form of *PriorityPockets* or *PrioritySequences* is used in many ways to improve the GPQIEA:

- Initializing the Q-bit Individuals (section 2.2.2); and/or
- Re-initializing the Q-bit individuals (section 2.2.8); and/or
- Repairing the infeasible solutions obtained after collapsing the Q-bit individuals (section 2.2.5).

Figure 1. Partitioning items into PriorityPockets based on ranges of priorities of inclusion identified using domain knowledge



2.2. Features of GPQIEA

A list of features of GPQIEA is given in Table 4. The features F1 to F5 strengthen search using domain knowledge in a deterministic way in order to find good solutions in identified good regions. On the other hand, the features F6 to F9 add randomness to search process in order to increase diversity and improve exploration. A careful selection and incorporation of these features is required for an effective implementation of GPQIEA for a problem.

2.2.1. Initialization of the Best Solution (Global Attractor) Using a Heuristic (F1)

The global attractor (as explained in section 2.2.3) is initialized with a very small value (large value) in case of maximization (minimization) problem if no heuristic is available. When a good heuristic is available the global attractor is initialized with the solution obtained using it. This helps in guiding the search process towards good region of the search space early in the search process.

Table 4. List of distinguished features proposed in GPQIEA

Feature	Description
F1.	The global attractor initialized using known best heuristic
F2.	Q-Bit initialization based on <i>PriorityPockets</i> or <i>PrioritySequences</i> of input items
F3.	Modified Structure
F4.	Local Exploitation before exploration
F5.	Modified Repair based on heuristic
F6.	Local Search
F7.	Mutation
F8.	Re-initialization
F9.	StochasticPurge
F10.	Size Reduction
F11	Termination Criteria

2.2.2. Applications of Domain Knowledge to Initialize the Q-Bit Individuals (F2)

The Q-bit strings are initialized such that each solution has same probability of generation when no domain knowledge is available or is not being used. This implies that in the initial part of the search process the solutions are generated randomly and the search is guided by the best amongst those. This is a slow process of improvement towards getting to the optimal solution.

However, the Q-bits may be assigned different values initially, based on domain knowledge, to speed up convergence. This initialization essentially amounts to introducing bias towards selecting some items over the others.

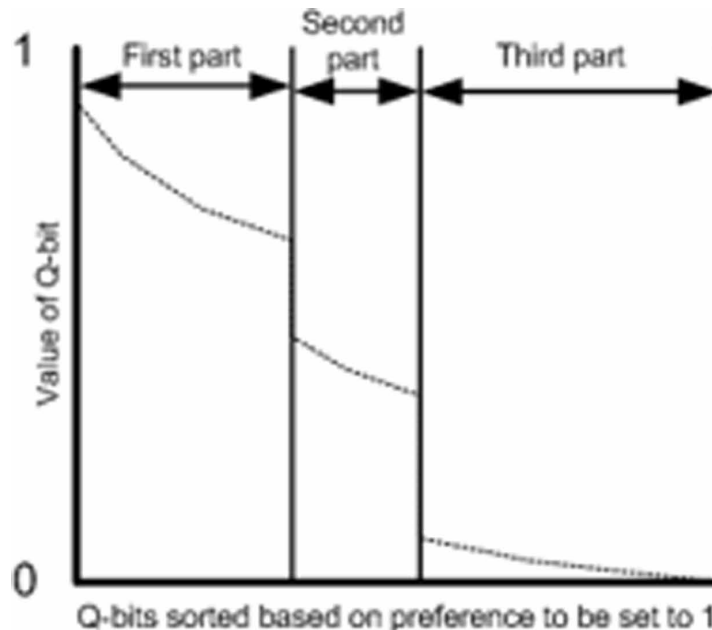
In GPQIEA, multiple ways for Q-bit individuals are available. The proposed methods are summarized in Table 5 with their perceived advantages and disadvantages.

The *PrioritySequences* may be used to initialize Q-bit individuals in a better way as shown in Figure 2. The elements are divided into three classes: the first class contains elements having high preference for attaining value 1, second part contains items having medium preference and third contains the items having low selection preference. Hence, Q-bits for items lying in the first class (third class) are assigned values closer to 1 (0) so that they have high (low) probability of collapsing to value 1(0). The first few in this sequence are almost definitely selected and the last few are almost definitely not selected. If the method used to find a *PrioritySequence* is good, this cuts down the size of search space considerably. Then Q-bits for items lying in second part are the one which primarily require more search for convergence and appropriate values between 0 and 1 are assigned to items lying in second part. Width of various segments in the sorted list can be adjusted based on the level of confidence about the correctness of the priorities assigned to items. More than one *PrioritySequence* may be formed based on different criteria to assign the biases. Different Q-bit individuals may then be assigned values based on a different *PrioritySequence*. The algorithm with such an assignment starts exploiting the favorable areas in solution space represented by such initialized Q-bit individuals quite early in the search process.

Table 5. Methods proposed for initialization of Q-bit individuals in GPQIEA

S. No.	Initialization Method	Effects	Advantages	Disadvantages
1	Same value $1/\sqrt{2}$ is assigned to all Q-bits.	Same probability to generate every solution	Maximum exploration is possible.	May need too much time to reach good solutions
2	Same value to Q-bits such that their square is closer to 1 (say 0.9) or closer to 0 (say 0.1)	Will find a solution near the trivial solution where all bits are 1 or 0 faster.	Useful when optimal solution is close to these trivial solutions.	May become redundant when solution is not close to any of these trivial solutions
3	Some random value in the range around $1/\sqrt{2}$, say between 0.6 and 0.8	Will find a solution near to non-trivial solution where all bits are away from 1 or 0 faster.	Useful when optimal solution is not close to any trivial solution.	May be unnecessarily biased towards a not so good solution
4	Values are assigned on the basis of known good solution, such that a value closer to 1 say 0.8 is assigned to selected items and closer to 0 say 0.2 is assigned for not selected items.	Converges to the heuristic good solution very fast	Generates a good solution faster	May get stuck in local optima around the known good solution
5	Single set of <i>PriorityPockets</i> or single <i>PrioritySequence</i> is formed based on heuristic function, and value based on the heuristic function values are assigned to the Q-bits	Focuses on the area around good heuristic solution for exploitation	Good solutions are expected to be found faster	The possibility to get stuck in a local optimum is reduced but it still exists. The overhead of initial calculations increases.
6	Multiple set of <i>PriorityPockets</i> or <i>PrioritySequences</i> are formed and different Q-bit individuals are initialized based on these different <i>PriorityPockets</i> or <i>PrioritySequences</i> .	Focuses on a number of different areas in search space around some good solutions for exploitation.	Good solutions are expected to be found faster. More diversity is maintained	The possibility to get stuck in a local optimum is further reduced which may still exist to some extent. The overhead of initial calculations increases and a trade-off needs to be found.

Figure 2. A typical initialization of Q-bits in proposed GPQIEA framework. Q-bits for items shown are sorted in an order of their preference (PrioritySequence of items) from left to right.



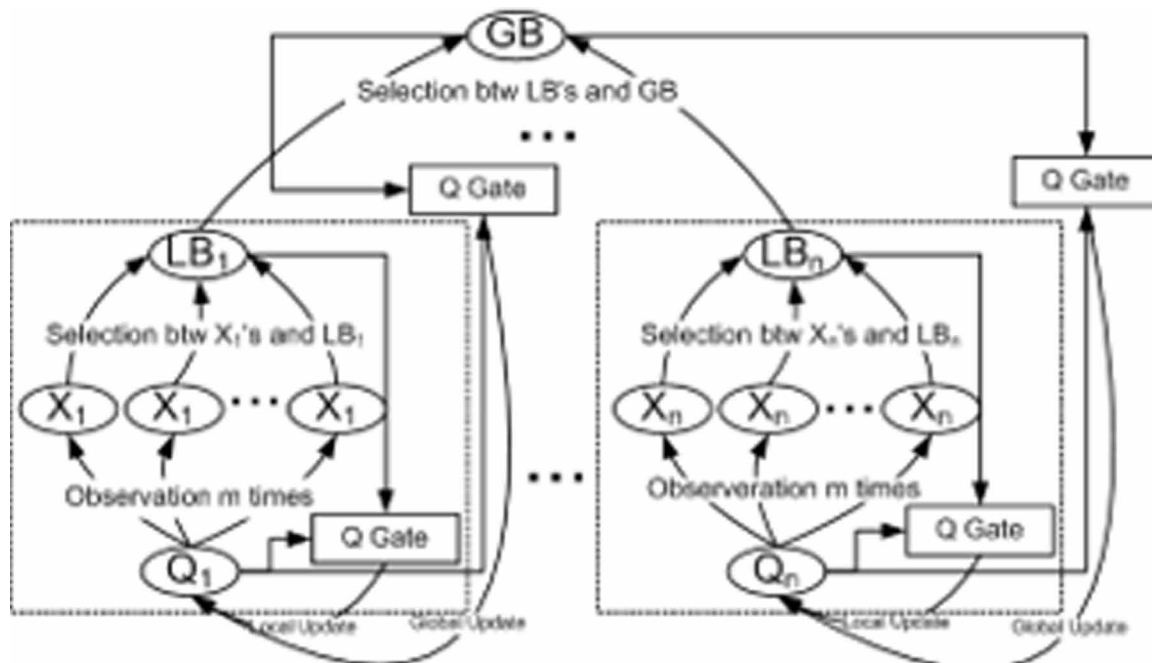
2.2.3. Parallelizable Balanced Structure (F3)

As shown in Figure 3, local and global attractors are used in the Q-gate to update the Q-bit individuals at two different levels simultaneously in GPQIEA. The local attractors (LB's) are never replaced by the global attractor (GB) unlike (Han & Kim, 2002). Only the solutions generated using the corresponding Q-bit individuals replaces the Local attractors. The LB and GB are both used to update each Q-bit individual again unlike (Han & Kim, 2002). These changes in the structure speed up the evolution while maintaining diversity by the simultaneous exploitation of local and global traits of generating populations. The local traits through local best solutions are preserved in local attractors whereas the global attractor preserves the global traits through the global best solutions evolved. This helps in achieving a steady, controlled and balanced evolution. The proposed structure implements non-elitism as local attractors may be worse than the global attractors. The idea of using multiple attractors and/or non-elitist attractor has also been used in earlier attempts to avoid local optima (2007; Kliemann, Kliemann, Patvardhan, Sauerland, & Srivastav, 2013).

For selecting the local attractor, multiple observations on a Q-bit individual are made in GPQIEA. Making multiple observations on a Q-bit individual helps the search as follows:

- It helps in better exploitation of the areas represented by the Q-bit individuals;
- It helps in assessing the capability of Q-bit individuals to generate different solutions. When multiple observations made on a Q-bit individual lead to the same solution after having repair (section 2.2.5), it is futile for further evolution.

Figure 3. Structure of GPQIEA with balanced exploration and exploitation. LB- Local Best Solution, GB- Overall best solution observed so far dubbed Global Best Solution.



In the proposed structure, local attractors are never assigned the value of global attractor or another neighbor unlike (Han & Kim, 2002). Rotations of Q-bit individuals are performed towards local attractors. Thus, a larger proportion of work can be done independently and hence, in parallel, as shown by the dotted regions in Fig. 3 in an iteration of the QIEA.

2.2.4. Faster Exploitation of Systematically Initialized Q-Bit Individuals (F4)

The QIEA improves the estimation of distribution represented by initialized Q-Bit strings (Han & Kim, 2004). Thus, the following computationally inexpensive steps of the QIEA may be performed on some or all of the initialized Q-bit individuals for a small number of iterations before beginning the evolution of GPQIEA:

- Collapse or observe Q-bit individuals;
- Repair the observed solutions;
- (optional) Perform heuristic-based local search using observed solutions;
- Evaluate and save best solution;
- Update Q-bit individuals using best solution as attractor.

It initializes the Q-bit individuals in a better way and performs a quick scan of promising regions of search space represented by them. It may help in solving the easier instances quickly. This task can be executed independently for each individual and hence performed in parallel.

2.2.5. Applications of Domain Knowledge to Repair Infeasible Solutions (F5)

Observation of Q-bit strings may result in infeasible solutions. These are rendered feasible through a repair step, in GPQIEA, which may result in quality improvements too.

In the trivial repair method, the binary value of elements in the infeasible solution is inverted in some random order iteratively. The bits are flipped randomly for few times and only those flips that yield a better feasible solution are retained. After the solution is made feasible, the process may continue to improve its quality by flipping the randomly selected bits in opposite direction till it remains feasible.

If a *PrioritySequence* is known, it may be used to select elements in order while repairing or improving the solution quality. A steepest hill climbing procedure may be adopted to obtain the best possible feasible solution from an available feasible solution using the priority order provided by *PriorityPockets* or *PrioritySequences*.

In a maximization effort, the iterative process to repair using *PrioritySequences* is as follows. First the elements are removed iteratively to make the solution feasible and then the elements are included to improve its quality. While making a solution feasible, the items positioned towards the end of these sequences are preferred for removal whereas while improving them, the ones positioned towards the beginning are preferred for inclusion. The multiple *PrioritySequences* may be used to repair an infeasible solution to produce different feasible solutions to maintain diversity. In case of COPs where the priorities of elements for selection are interrelated, *PrioritySequences* may be dynamically formed after each change in partial solution during repair procedure. The dynamic method is computationally expensive and requires careful analysis before applying it.

2.2.6. Specialized Heuristic-Based Local Search (F6)

The local attractors or global attractor are further improved after repair step using some iterative local search strategy. The iterations are repeated until no further improvement in objective function value is observed.

In place of a more exhaustive local search, which searches all possible solutions in the vicinity, one may look for only a few randomly selected neighbouring solutions. In parallel implementation this search function may be executed for each individual independently.

To summarize, domain information is utilized in GPQIEA using three methods as shown in Table 6 viz. heuristics, exhaustive local search and random local search. QIEAs suffer from a tendency to get stuck in local optima. Most of the modifications described above help the algorithm to exploit the search space around the heuristic solutions. This increases the speed of convergence but also increases the tendency of the algorithm to get stuck in local optima. The following features are proposed in GPQIEA for combating this problem by improving exploration capability of the algorithm.

2.2.7. Mutation (F7)

It has been observed while solving COPs using QIEAs that they sometimes converge very close to the optimal solution but have difficulty in pinpointing the global optimum. Thus, in GPQIEA when the Hamming distance between generated solution and the known best solution is lesser than a threshold the new solution is mutated. First, a few randomly selected items are removed. The resulting partial solution is then improved by randomly including some items iteratively in the solution as long as the solution remains feasible. This operation improves diversity without much computational effort. It helps to explore the solution space around a current solution so that an optimum in its vicinity is not missed. This improves the chance of finding global optimum in case it is near the converged solution.

2.2.8. Re-Initialization of Q-Bit Individuals (F8)

After a sequence of generations, the Q-bit individual almost converges and generates the same solution on almost (say 90%) every observation. Such Q-bit strings are re-initialized to restore diversity. The method/s for re-initialization may be chosen from those listed in Table 5.

2.2.9. Removal of the Non-Performing Q-Bit Individuals (StochasticPurge) (F9)

If the solutions generated using some Q-bit string are of poor quality consistently (e.g. much less than the average fitness), it may be removed from further evolution and be replaced with those Q-bit individuals which lead to generation of better solutions. In GPQIEA a Q-bit individual is given a specific lifetime to perform. If it continues to produce solutions of poorer quality than the average after its assigned lifetime, it is allowed to survive only with some reduced probability, say, 0.5. In case it ceases to exist, the best performer found so far replaces it.

2.2.10. Size Reduction (F10)

The QIEA keeps rotating the Q-bits of initialized Q-bit individuals towards the best solution it finds during evolution. When Q-bits are initialized based on domain knowledge as described in (2), the elements corresponding to the Q-bits assigned values close to 1(0), are preferably selected (not selected) in a generated good solution. Thus, the Q-bits assigned values close to 1(0) become closer to 1(0) during evolution and the possibility of rotating these Q-bits in the opposite direction reduces gradually and becomes very low. Continuing with such Q-bits in subsequent iterations of evolution may be futile, so the corresponding items may be removed from the population of individuals in next iteration as follows.

Table 6. Methods for forming problem specific information and its incorporation in GPQIEA

Problem Specific Feature	Steps in GPQIEA		
	Initialization	Every Step	Post-Processing
Heuristics	Heuristics are proposed to be used to form <i>PriorityPockets</i> or <i>PrioritySequences</i> , which are further used in initialization of Q-bit individuals. It is also used to initialize the global attractor which provides direction for updating the Q-bit individuals.	Heuristics are also proposed to be used while repairing the observed solutions, so that apart from becoming feasible the resulting solutions have better function value.	
Exhaustive Local Search	Problem specific exhaustive local search method is proposed for improving the global attractor after it is formed based on the heuristic.	Problem specific exhaustive local search methods are proposed for improving the intermediate local solutions generated during evolution.	Problem specific exhaustive local search methods are proposed to be used optionally for improving the final solution obtained after evolution is terminated.
Randomized Local Search		Problem specific randomized local search methods are proposed for improving the intermediate local solutions generated during evolution.	

Let Q-bit individual that generated the best individual is saved as “BestQ-bit”. When the Q-bit values in it cross the stipulated thresholds i.e. TU, upper threshold, or TL, lower threshold, (say valued to 0.95 and 0.05 respectively), the corresponding bits in solutions are permanently set to 1 (for Q-bit value > 0.95) or set to 0 (for Q-bit value < 0.05). The effective size of individual in further iterations of evolution reduces by these many bits. The reduction process is illustrated in Figure 4.

2.2.11. Termination Criteria (F11)

Empirically decided threshold limits are used as termination criteria like a fixed large number of generations, a fixed large number of function evaluations, etc.

For QIEA’s the values of Q-bits in Q-bit individuals may be used as a criterion for identifying whether the algorithm has converged or not. When sufficient number of the Q-bits attains values close to either one or zero, the algorithm may be terminated. When the reduction of problem size is used as a feature in GPQIEA a good criterion to stop the evolution is the size of the current problem. For example, if capac-

ity of the knapsack in current problem under consideration is reduced to $1/10^{\text{th}}$ of the original capacity then it may be assumed that there is not much left to be done.

2.3. The GPQIEA

The features proposed to be incorporated in GPQIEA, have been discussed in detail with their possible variations in section 2.2. Based on this discussion the overall framework crafted as pseudo-code is given in Figure 5. In this pseudo-code, $Q(t)$ refers to the Q-bit population after t^{th} iteration, $P(t)$ is the population of individual solutions, $B(t)$ is the set of best solutions found so far corresponding to each individual. The population of Q-bits and other individuals changes after each iteration. S is the variable to measure size of the problem (like number of items) and S_{original} defines the size of original problem. Individuals in $Q(t)$, $P(t)$ and $B(t)$ are referred using q_j^t , p_j^t and b_j^t respectively for $j \in [1, \dots, W]$, where W is the size of population; b refers to global best solution found so far and bqbit refers to best Q-bit individual which produced the best solution. Let m be the number of items to be considered in the problem. Some functions called in GPQIEA are defined as follows:

- **HamDistance**(p_j^s , \mathbf{b}): Returns Hamming distance between two binary strings.
- **Mutate**(p_j^s): Mutates the solution p_j^s as described in section B.
- **Update** q_j^t based on b_j^t : Q-bits of q_j^t are rotated towards bits in b_j^t using a rotation gate.
- **StochasticPurge** ($\mathbf{B}(t)$, \mathbf{be} , \mathbf{we} , $\mathbf{Q}(t)$, \mathbf{bqbit}): ‘Be’ and ‘we’ refers to the best and worst values evolved so far in $\mathbf{B}(t)$. It replaces the Q-bit individual q_j^t by bqbit with probability 0.5 if value of b_j^t is below $(\mathbf{be} + \mathbf{we})/2$ after a predefined purge period. The values of ‘be’ and ‘we’ are updated during each call of this function;
- **SizeReduction** ($\mathbf{bqbit}, \mathbf{K}$): The flowchart is shown in Figure 4 where bqbit , the best Q-bit is shown as Q_i . The partial solution is represented as a set \mathbf{K} of selected items;
- **R**($\mathbf{S}, \mathbf{S}_{\text{original}}$): It is some relation between \mathbf{S} and $\mathbf{S}_{\text{original}}$ used as a criterion to stop the evolution when feature of size reduction is incorporated in algorithm that is designed based on GPQIEA.

The maximum number of iterations in algorithm is controlled using a global constant, MaxIterations . The stopping criteria may be decided in other ways too. The steps of GPQIEA are described in brief as follows:

1. The algorithm starts by creating *PriorityPockets or Sequences* (lines 1 and 2). After initializing the parameters and best solution (lines 3 and 4), Q-bits in $Q(t)$ are initialized as described earlier (line 5);
2. Fast exploitation of some Q-bit individuals is performed using basic steps of QIEA (line 6) and population of best solutions in initialized (lines 7 to 9);
3. The evolution is carried out for MaxIterations times (or until the criterion based on size of current problem is satisfied), through the tasks described in the lines 11 to 31;

Figure 4. Procedure for size reduction

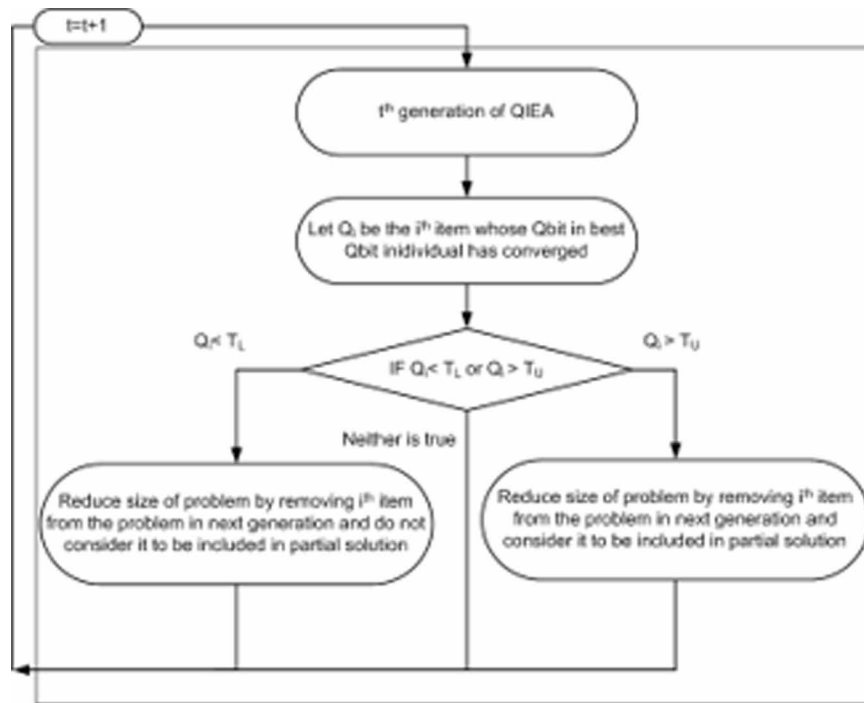


Figure 5. Pseudo-code for GPQIEA

```

Procedure GPQIEA
1 N ← number of methods or heuristics to be used.
  W ← population size, m ← size of problem universe U.
2 Define pockets of items in N ways based on N methods or heuristics decided in step 1. Let  $M_i$  be the number of pockets when  $i^{th}$  method is used,  $i \in \{1, \dots, N\}$ . Let  $P_i^k \subseteq U, \rho \in \{1, \dots, M_i\}$ , denotes the priority pockets formed using  $i^{th}$  method. So that,  $U = \bigcup_{i=1}^N P_i^k = U$  and  $\bigcap_{i=1}^N P_i^k = \emptyset, \forall i$ . Also, let  $l_i^k$  and  $u_i^k$  in  $[0, 1]$  are lower and upper bounds for the range of priority value assigned to  $\rho^{th}$  pocket when  $i^{th}$  method is used. When  $i^{th}$  method forms a PrioritySequence,  $|P_i^k|=1, \forall \rho$ . Different sequences can be formed independently and concurrently.
3 Initialize the global best solution, b, using the known best heuristic.
4 Set following-  $t \leftarrow 0, S_{best} \leftarrow S, w \leftarrow b, be \leftarrow 0$ , let initial solution K is an empty set.
5 Initialize  $q_i^k, i \in \{1, \dots, W\}$ , based on priority pockets defined above. Let items in U are numbered from 1 to m and  $q_i^k[k], k \in \{1, \dots, m\}$ , represents corresponding Q-bit value. When a  $q_i^k$  is initialized using priority pockets formed using  $i^{th}$  method,  $q_i^k[k]$ s assigned a value in range  $[l_i^k, u_i^k]$  if  $k^{th}$  item is in  $\rho^{th}$  pocket. Similarly initialize the best Q-bit individual using one of the method, qbit. Initialization of different individuals can be done concurrently.
6 Update some Q-bit individuals,  $q_i^k$ , using a few iterations of basic QIEA. May be done concurrently.
7 Collapse the population  $q_i^k$  in  $Q(t)$ , to form  $p_i^j$  in  $P(t)$ . (May be concurrently)
8 Repair each  $i^{th}$  solution  $p_i^j, j \in \{1, \dots, W\}$ , using some  $i^{th}$  set of priority pockets  $P_i^k, i \in \{1, \dots, N\}$ , in order to improve the solutions apart from making them feasible. (May be concurrently)
9 Initialize the population of best solution B(t) using repaired solutions in P(t). (May be concurrently)
10 while (t < MaxIterations and R(S, S_{best})) {
11   for each  $j \in \{1, \dots, W\}$  (may perform concurrently)
12     for t from 0 to  $n_t$  do {
13       count ← 0
14       for s from 0 to  $n_s$  do {
15         Collapse the population of Q-bit individuals,  $Q(t)$ , to form  $i^{th}$  solution in P(s).
16         Repair  $i^{th}$  solution in P(s), using  $P_i^k, i \in \{1, \dots, N\}$  for some i.
17         if (HamDistance( $p_i^j, b$ ) > 2) Mutate( $p_i^j$ )
18         Evaluate P(s)
19         if ( $p_i^j$  better than  $p_i^j$ ) then  $p_i^j \leftarrow p_i^j$ 
20         if (P(s) equals P(s-1)) Increment count by 1
21       } // for s*
22     } // for t*
23     Improve solutions  $p_i^j, j \in \{1, \dots, W\}$ , using a heuristic-based local search method. Randomized local search may instead be used for improving some of the solutions to decrease the overhead.
24     for each  $j \in \{1, \dots, W\}$  if ( $p_i^j$  is better than  $b$ ) then  $b \leftarrow p_i^j$ 
25     for each  $j \in \{1, \dots, W\}$  if ( $b$  is better than  $b$ ) then  $b \leftarrow b, qbit \leftarrow q_i^k$ 
26     for each  $j \in \{1, \dots, W\}$  Update  $q_i^k$  based on  $b$ 
27     Re-initialize the Q-bit individual  $q_i^k$  if the required criterion is satisfied.
28     StochasticPurge (B(t), be, we, Q(t), qbit)
29   } // for t*
30   for each  $j \in \{1, \dots, W\}$  Update  $q_i^k$  based on b
31   t ← t + 1
32 } // while*
SizeReduction (qbit, K)
for each  $i^{th}$  bit in solution of reduced problem (if (b(i)) { K ← K U i }
  
```

4. Each individual of $Q(t)$ is observed η_1 times and the solutions are repaired using the RepairGreedy function to make them feasible (lines 14 and 15). These solutions are mutated based on the Hamming distance (line 16). Only the best solution out of observed η_1 solutions is retained for further processing. The count of same solutions generated in this process is saved for re-initialization of the Q-bit individuals;
5. The solutions retained above are improved using deterministic or randomized local search technique (line 21). The local best and global best solutions are recognized (line 22 and 23). The Q-bit individuals are updated based on respective local best solutions (local update) (line 24). Re-initialization and StochasticPurge operations are performed in lines 25 and 26 respectively;
6. After performing local updates η_2 times, the Q-bits individuals are updated based on global best solution (global update) (line 28). Size reduction is carried out in line 30. If the problem size after several reductions becomes very small, the evolution may terminate before MaxIterations (line 7);
7. Finally, after the evolution terminates the solution is formed (line 32).

3. GPQIEA IMPLEMENTATIONS

The features of GPQIEA are listed in Table 7 with a brief remark about their implementation for solving different problems considered here. The detailed description for these implementations is discussed in following subsections. The experiments for serial implementations are performed on a machine with Intel→Xeon→ Processor E5645 (12M Cache, 2.40 GHz, 5.86 GT/s Intel→ QPI). For parallel implementation the computation is performed on Dell HPCC having one DELL PowerEdge R710 Rack Server as master blade and 24 DELL PowerEdge M610 Blade Servers as compute nodes. Each blade uses Intel→Xeon→ processor (5500 and 5600 series) @2.67 Ghz.

Table 7. An overview of features to be incorporated in proposed GPQIEA

Feature	Description	Remarks on Implementation		
		DKP	QKP	MKP
F1.	Initializing Best Solution	Initialized using the greedy heuristic for KP	The combination of RVD based heuristic and local search is used.	Initialized using the MTHM
F2.	Q-Bit initialization using <i>PrioritySequences</i> .	The items are sorted initially based on heuristic to form a single <i>PrioritySequence</i> . Corresponding Q-bits are then initialized to adjust the biases based on the position in this sequence.	Multiple <i>PrioritySequences</i> for items is generated based on heuristic defined statically to form multiple <i>PrioritySequences</i> . Corresponding Q-bits of different individuals are then initialized to reflect these priorities based on the position in these sequences.	The items are sorted based on heuristic to form single <i>PrioritySequence</i> . Corresponding Q-bits are then initialized to adjust the biases based on the position in this sequence.
F3.	Modified Structure	The new proposed structure is used. Parallel implementation not required.	The new proposed structure is used with parallel implementation for larger instances.	The new proposed structure is used without parallel implementation.

continues on following page

Table 7. Continued

Feature	Description	Remarks on Implementation		
		DKP	QKP	MKP
F4.	Local Exploitation before exploration	Not found beneficial as the time required by the actual iterations was very less.	It is used for improved solution quality in lesser time.	Not found beneficial as the time required by the actual iterations was very less.
F5.	Modified Repair based on heuristic	The position of an item in sorted input is used to decide which items to include or exclude.	The position of an item in sorted input is used to decide which items to include or exclude.	The position of an item in sorted input is used to decide which items to include or exclude.
F6.	Local Search	Not Implemented	The Local search is performed to improve intermediate local best solutions. Two versions of the search procedure are adopted to improve two sets of solutions. One set of solutions is improved using the exhaustive local search and another using the Randomized local search.	Local search based on MTHM is performed to improve intermediate solutions.
F7.	Mutation	Not Implemented	The solution is first changed by making a few randomly selected bits to 0. This is further improved assigning 1 to some of the components iteratively in the solution as long as the solution remains feasible.	Not Implemented
F8.	Re-initialization	Not Implemented	A Q-bit individual is chosen for re-initialization if it generates same solutions more than 60% of times. The Q-bits are re-initialized using original initialization QIEA approach.	Not Implemented
F9.	Stochastic Purge	Not Implemented	The same approach is adopted as described in section 2.7.	Not Implemented
F10.	Size Reduction	Since many Q-bits settle early it becomes effective in reducing the effort without compromising the quality of solutions.	Not Implemented	Not Implemented
F11.	Termination criterion due to size reduction	The termination criterion is enhanced to use the capacity of reduced problem.	Not Implemented	Not Implemented

3.1. Difficult Knapsack Problems (DKP)

In the most basic form of 0/1 Knapsack Problem (KP) a set of n items are considered each having a profit p_j and weight w_j . The KP is to maximize the total profit of a subset of items such that their total weight does not exceed the capacity C :

$$\text{Maximize: } \sum_{j=1}^n p_j x_j \tag{5}$$

$$\text{Subject to: } \sum_{j=1}^n w_j x_j \leq C \tag{6}$$

$$x_j \in \{0,1\}, j \in \{1, \dots, n\} \tag{7}$$

The problem is NP-Hard but it can be solved in pseudo-polynomial time (running time is polynomial in the numeric value or magnitude of the input and the capacity of knapsack, but exponential in the length of input) through dynamic programming (Pisinger, 1995). Several variants of KP can be obtained by relaxing some of the constraints.

Some types of instances called Difficult Knapsack Problems called (DKPs) have been found difficult in actual practice (Martello, Pisinger, & Paolo, 2000; Pisinger, 2005; Martello, Pisinger, & Toth, 1999; Reilly, 2009). The selected DKPs for computational experiments are shown in Table 8.

Table 8. Selected DKPs for computational experiments

Type	Name of Problem
1	Uncorrelated data instances
2	Strongly correlated instances
3	Bounded strongly correlated instances
4	Multiple strongly correlated instances: mstr(3R/10, 2R/10, 6).
5	Profit ceiling instances: pceil(3)
6	Spanner Instances: uncorrelated span(2,10)
7	Spanner Instances: strongly correlated span(2, 10).

Several deterministic (Balas & Zemel, 1980; Fayard & Plateau, 1975; Martello & Toth, A new algorithm for the 0-1 knapsack problem, 1988; Martello & Toth, An upper bound for the zero-one knapsack problem and a branch and bound algorithm, 1977; Martello & Toth, Knapsack Problems: Algorithms and Computer Implementations, 1990; Pisinger D., A minimal algorithm for the 0-1 knapsack problem, 1997; Pisinger D., An expanding-core algorithm for the exact 0-1 knapsack problem, 1995; Boyer, Baz, & Elkihel, 2012) and non-deterministic (Ezziane, 2002; Mohanty & Satapathy, 2009; Bansal & Deep, 2012; Wang, et al., 2005) approaches have been used to solve KP in literature. The GPQIEA is implemented with an objective to solve larger and harder instances of KP. In section 3.1.1 the domain knowledge representation for DKP vis-à-vis the proposal in GPQIEA is explained. The implementation details for some features specific to the DKP is discussed in section 3.1.2.

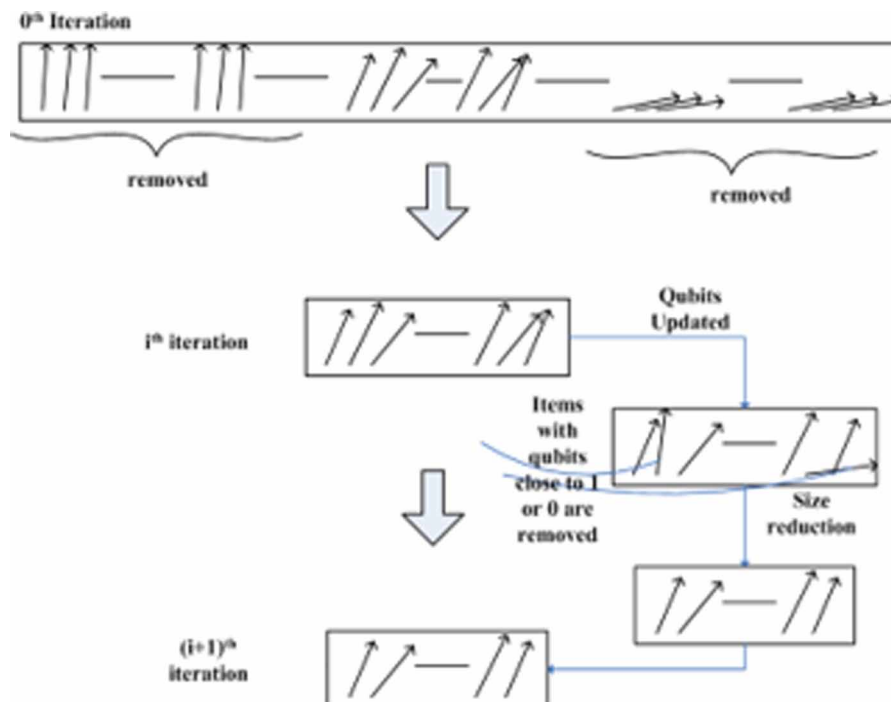
3.1.1. Heuristic of KP Used for Representing Domain Knowledge as Proposed in GPQIEA

A popular greedy heuristic to solve KP sorts the items in decreasing order of their efficiencies p_j/w_j . They are then packed into the knapsack in that order such that the capacity constraint is not violated. In GPQIEA, *PrioritySequence*, is formed using the above greedy heuristic the Q-bits corresponding to the items having higher efficiencies p_j/w_j are initialized to have higher probabilities of collapsing to 1.

3.1.2. Feature-Wise Implementation Details Specific to DKP

- F1:** The global attractor is initialized to the solution generated using greedy heuristic where the items are included in solution on the basis of decreasing efficiencies p_j/w_j .
- F2:** To initialise Q-bit strings, the items are assigned probabilities of inclusion which decreases with their position in *PrioritySequence*. As explained in section II.A.2, The Q-bits are initialized to values decreasing from 0.95 to 0.2 for items sorted in the decreasing order of the profit by weight ratios as follows. Q-bits in first and third parts are assigned values closer to 1 and 0 respectively while the Q-bits in second part are assigned values around $1/\sqrt{2}$.
- F5:** The repair step, named RepairGreedy, improves the quality of solution after making it feasible using *PrioritySequence* as explained in section II.A.2.
- F10:** Size reduction: As explained in section 2.2.10 the size of the problem is reduced also illustrated in Figure 6.

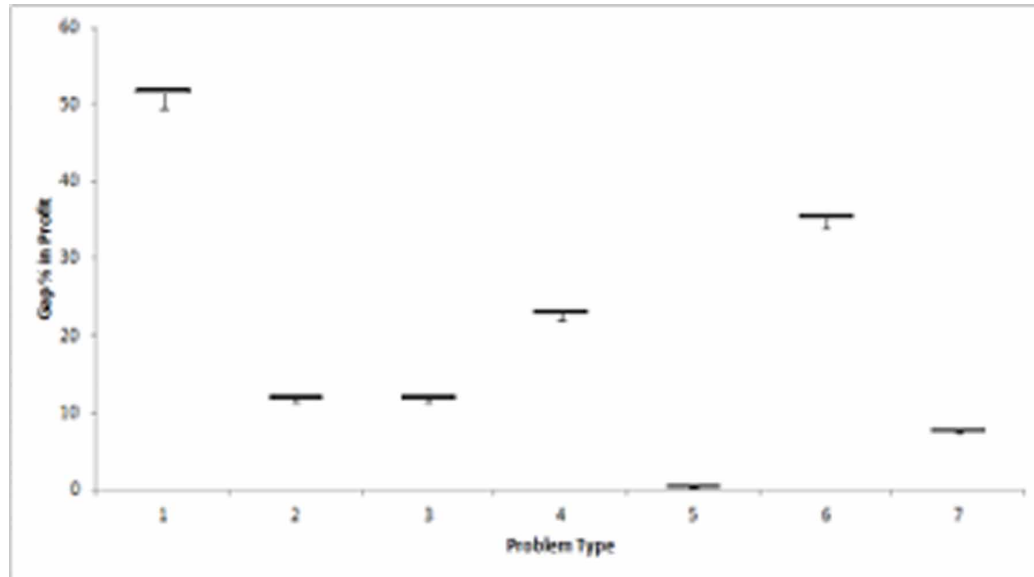
Figure 6. Illustrating the process of size reduction during subsequent generations of GPQIEA



Suppose bqbit store the Q-bit string that generates the best individual. When the Q-bits in bqbit cross the stipulated thresholds, the corresponding items are permanently considered as selected (for Q-bit value > 0.9) or outright rejected (for Q-bit value < 0.1) and hence removed from further search process. The population of best solutions is re-initialized whenever the size of the problem is reduced as the problem changes after the size reduction. This is also beneficial in improving the exploration capability of the algorithm as it increases the diversity in the population.

F11: Termination criteria: The capacity of the knapsack reduces with the reduction in the size of problem. Evolution process is terminated either when maximum number of iterations is reached or when the capacity of the problem reduces to $1/10^{\text{th}}$ of the original.

Figure 7. Boxplots for gap% in profit between QIEA and GPQIEA for various types of problems

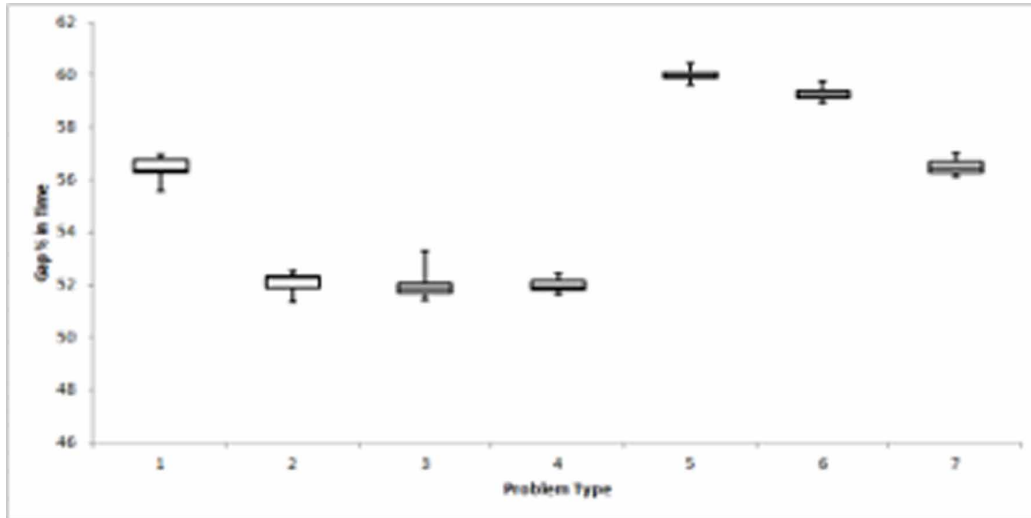


3.1.3. DKP Results and Discussion

The experiments are conducted on a machine with Red Hat Linux (RHEL6) operating system running on Intel→ Xeon→ Processor E5645 having specifications as 12M Cache, 2.40 GHz, 5.86 GT/s Intel→ QPI to study effects of various modifications introduced in GPQIEA. The value of each η_1 and η_2 is empirically set to 5, population size to 5 and MaxIterations to 10. Comprehensive results for various types of KP instances with size ranging from 10K to 290K of items are presented here.

The box-plots in Figure 7 present the comparison of gap% in profit observed between QIEA and GPQIEA for different types of problems based on results obtained from experiments. Similarly, the box plots of Figure 8 present the comparison of gap% in time taken for different types of problems.

Figure 8. Box plots for gap% in time between QIEA and GPQIEA for various problem types



A large gap% in profits indicates that GPQIEA found much better solution than QIEA. This is because QIEA found solutions far from optimal and so GPQIEA had considerable scope for improvement. Further a larger gap% in time indicates that GPQIEA converged much faster than QIEA either due to faster setting of Q-bits or due to quick reduction in size.

Following observations are made from the experimental results:

- GPQIEA outperforms the simple QIEA in terms of the quality of solutions and time taken to compute them for all types of KP instances considered;
- The problem types considered are arranged in decreasing order of gap% in solution quality as follows:
 - Uncorrelated instances;
 - Spanner uncorrelated instances;
 - Multiple strongly correlated instance;
 - Strongly correlated and bounded strongly correlated;
 - Spanner strongly correlated instances;
 - Profit ceiling type of instances;
- The problem types considered below are in decreasing order of gap% in computation time:
 - Profit ceiling instances;
 - Spanner uncorrelated instances;
 - Spanner strongly correlated instances;
 - Uncorrelated instances;
 - Strongly correlated, bounded strongly correlated and Multiple strongly correlated;
- Thus, GPQIEA provides good solutions in lesser time even for those problem types for which QIEA does not provide good solutions. For those types for which QIEA provides good solutions, GPQIEA provides similar or better solutions in much lesser time;

- Strongly correlated, Bounded Strongly Correlated, and Multiple Strongly Correlated are found equally hard in both, the QIEA and the GPQIEA. All of them show improvement in profit of around 10% with reduction in time of almost 52%. They are referred to as the trio in the following discussion.

An analysis of the above observation yields the following points:

- For Un-correlated and spanner uncorrelated both gap% (time and profit) are high. This means that they are very difficult for QIEA but very easy for GPQIEA. This is because, searching for good solution of these problems is directionless in simple QIEA whereas the heuristic provides better focus to the search process in GPQIEA;
- Spanner strongly correlated show profit increment of around 10% which is obtained faster in GPQIEA. Therefore, they are easier than the trio. The reason is that many elements in these are of similar weights and profits and so the QIEA and local search method find good solutions in such a solution space faster. Thus, this problem is a bit easier for QIEA than the trio while much easier for GPQIEA than the trio;
- For profit ceiling the gap% in profit is not high, but gap% in computation time is quite high. It means that they are easier than the trio. Here, values of profit and weight for each item are similar. Many items have same profit but slightly different weights. So, finding good solution in such a search space is easier. Further the greedy heuristic makes the search easier. These problems are very easy for QIEA and easier for GPQIEA.

3.2. Quadratic Knapsack Problem (QKP)

The 0/1 Quadratic Knapsack Problem (QKP) introduced by Gallo et al. (1980) is a generalization of the KP. Suppose n items and a knapsack are given, where w_j is the positive integer weight of the j^{th} item, C is a positive integer knapsack capacity, in an $n \times n$ nonnegative integer matrix $P = (p_{ij})$, p_{ij} is a profit achieved if item j is selected, and, for $j > i$, $p_{ij} + p_{ji}$ is the additional profit achieved if both items i and j are selected. The QKP is to find a subset of items whose total weight is not more than knapsack capacity C such that the overall profit is maximized. If x_j is a binary variable which is equal to 1 if j^{th} item is selected and 0 otherwise. Sometimes matrix P is considered symmetric such that $p_{ij} = p_{ji}$ for all i and j . In such a problem, additional profit achieved on selection of both items i and j is considered as p_{ij} rather than $p_{ij} + p_{ji}$, for $j > i$. Thus, researchers formulate the problem as follows:

$$\text{Maximize: } \sum_{i=1}^n \sum_{j=i}^n p_{ij} x_i x_j$$

$$\text{subject to: } \sum_{j=1}^n w_j x_j \leq C$$

$$x_j \in \{0, 1\}, j \in \{1, \dots, n\} \tag{8}$$

Several deterministic (Billionet & Soutif, An exact method based on Lagrangian decomposition for the 0-1 quadratic knapsack problem., 2004a; Caprara, Pisinger, & Toth, 1999; Fomeni & Letchford, 2012; Hammer & Rader, 1997; Létocart, Nagih, & Plateau, 2012; Pisinger D., The quadratic knapsack problem - a survey, 2007; Pisinger, Ramussen, & Sandvik, 2007) and non-deterministic (Azad, Rocha, & Fernandes, 2013; Julstrom, 2005; Pulikanti & Singh, 2009; Xie & Liu, 2007) approaches have been used to solve QKP in literature.

3.2.1. Heuristics Used to Formulate Domain Knowledge in GPQIEA for QKP

The Absolute Value Density (AVD_i) of any object *i* (in a QKP instance) is defined as the ratio of the sum of all values (linear as well as quadratic) associated with that object to its weight. A greedy heuristic that uses this parameter for selecting objects into the knapsack is given in Julstrom (2005). According to this, the objects are added into the knapsack in descending order of their absolute value densities until all objects have been considered, while ensuring that the capacity constraint is not breached.

The Relative Value Density (RVD) is the value density calculated based on the objects actually present in the knapsack at a time. Let a set *P* represents a partial solution such that $i \in P$ iff i^{th} item is included in the knapsack. The relative value density (RVD_i^P), of an item *i* with respect to partial solution *P*, is computed as:

$$\left(P_{ii} + \sum_{j \in P/\{i\}} P_{ij} \right) / w_i$$

A RVD-based greedy heuristic is an iterative algorithm such that each iteration begins with different object included in the solution and computes the relative value densities of objects not included with respect to the included ones, and adds to the solution the object *i* that fits and has the largest r_i , continuing until no more objects can be added to the solution. It then reports the solution with the largest total value.

Since pair-wise relations within the included elements also have an importance in QKP, the heuristic based on RVD is better than the AVD to solve the QKP. While finding a solution based on RVD the following points can be observed:

- The solution is built element by element starting with an arbitrary first element;
- The selection of next element depends on the partial solution built till that instant.

This means that to find a good solution for QKP what matters is not only the knowledge of which elements are finally chosen to form the solution but also the sequence in which they are chosen. This knowledge may be represented in *PrioritySequences*.

A *PrioritySequence* of items in QKP is formed by adding them iteratively starting with an empty solution without any constraint on capacity, such that each time an item, having maximum RVD with respect to the partial solution formed so far, is added. The item having the maximum diagonal profit (i.e. individual profit without considering pairs) can be selected as the first item with the rest being selected as stated above. The multiple sequences are generated by taking different items as the first item instead of item having the maximum diagonal profit.

3.2.2. Feature-Wise Implementation for QKP

The feature of size reduction is not used in implementation of GPQIEA for QKP. There are two reasons for this. One is the slight worsening of quality of solutions obtained when the feature of size reduction is activated. Another important reason is that the performance presented in literature for existing population-based search algorithms shows computation effort based on time taken by an implementation to reach best solution during a run and not the time taken to terminate. The experiments have shown that the size reduction plays more important role when complete time till termination is considered. Thus, in this section the feature of size reduction is removed to enable a fair comparison with other population-based search algorithms in literature.

A parallel implementation of GPQIEA is developed using Open MP. A study has been performed to observe the contribution of each feature in a parallel implementation towards performance improvement. Starting with a brief presentation of this study, the results of the parallel implementation are presented for 80 instances containing 1000 and 2000 variables. The results obtained are competitive with the best-known results for the considered benchmark instances of size 1000 and 2000 variables.

- F1:** A greedy solution is formed for QKP using the dual heuristic described above. Starting with an infeasible solution where all items are included in the knapsack, the greedy algorithm removes items iteratively till the solution becomes feasible. Each time the item that has minimum relative profit density is removed from solution. The solution thus generated is improved using the local search procedure.
- F2 and F5:** Initialize the Q-bit Individuals and Repair the Solutions: The multiple *PrioritySequences* formed as described above are used to initialize the Q-bits in an individual. The implementation of GPQIEA for QKP also improves the infeasible solution obtained after collapsing a Q-bit individual as was done for DKP.
- F4:** Faster local exploitation before global exploration: As described in section 2.2.3 a few basic steps as in original QIEA can be used to fine tune the initialization of Q-bit individuals. This feature has been included in enhanced implementation of GPQIEA here to solve QKP. Fifteen iterations of these steps are performed only on half of the Q-bit individuals in order to closely target the region of search space which is to be prioritized using an estimation of distribution of better solutions performed just by the original QIEA.
- F6:** Improving the Local Best Solutions Using Heuristic: As proposed in GPQIEA, local search method is used for improving the intermediate solutions obtained during evolution.

A local search function is used to improve the local best solutions, which are best among the multiple solutions generated using single Q-bit individual, to solve QKP. It iteratively executes passes as long as gain in profit is observed. The i^{th} element (if not in solution) is either included or replaced by an item j already in solution after each pass. The action of inclusion (or replacement) is performed for an item i (or pair i and j) which results in maximum gain in overall profit of the solution. All actions (inclusion and replacement) pertaining to combinations of i and j are first observed and only the change which gives best gain in profit is made effective in a pass.

The procedure defined above is deterministic and thus generate very similar solutions starting with different feasible solutions. Since it searches for all possible options of replacing and/or including a non-included item into the knapsack, it is computationally very expensive. To increase diversity and reduce

the cost, a lighter version is also used, where only some randomly picked actions are considered. It is applied on half of the population.

- F7:** Mutation of solutions when they appear to be stuck in local optimum: During mutation when new solutions are found too close to the overall best solution generated so far, 2-3 bits in the solution vector are randomly selected and changed to 0. Elements with better RVD are then iteratively included in solution as long as the solution remains feasible. To check closeness of the two solutions, Hamming distance between them is calculated. It helps in targeting better solutions in a search region more precisely.
- F8:** Re-initialization of Q-bit individuals: Each Q-bit of the Q-bit individuals which generate same solution for more than 3 times out of 5 observations is set to $1/\sqrt{2}$. It increases the diversity of solutions explored through Q-bit individuals using same computational effort and thus improves exploration.
- F9:** Replacing the non-performing Q-bit individuals by best (StochasticPurge): The Q-bit individuals are assigned a time span to perform. If a Q-bit individual is found to perform less than average after that, there remains 50% chance for it to survive. In case it ceases to exist it is replaced by the best performer found so far.

3.2.3. QKP Results and Discussion

The experiments are performed on a machine with Intel → Xeon → Processor E5645 (12M Cache, 2.40 GHz, 5.86 GT/s Intel → QPI). The machine uses Red Hat Linux Enterprise 6. The programs are written in C. For parallel implementation the computation is performed on Dell HPCC having one DELL PowerEdge R710 Rack Server as master blade and 24 DELL PowerEdge M610 Blade Servers as compute nodes. Each blade uses Intel → Xeon → processor (5500 and 5600 series) @2.67 Ghz.

The results obtained using serial implementation of GPQIEA with respect to QIEA is presented for experiments performed using the BS benchmark instances having 100, 200 and 300 binary variables. Almost all the problem instances considered here have been solved to optimality within 60 iterations, hence MaxIterations is set to 60. η_1 and η_2 are set empirically to 5 and population size is set to 160. Problems are named as n_d_i which specifies parameters size (n), density (d), seed (i) of an instance. Parallel implementation not required for these smaller instances.

The experiments were done to compare performance of QIEA with proposed GPQIEA using BS Benchmark Instances (Billionet & Soutif, QKP Instances, 2004b). GPQIEA is significantly better than the QIEA. GPQIEA provides optimal solution for all problems of size 100 variables in all 30 runs taking 0.02 sec on an average and requiring around 238 FES per trial on average for all 20 instances. GPQIEA provides optimal solution in less than 0.4 sec on average per trial (requiring around 2118 FES per trial) on an average for 20 instances of size 200 variables in all its 30 runs. GPQIEA provides optimal solution 99% times in 2 sec (requiring around 6369 FES) per trial on an average for 10 instances of size 300 variables. Out 10 instances, it provides optimal solution for all but one in all 30 runs. The comparison between QIEA and GPQIEA is illustrated using boxplots drawn on gap% of values from two algorithms, average time taken by each instance to reach best value in sec, average FES performed by each instance to reach best value (Figures 9, 10, 11, 12, and 13).

Figure 9. Boxplot to show avg. gap% between best profit values obtained using QIEA and GPQIEA for BS Benchmark Instances

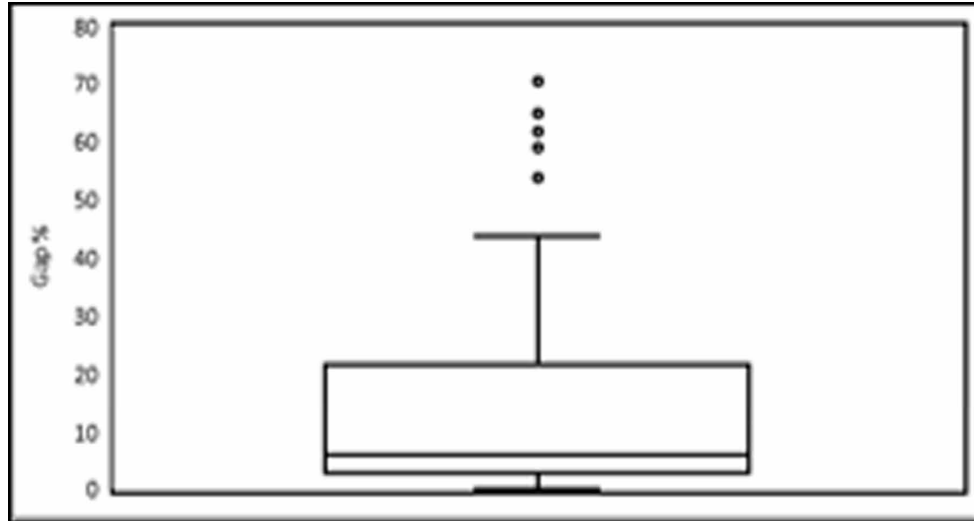
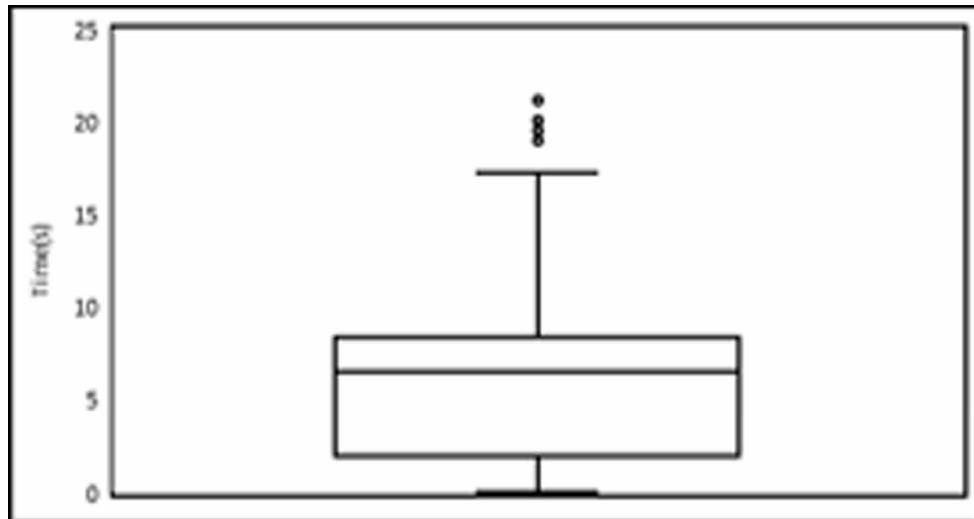


Figure 10. Boxplot for average time taken for each instance over 30 runs by QIEA for BS Benchmark Instances



The large instances of QKP (1000 and 2000 variables) used by Yang et al. (An effective GRASP and tabu search for the 0-1 quadratic knapsack problem, 2013) are solved here using GPQIEA. Max Iterations is set to 60 and population size is set to 320. 24 threads are spawned to process different individuals in parallel. The simple QIEA could not solve these pragmatically while GPQIEA provides the best known solution in significantly less time. RPD^k , value of best solution and average time taken to compute the best solution per run out of 100 runs is shown in Table 9. The instances are referred to as n_d_i where n means the size of problem, d means the density of profit matrix and i mean seed value ranging from

1 to 10. RPD^K (average of relative percentage deviation of v from known best value over total number of runs) is one of the parameter considered. It is calculated as $Average_{total\ runs} \left(\left(\frac{v^{bk} - v}{v^{bk}} \right) * 100 \right)$ where v is value obtained in a run for an instance and v^{bk} is its best-known value. The GPQIEA provided results comparable to state of the art for these large instances whereas the QIEA could not even provide considerable solutions.

Figure 11. Boxplot for average time taken for each instance over 30 runs by GPQIEA for BS Benchmark Instances

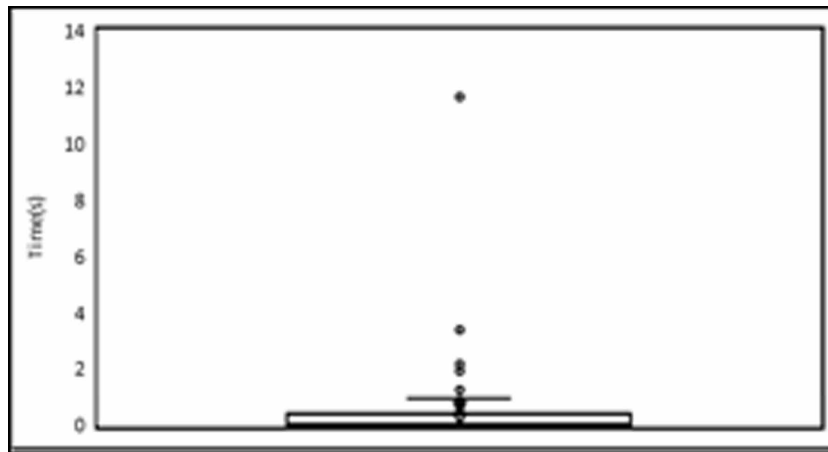
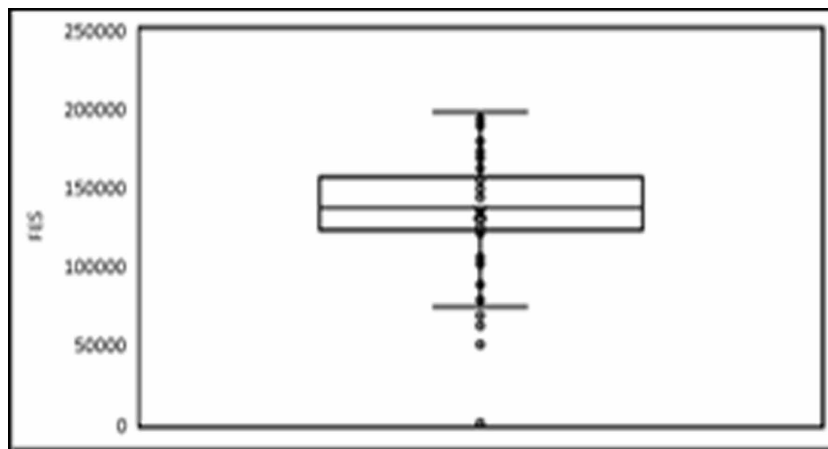


Figure 12. Boxplot for average FES for each instance over 30 runs in QIEA for BS Benchmark Instances



3.3. Multiple Knapsack Problem (MKP)

0/1 Multiple Knapsack Problem (MKP) is a generalization of the standard KP where multiple knapsacks are considered to be filled instead of one. The MKP problem is strongly NP-complete and no FPTAS is possible for MKP (Chekuri & Khanna, 2006).

Figure 13. Boxplot for average FES for each instance over 30 runs in GPQIEA for BS Benchmark Instances

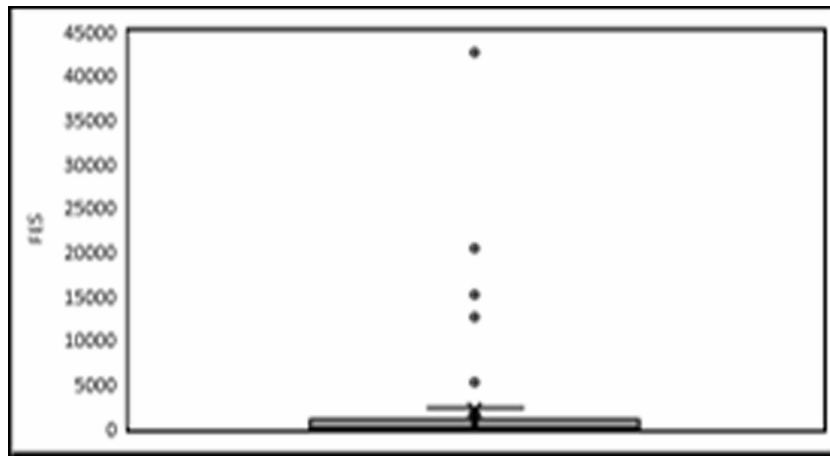


Table 9. Performance of GPQIEA for QKP instances of size 1000 and 2000 variables

n_d_l	Best Known	GPQIEA			n_d_l	Best Known	GPQIEA		
		RPD ^k	Best Achieved	t(s)			RPD ^k	Best Achieved	t(s)
1000_25_1	6172407	0	6172407	0.146	2000_25_1	5268188	0	5268188	451.067
1000_25_2	229941	0	229941	17.824	2000_25_2	13294030	0	13294030	186.651
1000_25_3	172418	0	172418	14.042	2000_25_3	5500433	0	5500433	509.844
1000_25_4	367426	0	367426	2.735	2000_25_4	14625118	0	14625118	13.286
1000_25_5	4885611	0	4885611	18.023	2000_25_5	5975751	0	5975751	21.035
1000_25_6	15689	0	15689	2.794	2000_25_6	4491691	0	4491691	317.178
1000_25_7	4945810	0	4945810	10.635	2000_25_7	6388756	0	6388756	20.841
1000_25_8	1710198	0	1710198	38.016	2000_25_8	11769873	0	11769873	16.236
1000_25_9	496315	0	496315	2.693	2000_25_9	10960328	0	10960328	187.348
1000_25_10	1173792	0	1173792	32.684	2000_25_10	139236	0	139236	24.982
1000_50_1	5663590	0	5663590	15.852	2000_50_1	7070736	3.96E-06	7070736	470.694
1000_50_2	180831	0	180831	9.837	2000_50_2	12587545	4.13E-06	12587545	501.619
1000_50_3	11384283	0	11384283	6.966	2000_50_3	27268336	0	27268336	14.263
1000_50_4	322226	0	322226	11.512	2000_50_4	17754434	4.35E-05	17754434	396.971
1000_50_5	9984247	0.000814	9984247	16.492	2000_50_5	16805490	0.002995	16805435	589.315
1000_50_6	4106261	0	4106261	26.888	2000_50_6	23076155	2.14E-05	23076155	243.05
1000_50_7	10498370	0	10498370	6.197	2000_50_7	28759759	0.006756	28758651	201.994
1000_50_8	4981146	0.00475	4981129	101.504	2000_50_8	1580242	0	1580242	116.759
1000_50_9	1727861	0	1727861	2.561	2000_50_9	26523791	3.74E-05	26523791	232.279
1000_50_10	2340724	0	2340724	38.948	2000_50_10	24747047	0	24747047	169.517
1000_75_1	11570056	7.93E-05	11570056	57.801	2000_75_1	25121998	0.000211	25121998	571.806
1000_75_2	1901389	0	1901389	35.46	2000_75_2	12664670	0	12664670	341.354
1000_75_3	2096485	0	2096485	33.272	2000_75_3	43943994	0	43943994	128.524
1000_75_4	7305321	0	7305321	19.986	2000_75_4	37496613	6.93E-07	37496613	234.359

continues on following page

Table 9. Continued

n_d_l	Best Known	GPQIEA			n_d_l	Best Known	GPQIEA		
		RPD ^k	Best Achieved	t(s)			RPD ^k	Best Achieved	t(s)
1000_75_5	13970240	0.002328	13970240	64.035	2000_75_5	24834948	0	24834948	395.601
1000_75_6	12288738	0	12288738	10.512	2000_75_6	45137758	0	45137758	12.759
1000_75_7	1095837	0	1095837	20.654	2000_75_7	25502608	0	25502608	340.182
1000_75_8	5575813	0	5575813	65.745	2000_75_8	10067892	0	10067892	291.29
1000_75_9	695774	0	695774	12.471	2000_75_9	14171994	0.000222	14171994	646.902
1000_75_10	2507677	0	2507677	2.586	2000_75_10	7815755	8.29E-05	7815755	394.449
1000_100_1	6243494	0.000339	6243494	96.208	2000_100_1	37929909	0	37929909	321.09
1000_100_2	4854086	3.63E-05	4854086	80.487	2000_100_2	33648051	0.000133	33648051	607.696
1000_100_3	3172022	0	3172022	31.601	2000_100_3	29952019	0.00024	29952019	529.829
1000_100_4	754727	0	754727	13.756	2000_100_4	26949268	1.48E-07	26949268	602.483
1000_100_5	18646620	0.000334	18646620	44.278	2000_100_5	22041715	0.001002	22041715	861.113
1000_100_6	16020232	0	16020232	11.393	2000_100_6	18868887	6.84E-05	18868887	715.625
1000_100_7	12936205	0	12936205	15.528	2000_100_7	15850597	0.000275	15850597	650.508
1000_100_8	6927738	0.000306	6927738	84.706	2000_100_8	13628967	0	13628967	292.19
1000_100_9	3874959	0	3874959	2.563	2000_100_9	8394562	0	8394562	369.983
1000_100_10	1334494	0	1334494	36.037	2000_100_10	4923559	7.23E-05	4923559	193.325
Average		0.0002247		27.8857			0.0003042		329.64993

Given a set of n items with their profits p_j and weights $w_j, j \in \{1, \dots, n\}$, and m knapsacks with capacities $c_i, i \in \{1, \dots, m\}$, the MKP is to select a subset of items to fill the given m knapsacks such that the total profit is maximized and sum of weights in each i^{th} knapsack does not exceed its capacity c_i :

$$\text{Maximize: } \sum_{i=1}^m \sum_{j=1}^n p_j x_{ij} \tag{9}$$

$$\text{Subject to: } \sum_{j=1}^n w_j x_{ij} \leq c_i, i \in \{1, \dots, m\}, \tag{10}$$

$$\sum_{i=1}^m x_{ij} \leq 1, j \in \{1, \dots, n\}, \tag{11}$$

$$x_{ij} \in \{0, 1\}, \forall i \in \{1, \dots, m\}, \forall j \in \{1, \dots, n\}, \tag{12}$$

Thus, $x_{ij} = 1$ means that item j is packed in to knapsack i , and when item j is not selected in any knapsack $x_{ij} = 0 \forall i \in \{1, \dots, m\}$. The coefficients p_j, w_j and c_i are positive integers. Several attempts have been made to solve MKP in literature (Hung & Fisk, 1978; Jansen, 2012; Lalami, Elkihel, El-Baz, & Boyer, 2012; Martello & Toth, A bound and bound algorithm for the zero-one multiple knapsack

problem, 1981; Martello & Toth, Solution of the zero-one multiple knapsack problem, 1980; Pisinger, 1999; Jansen, 2009).

In order to avoid any trivial case, the following assumptions are made:

1. Every item has a weight less than the largest knapsack:

$$\max_{j \in \{1, \dots, n\}} w_j \leq \max_{i \in \{1, \dots, m\}} c_i \quad (13)$$

2. There is at least one element whose weight is less than the smallest knapsack:

$$\min_{i \in \{1, \dots, m\}} c_i \geq \min_{j \in \{1, \dots, n\}} w_j \quad (14)$$

3. There is no knapsack whose capacity is larger than the sum of weights of all items:

$$\sum_{j=1}^n w_j \geq c_i, \forall i \in \{1, \dots, m\} \quad (15)$$

3.3.1. A Heuristic for MKP

Martello and Toth (Solution of the zero-one multiple knapsack problem, 1980) proposed a popular heuristic for solving the MKP, called MTHM, which consists of three phases. The MTHM is briefly explained as follows. The details of the MTHM are available in (Martello & Toth, Knapsack Problems: Algorithms and Computer Implementations, 1990, pp. 179-181). It consists of three phases:

1. In the first phase of MTHM an initial feasible solution is obtained. The greedy algorithm is first applied to the first knapsack. The set of remaining items is obtained and considered in next step. The same procedure is applied for the second knapsack in the next step. This is continued till the m^{th} knapsack is considered;
2. In the second phase, the initial solution is improved. Every pair of items is considered such that both are assigned to different knapsacks. The items of such a pair are swapped and a new item is inserted, if swapping them and inserting a new item in any of the knapsack results into an increase in the profit;
3. In last phase, each selected item is tried to be replaced by one or more remaining items. Such a change is made effective if it results into an increase in the total profit.

The MTHM has the advantage that some items can be exchanged from a knapsack with another or excluded from the solution set so that the total profit increases, which can lead to an efficient and fast solution when the solution given by the first phase is good. Moreover, they can be applied to any feasible solution effectively. The main drawback of MTHM is that it considers only the exchanges between a pair of items and not the combinations of items.

Various phases of this heuristic are proposed to be introduced at different steps of GPQIEA to improve the quality of solutions. The first phase of this heuristic is used while repairing the infeasible solutions generated by collapse operation of GPQIEA. The second and third phases are applied as local search techniques on the intermediate solutions during the iterations of GPQIEA.

3.3.2. Feature-Wise Implementation of GPQIEA for MKP

A solution to MKP is represented by a string of non-binary integers greater than or equal to zero. A non-zero integer specifies the knapsack where the particular item is placed if selected otherwise a zero is specified. Solution of MKP involves two levels of choice – one for selecting an item to be placed in the knapsack and other for selecting the knapsack in which it is to be placed. However, the standard Q-bit collapses to either 0 or 1 so to generate the binary solutions. When standard Q-bit is used in an implementation, a solution may be represented using a set of two sequences. First sequence identifies if an item is selected or not. Whereas, the second sequence provides an integer coded in binary identifying the knapsack where the item is placed.

F1 - Heuristic Used to Initialize the Global Attractor in GPQIEA to Solve MKP: The solution obtained using the MTHM, i.e. using all three phases mentioned, is considered as the initial global attractor so that GPQIEA converges quickly to the heuristic solution.

F2 - The items are sorted in decreasing order of their profit by weight ratio to form a *PrioritySequence*: Thereafter, the values in Q-bit individuals are initialized to represent probability distributions of good solutions. The method for sorting and initializing the Q-bit individuals used to solve MKP is similar to that used to solve KP as described earlier.

F5 - Improved Repair Procedure in GPQIEA to Solve MKP: To repair infeasible MKP solutions obtained after collapsing a Q-bit individual, the items are removed from every such knapsack where the total weight of included items exceeds its capacity. Since items have been sorted in decreasing order of their profit by weight ratios, removing items lying in latter part in this *PrioritySequence* will lead to minimum reduction in profit and/or maximum reduction in weight contained in a knapsack. Therefore, items are removed in that order from each knapsack until the weight contained in it becomes less than the capacity.

The partial feasible solution obtained after performing the above operation is further improved using the first phase of MTHM heuristic described in section 3.3.1. The knapsacks are sorted in increasing order of their capacities and considered in that order. In every new knapsack considered the items which have not been selected in any other knapsack are packed. Items are considered for inclusion in the order provided by their sequence obtained after sorting them based on their profit by weight ratio.

F6 - Local Search: Phase 2 and phase 3 of MTHM provide methods to improve a solution of MKP by exchanging some items from a knapsack to another or excluding from the solution set so that total profit increases.

These two methods have been implemented separately. Applying both of them together may require too much computational effort without producing much improvement in the solution. Since they are implemented separately, they can either both be used in combination to improve a local solution or any

one of them may be used independently. It is observed that applying both of the phases prove beneficial only in the beginning of evolution because obtained solution is far from optimal. But when the solution is closer to optimal, applying the second phase of MTHM rarely improves the solution even after expending considerable computational effort. They are both used together to repair a solution obtained after collapsing a Q-bit individual during initial faster exploitation of Q-bit individuals. However, the local best solutions of GPQIEA are improved using only the third phase of MTHM.

F7 & F8: The procedure as defined for DKP is used here too for MKP.

3.3.3. MKP Results and Discussion

The solutions converged for most of the problem instances considered here within 10 iterations hence maxIterations is set to 10. These instances are randomly generated, using the generator of instances available at the Pisinger's home page¹. Two types of instances have been generated, first the strongly correlated where weights w_j are distributed in $[1, R]$ and profits p_j are calculated as $p_j = w_j + R/10$ and second the uncorrelated where weights w_j and profits p_j are independently distributed in $[1, R]$. Such instances correspond to a real-life situation where the return is proportional to the investment plus some fixed charge for each project. Two different cases of capacities are considered: similar and dissimilar.

In case of similar capacities, the first $m-1$ capacities $c_i, i \in \{1, \dots, m-1\}$ are distributed in:

$$\left[0.4 \sum_{j=1}^n w_j / m, 0.6 \sum_{j=1}^n w_j / m \right] \forall i \in \{1, \dots, m-1\} \quad (16)$$

In case of dissimilar capacities the first $m-i$ capacities c_i are distributed in:

$$\left[0, 0.5 \sum_{j=1}^n w_j - \sum_{k=1}^{i-1} c_k \right] \forall i \in \{1, \dots, m-1\} \quad (17)$$

The last capacity c_m is chosen as:

$$c_m = 0.5 \sum_{j=1}^n w_j - \sum_{i=1}^{m-1} c_i \quad (18)$$

Strongly correlated instances having similar and dissimilar capacities are randomly generated using random generator by Pisinger with number of elements ranging from 1000 to 10000 with the number of knapsacks ranging from 2 to 100.

Figure 14 shows the comparison of how the best profit value obtained through QIEA and GPQIEA converges. The iteration number and the profit achieved have been plotted on x-axis and y-axis respectively.

Figure 14. Comparing convergence of best value achieved using QIEA and GPQIEA (an instance having $n=5000$, $m=100$)

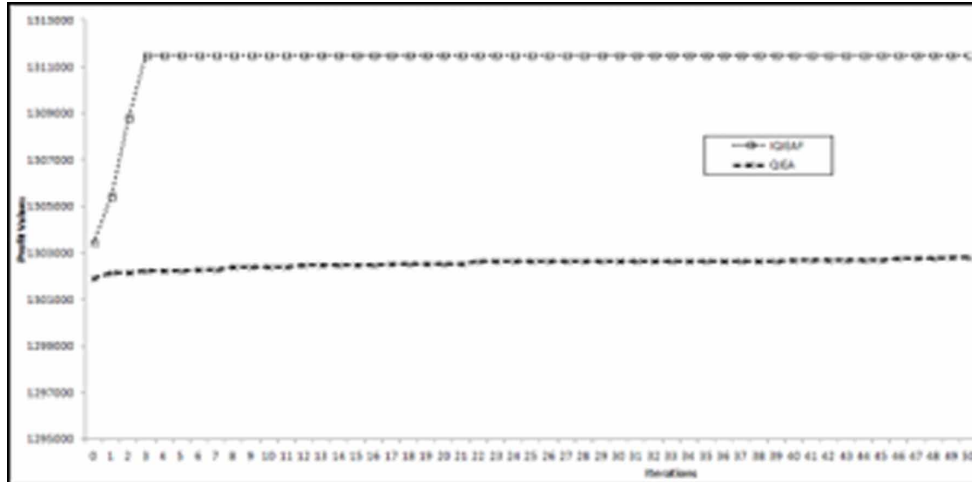
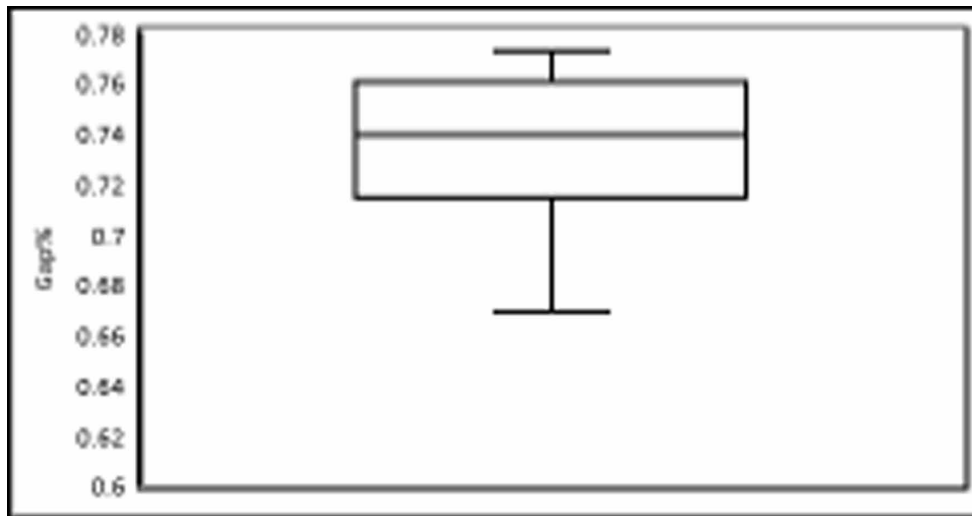


Figure 15. Box plot for Gap% between average values per instance over 30 runs obtained from QIEA to those obtained with GPQIEA for MKP



It is clear from Figure 14 that:

- GPQIEA is able to initialize the solution with better values than QIEA due to better initialization;
- Moreover, during the evolution GPQIEA finds significantly better solutions within a few iterations of the main loop of the algorithm. GPQIEA shows little modification in the values attained after these initial iterations;
- Even after 50 iterations of the main loop, QIEA is still far away from the value achieved using GPQIEA in a few iterations.

Figure 16. Box plot for average std dev. per instance over 30 runs in values obtained from QIEA

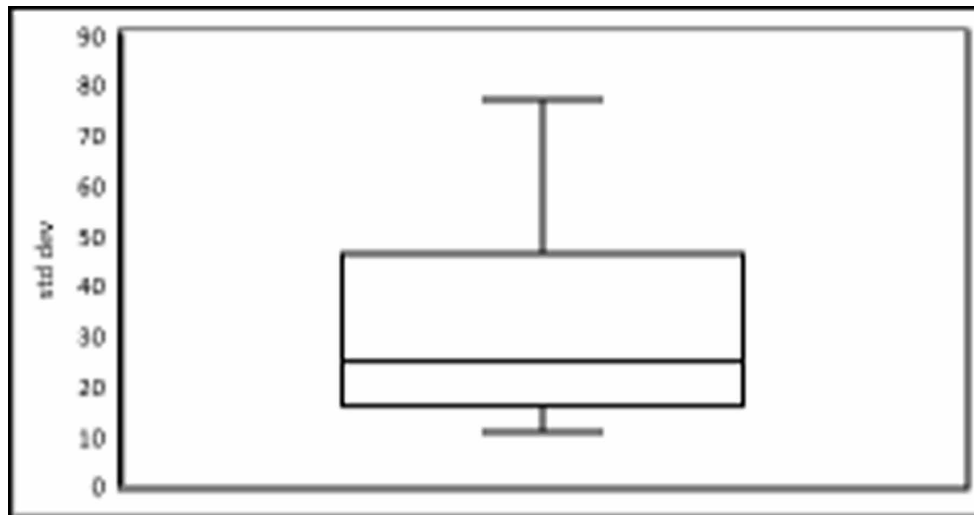
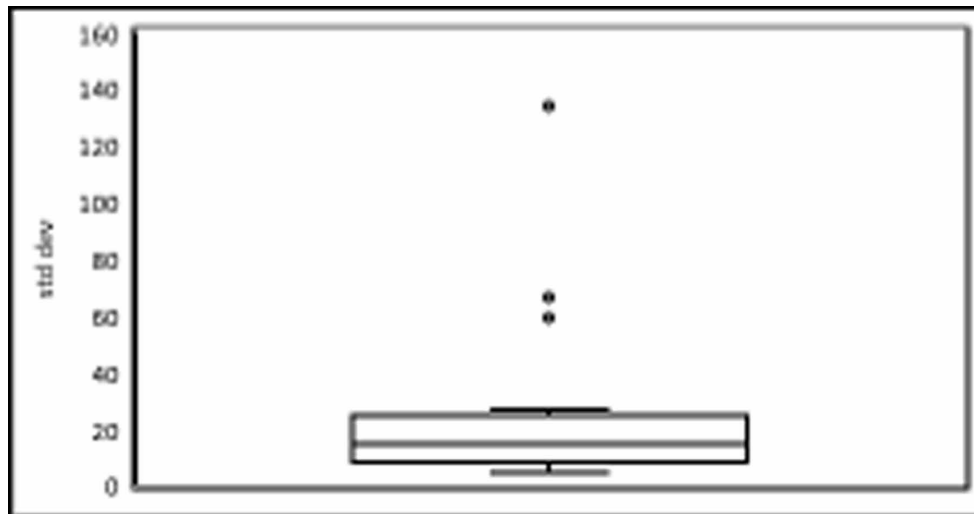


Figure 17. Box plot for average std dev. per instance over 30 runs in values obtained from GPQIEA



30 runs are performed for each instance using each strategy. The box plots have been used here to show comparison of comprehensive performance of QIEA and GPQIEA. Figure 15 presents a comparison on percentage of gap of average values obtained over 30 runs using QIEA from those obtained using GPQIEA. Figures 16 and 17 show a comparison of average std dev in values from QIEA and GPQIEA. Figures 18 and 19 show comparison of average FES by QIEA and GPQIEA.ng different classes of capacities considered.

Figure 18. Box plot for average FES per instance over 30 runs by QIEA

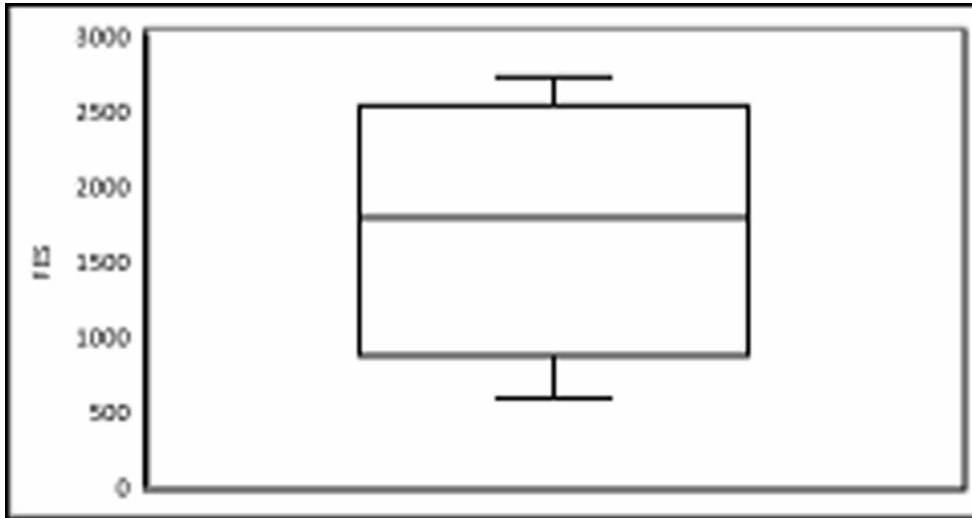
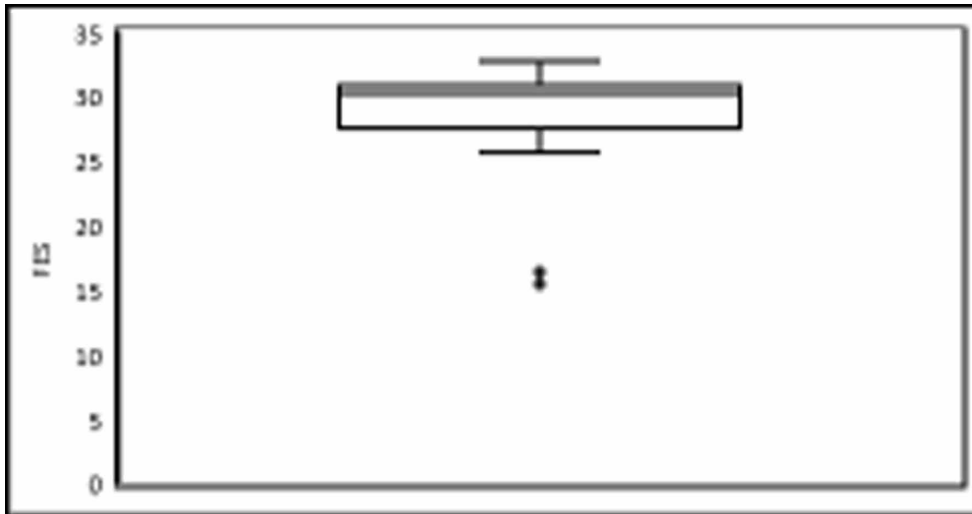


Figure 19. Box plot for average FES per instance over 30 runs by GPQIEA



The following points are observed from the results:

- GPQIEA shows considerable improvement in quality of solutions obtained as compared to QIEA;
- GPQIEA shows significant improvement in computational effort required to reach the best as compared to QIEA.

The GPQIEA is able to provide much better solutions within very less number of FES as compared to the QIEA used as the base. A parallel implementation of GPQIEA has also been used to solve large instances of MKP providing good solutions where QIEA could not even be implemented to execute within practical time limits.

4. CONCLUSION AND FUTURE WORK

A generalized framework is proposed based a prominent meta-heuristic approach, QIEAs. The proposed framework, GPQIEA, is applied for the solution of some different SSPs focusing on to provide the possibility to incorporate as many features as necessary for the effective solution of the problem at hand. It is demonstrated and verified using benchmark instances GPQIEA is applicable and effective for many different SSPs namely Difficult Knapsack Problem (DKP), Quadratic Knapsack Problem (QKP) and Multiple Knapsack Problem (MKP).

The GPQIEA can be effectively implemented on multi-core environment. This provides possibility to scale the algorithm up in order to solve larger and more complex problems within reasonable execution time.

Some areas for further work are as follows:

1. This framework may further be enhanced to solve other types of optimization problems;
2. Possibility for theoretical analysis of GPQIEA may also be explored;
3. Possibility of designing such an algorithm which chooses features adaptively based on the problem at hand may be explored;
4. Development of generalized frameworks based on other population based random search techniques than QIEA can be explored on similar lines.

REFERENCES

- Arpaia, P., Maisto, D., & Manna, C. (2011). A Quantum-inspired Evolutionary Algorithm with a competitive variation operator for Multiple-Fault Diagnosis. *Applied Soft Computing*, 11(8), 4655–4666. doi:10.1016/j.asoc.2011.07.017
- Azad, M. A., Rocha, M. A., & Fernandes, E. M. (2013). A simplified binary artificial fish swarm algorithm for 0-1 quadratic knapsack problems. *Journal of Computational and Applied Mathematics*. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0377042713005074>
- Bäck, T., Fogel, D., & Michalewicz, Z. (1997a). *Handbook of Evolutionary Computation*. Oxford Univ. Press. doi:10.1887/0750308958
- Bäck, T., Hammel, U., & Schwefel, H.-P. (1997b). Evolutionary Computation: Comments on the History and Current State. *IEEE Transactions on Evolutionary Computation*, 1(1), 3–16. doi:10.1109/4235.585888
- Balas, E., & Zemel, E. (1980). An algorithm for large zero-one knapsack problems. *Operations Research*, 28(5), 1130–1154. doi:10.1287/opre.28.5.1130
- Bansal, J. C., & Deep, K. (2012). A Modified Binary Particle Swarm Optimization for Knapsack Problems. *Applied Mathematics and Computation*, 218(22), 11042–11061. doi:10.1016/j.amc.2012.05.001
- Billionet, A., & Soutif, E. (2004a). An exact method based on Lagrangian decomposition for the 0-1 quadratic knapsack problem. *European Journal of Operational Research*, 157(3), 565–575. doi:10.1016/S0377-2217(03)00244-3

Billionet, A., & Soutif, E. (2004b). *QKP Instances*. Retrieved from <http://cedric.cnam.fr/~soutif/QKP/QKP.html>

Boyer, V., Baz, D. E., & Elkihel, M. (2012). Solving knapsack problems on GPU. *Computers & Operations Research*, 39(1), 42–47. doi:10.1016/j.cor.2011.03.014

Caprara, A., Pisinger, D., & Toth, P. (1999). Exact Solution of the Quadratic Knapsack Problem. *INFORMS Journal on Computing*, 11(2), 125–137. doi:10.1287/ijoc.11.2.125

Chekuri, C., & Khanna, S. (2006). A PTAS for the multiple knapsack problem. *SIAM Journal on Computing*, 35, 713–728. doi:10.1137/S0097539700382820

Ezziane, Z. (2002). Solving the 0/1 knapsack problem using an adaptive genetic algorithm. *Artificial Intelligence for Engineering Design, Analysis and Manufacturing*, 16(1), 23–30. doi:10.1017/S0890060401020030

Fayard, D., & Plateau, G. (1975). Resolution of the 0-1 knapsack problem. *Comparison of methods. Mathematical Programming*, 8(1), 272–307. doi:10.1007/BF01580448

Fomeni, F. D., & Letchford, A. N. (2012). *A Dynamic Programming Heuristic for the Quadratic Knapsack Problem*. Retrieved from http://www.optimization-online.org/DB_HTML/2012/03/3392.html

Goldberg, D. E. (1989). *Genetic algorithms in search, optimization and machine learning*. Boston, MA, USA: Addison-Wiley Longman Publishing Co.

Hammer, P. L., & Rader, D. J. (1997). Efficient Methods for solving quadratic 0-1 knapsack problem. *INFOR*, 35, 179–182.

Han, K., & Kim, J. (2003). On setting the parameters of quantum-inspired evolutionary algorithm for practical application. In *Proc. CEC* (Vol. 1, pp. 178-194). Academic Press.

Han, K., & Kim, J. (2004). Quantum-inspired evolutionary algorithms with a new termination criterion, h-epsilon gate, and two-phase scheme. *IEEE Transactions on Evolutionary Computation*, 8(2), 156–169. doi:10.1109/TEVC.2004.823467

Han, K., Park, K., Lee, C., & Kim, J. (2001). Parallel quantum-inspired genetic algorithm for combinatorial optimization problem. In *Proc. CEC* (Vol. 2, pp. 1422-1429). Academic Press.

Han, K.-H. (2006). On the Analysis of the Quantum-inspired Evolutionary Algorithm with a Single Individual. In *Proceedings of the IEEE Congress on Evolutionary Computation*, Vancouver, Canada (pp. 2622-2629). 10.1109/CEC.2006.1688636

Han, K.-H., & Kim, J.-H. (2002, December). Quantum-Inspired Evolutionary Algorithm for a Class of Combinatorial Optimization. *IEEE Transactions on Evolutionary Computation*, 6(6), 580–593. doi:10.1109/TEVC.2002.804320

Hey, T. (1999). Quantum computing: An introduction. *Computing & Control Engineering Journal*, 10(3), 105–112. doi:10.1049/cce:19990303

Hung, M. S., & Fisk, J. C. (1978). An algorithm for the 0-1 multiple knapsack problems. *Naval Research Logistics Quarterly*, 24(3), 571–579. doi:10.1002/nav.3800250316

- Imabeppu, T., Nakayama, S., & Ono, S. (2008). A study on a quantum-inspired evolutionary algorithm based on pair swap. *Artificial Life and Robotics*, 12(1-2), 148–152. doi:10.1007/10015-007-0457-5
- Jansen, K. (2009). Parameterized approximation scheme for the multiple knapsack problem. *SIAM Journal on Computing*, 39(4), 665–674.
- Jansen, K. (2012). A fast approximation scheme for the multiple knapsack problem. In M. Bieliková, G. Friedrich, G. Gottlob, S. Katzenbeisser, & G. Turán (Ed.), *38th Conference on Current Trends in Theory and Practice of Computer Science* (pp. 313-324). Springer. 10.1007/978-3-642-27660-6_26
- Julstrom, B. A. (2005). Greedy, genetic and greedy genetic algorithms for the quadratic knapsack problem. In *Genetic and evolutionary computation conference* (pp. 607-614). ACM.
- Kim, Y., Kim, J. H., & Han, K. H. (2006). Quantum-inspired multiobjective evolutionary algorithm for multiobjective 0/1 knapsack problems. In *Proc. CEC* (pp. 2601-2606). Academic Press.
- Kliemann, L., Kliemann, O., Patvardhan, C., Sauerland, V., & Srivastav, A. (2013). A New QEA Computing Near-Optimal Low-Discrepancy Colorings in the Hypergraph of Arithmetic Progressions. *SEA, 2013*, 67–78.
- Konar, D., Bhattacharya, S., Sharma, K., & Pradhan, S. R. (2017). An Improved Hybrid Quantum-Inspired Genetic Algorithm (HQIGA) or Scheduling of Real-Time Task in Multiprocessor. *Applied Soft Computing*, 53, 296–307. doi:10.1016/j.asoc.2016.12.051
- Lalami, M. E., Elkihel, M., Baz, D. E., & Boyer, V. (2012). A procedure-based heuristic for 0–1 Multiple Knapsack Problems. *International Journal of Mathematics in Operational Research*, 4(3), 214–224. doi:10.1504/IJMOR.2012.046684
- Létocart, L., Nagih, A., & Plateau, G. (2012). Reoptimization in Lagrangian methods for the 0-1 quadratic knapsack problem. *Computers & Operations Research*, 39(1), 12–18. doi:10.1016/j.cor.2010.10.027
- Li, Y., Zhang, Y., Cheng, Y., Jiang, X., & Zhao, R. (2005, August). A novel immune quantum-inspired genetic algorithm. In *Proceedings of the International Conference on Natural Computation* (pp. 215-218). Springer. doi:10.1007/11539902_25
- Lu, T.-C., & Yu, G.-R. (2013). An adaptive population multi-objective quantum-inspired evolutionary algorithm for multi-objective 0/1 knapsack problems. *Information Sciences*, 243, 39–56. doi:10.1016/j.ins.2013.04.018
- Mahdabi, P., Jalili, S., & Abadi, M. (2008). A multi-start quantum-inspired evolutionary algorithm for solving combinatorial optimization problems. In *Proceedings of the 10th annual conference on Genetic and evolutionary computation (GECCO '08)* (pp. 613-614).
- Mani, A., & Patvardhan, C. (2010). A Hybrid quantum evolutionary algorithm for solving engineering optimization problems. *International Journal of Hybrid Intelligent Systems*, 7(3), 225–235. doi:10.3233/HIS-2010-0115
- Martello, S., & Toth, P. (1977). An upper bound for the zero-one knapsack problem and a branch and bound algorithm. *European Journal of Operational Research*, 1(3), 169–175. doi:10.1016/0377-2217(77)90024-8

- Martello, S., & Toth, P. (1980). Solution of the zero-one multiple knapsack problem. *European Journal of Operational Research*, 4(4), 276–283. doi:10.1016/0377-2217(80)90112-5
- Martello, S., & Toth, P. (1981). A bound and bound algorithm for the zero-one multiple knapsack problem. *Discrete Applied Mathematics*, 3(4), 275–288. doi:10.1016/0166-218X(81)90005-6
- Martello, S., & Toth, P. (1988). A new algorithm for the 0-1 knapsack problem. *Management Science*, 34(5), 633–644. doi:10.1287/mnsc.34.5.633
- Martello, S., & Toth, P. (1990). *Knapsack Problems: Algorithms and Computer Implementations*. Chichester, UK: Wiley.
- Martello, S., Pisinger, D., & Paolo, T. (2000). New trends in exact algorithms for the 0-1 knapsack problem. *European Journal of Operational Research*, 123(2), 325–332. doi:10.1016/S0377-2217(99)00260-X
- Martello, S., Pisinger, D., & Toth, P. (1999, March). Dynamic Programming and Strong Bounds for the 0-1 Knapsack Problem. *Management Science*, 45(3), 414–424. doi:10.1287/mnsc.45.3.414
- Mitchell, M. (1996). *An Introduction to Genetic Algorithms*. USA: The MIT Press.
- Mohanty, S. N., & Satapathy, R. (2009). An evolutionary multiobjective genetic algorithm to solve 0/1 Knapsack Problem. In *Proceedings of the 2nd IEEE International Conference on Computer Science and Information Technology, ICCSIT 2009* (pp. 397-399). 10.1109/ICCSIT.2009.5234668
- Narayanan, A., & Moore, M. (1996). Quantum-inspired genetic algorithms. In *Proc. CEC* (pp. 61-66). Academic Press.
- Nowotniak, R., & Kucharski, J. (2012). GPU-based tuning of quantum-inspired genetic algorithm for a combinatorial optimization problem. *Bulletin of the Polish Academy of Sciences. Technical Sciences*, 60(2), 323–330. doi:10.2478/v10175-012-0043-4
- Patvardhan, C., Narayan, A., & Srivastav, A. (2007). Enhanced Quantum Evolutionary Algorithms for Difficult Knapsack Problems. In *Proceedings of the 2nd international conference on Pattern recognition and machine intelligence PReMI'07* (pp. 252-260). Springer-Verlag Berlin.
- Patvardhan, C., Prakash, P., & Srivastav, A. (2012). A novel quantum-inspired evolutionary algorithm for the quadratic knapsack problem. *Int. J. Mathematics in Operational Research*, 4(2), 114–127. doi:10.1504/IJMOR.2012.046373
- Pelikan, M., Goldberg, D., & Lobo, F. (1999). *A survey of optimization by building and using probabilistic model*. IlliGAL.
- Pisinger, D. (1995). *Algorithms for Knapsack Problems*.
- Pisinger, D. (1995). An expanding-core algorithm for the exact 0-1 knapsack problem. *European Journal of Operational Research*, 87(1), 175–187. doi:10.1016/0377-2217(94)00013-3
- Pisinger, D. (1997). A minimal algorithm for the 0-1 knapsack problem. *Operations Research*, 45(5), 758–767. doi:10.1287/opre.45.5.758
- Pisinger, D. (1999, May). An exact algorithm for large multiple knapsack problems. *European Journal of Operational Research*, 114(3), 528–541. doi:10.1016/S0377-2217(98)00120-9

Pisinger, D. (2005). Where are the Hard Knapsack Problems. *Computers & Operations Research*, 32(5), 2271–2284. doi:10.1016/j.cor.2004.03.002

Pisinger, D. (2007). The quadratic knapsack problem - a survey. *Discrete Applied Mathematics*, 155(5), 623–648. doi:10.1016/j.dam.2006.08.007

Pisinger, W. D., Ramussen, A. B., & Sandvik, R. (2007). Solution of Large Quadratic Knapsack Problems Through Aggressive Reduction. *INFORMS Journal on Computing*, 19(2), 280–290. doi:10.1287/ijoc.1050.0172

Platel, M. D., Schliebs, S., & Kasabov, N. (2007). A versatile quantum-inspired evolutionary algorithm. In *Proc. CEC* (pp. 423-430). Academic Press.

Platel, M. D., Schliebs, S., & Kasabov, N. (2009). Quantum-Inspired Evolutionary Algorithm: A Multimodel EDA. *IEEE Transactions on Evolutionary Computation*, 13(6), 1218–1232. doi:10.1109/TEVC.2008.2003010

Pulikanti, S., & Singh, A. (2009, December). An artificial bee colony algorithm for the quadratic knapsack problem. In *Proceedings of the International Conference on Neural Information Processing* (pp. 196-205). Springer.

Qin, Y., Zhang, G., Li, Y., & Zhang, H. (2011, December). A comprehensive learning quantum-inspired evolutionary algorithm. In *Proceedings of the International Conference on Information and Business Intelligence* (pp. 151-157). Springer.

Reilly, C. H. (2009). Synthetic Optimization Problem Generation: Show Us the Correlations! *INFORMS Journal on Computing*, 21(3), 458–467. doi:10.1287/ijoc.1090.0330

Sailesh Babu, G. S., Bhagwan Das, D., & Patvardhan, C. (2008). Real-Parameter quantum evolutionary algorithm for economic load dispatch. *IET Generation, Transmission & Distribution*, 2(1), 22–31. doi:10.1049/iet-gtd:20060495

Tayarani-N, M.-H., & Akbarzadeh-T, M.-R. (2008). A Sinusoid Size Ring Structure Quantum Evolutionary Algorithm. In *Proceedings of the IEEE Conference on Cybernetics and Intelligent Systems*, (pp. 1165-1170). 10.1109/ICCIS.2008.4670952

Wang, L., & Li, L. (2010). An effective hybrid quantum-inspired evolutionary algorithm for parameter estimation of chaotic systems. *Expert Systems with Applications*, 37(2), 1279–1285. doi:10.1016/j.eswa.2009.06.013

Wang, Y., Feng, X. Y., Huang, Y. X., Zhou, W. G., Liang, Y. C., & Zhou, C. G. (2005). A novel quantum swarm evolutionary algorithm for solving 0-1 knapsack problem. *Lecture Notes in Computer Science*, 3611, 698–704. doi:10.1007/11539117_99

Wolpert, D. H., & Macready, W. G. (1997). No free lunch theorems for optimization. *IEEE Transactions on Evolutionary Computation*, 1(1), 67–82. doi:10.1109/4235.585893

Xiao, J., Yan, Y., Zhang, J., & Tang, Y. (2010). A quantum-inspired genetic algorithm for k-means clustering. *Expert Systems with Applications*, 37(7), 4966–4973. doi:10.1016/j.eswa.2009.12.017

- Xie, X., & Liu, J. (2007). A Mini-Swarm for the quadratic knapsack problem. In *Proceedings of the IEEE Swarm Intelligence Symposium*, Honolulu, HI (pp. 190-197). Academic Press. 10.1109/SIS.2007.368045
- Yang, S. Y., Wang, M., & Jiao, L. C. (2004a). A novel quantum evolutionary algorithm and its application. In *Proc CEC* (pp. 820-826). Academic Press.
- Yang, Z., Wang, G., & Chu, F. (2013). An effective GRASP and tabu search for the 0-1 quadratic knapsack problem. *Computers & Operations Research*, 40(5), 1176–1185. doi:10.1016/j.cor.2012.11.023
- Zhang, G. (2011). Quantum-inspired evolutionary algorithms: A survey and empirical study. *Journal of Heuristics*, 17(3), 303–351. doi:10.1007/10732-010-9136-0
- Zhang, G., & Rong, H. (2007, May). Parameter setting of quantum-inspired genetic algorithm based on real observation. In *Proceedings of the International Conference on Rough Sets and Knowledge Technology* (pp. 492-499). Springer.
- Zhang, G., Gheorghe, M., & Wu, C. (2008). A quantum-inspired evolutionary algorithm based on p systems for knapsack problem. *Fundamenta Informaticae*, 87(1), 93–116.
- Zhang, G., Li, N., Jin, W., & Hu, L. (2006). Novel quantum genetic algorithm and its applications. *Frontiers of Electrical and Electronic Engineering in China*, 1(1), 31–36. doi:10.1007/11460-005-0014-8
- Zhang, H., Zhang, G., Rong, H., & Cheng, J. (2010). Comparisons of Quantum Rotation gates in Quantum-Inspired Evolutionary Algorithms. In *Proceedings of the Sixth International Conference on Natural Computation (ICNC 2010)*, Hiroshima, Japan. Academic Press. 10.1109/ICNC.2010.5584179
- Zhang, R., & Gao, H. (2007). Improved quantum evolutionary algorithm for combinatorial optimization problem. In *Proc. ICMLC* (pp. 3501-3505). Academic Press. 10.1109/ICMLC.2007.4370753
- Zhao, Z., Peng, X., Peng, Y., & Yu, E. (2006). An Effective Repair Procedure based on Quantum-inspired Evolutionary Algorithm for 0/1 Knapsack Problems. In *Proceedings of the 5th WSEAS Int. Conf. on Instrumentation, Measurement, Circuits and Systems*, Hangzhou, China (pp. 203-206). Academic Press.
- Zhou, A., Qu, B. Y., Li, H., Zhao, S. Z., Suganthan, P. N., & Zhang, Q. (2011). Multiobjective evolutionary algorithms: A survey of the state of the art. *Swarm and Evolutionary Computation*, 1(1), 32–49. doi:10.1016/j.swevo.2011.03.001
- Zhou, S., & Sun, Z. (2005). A new approach belonging to EDAs: Quantum-inspired genetic algorithm with only one chromosome. In *Proc. ICNC* (Vol. 3, pp. 141–150). Academic Press. 10.1007/11539902_17

ENDNOTE

¹ <http://www.diku.dk/~pisinger/codes.html>

Chapter 4

Quantum–Behaved Bat Algorithm for Solving the Economic Load Dispatch Problem Considering a Valve–Point Effect

Pandian Vasant

 <https://orcid.org/0000-0002-0755-1046>

Department of Fundamental and Applied Sciences, Universiti Teknologi PETRONAS, Seri Iskandar, Malaysia

Igor Litvinchev

 <https://orcid.org/0000-0002-1850-4755>

Nuevo Leon State University, San Nicolás de los Garza, Mexico

Roman Rodriguez Aguilar

Universidad Panamericana, Escuela de Ciencias Económicas y Empresariales, Ciudad de México, Mexico

Fahad Parvez Mahdi

 <https://orcid.org/0000-0002-0081-7358>

University of Hyogo, Kobe, Japan

Jose Antonio Marmolejo-Saucedo

Universidad Panamericana, Facultad de Ingeniería, Ciudad de México, Mexico

Junzo Watada

Universiti Teknologi Petronas, Seri Iskandar, Malaysia

ABSTRACT

Quantum computing-inspired metaheuristic algorithms have emerged as a powerful computational tool to solve nonlinear optimization problems. In this paper, a quantum-behaved bat algorithm (QBA) is implemented to solve a nonlinear economic load dispatch (ELD) problem. The objective of ELD is to find an optimal combination of power generating units in order to minimize total fuel cost of the system, while satisfying all other constraints. To make the system more applicable to the real-world problem, a valve-point effect is considered here with the ELD problem. QBA is applied in 3-unit, 10-unit, and 40-unit power generation systems for different load demands. The obtained result is then presented and compared with some well-known methods from the literature such as different versions of evolutionary

DOI: 10.4018/978-1-7998-8593-1.ch004

programming (EP) and particle swarm optimization (PSO), genetic algorithm (GA), differential evolution (DE), simulated annealing (SA) and hybrid ABC_PSO. The comparison of results shows that QBA performs better than the above-mentioned methods in terms of solution quality, convergence characteristics and computational efficiency. Thus, QBA proves to be an effective and a robust technique to solve such nonlinear optimization problem.

INTRODUCTION

Thermal plants mainly utilize fossil fuels like coal, gas and oil to generate electricity. Capacity to deliver fossil fuels as per their growing demand is very much limited due to the shortage of fossil fuel supply and lack of adequate infrastructures (Mahdi, Vasant, Kallimani, & Abdullah-Al-Wadud, 2016). Moreover, fossil fuels are not always easily accessible to all as the reserves of the fossil fuels are concentrating into a small number of countries. Furthermore, the reserves of the fossil fuels are declining and it will be distinct and too expensive in near future. Thus, economic load dispatch (ELD) plays one of the most crucial parts in electrical power generation system. ELD deals with the minimization of fuel cost, while satisfying all other constraints (Wood & Wollenberg, 2012). The simplification of traditional ELD problem fails to offer satisfactory results in real-world system as they consider that the efficiency of power plant increases linearly or quadratically. However, in real-world system separate nozzle groups help the valves to control the steam entering the turbine. The system tries to achieve its highest efficiency by activating the valves in a sequential way and thus resulting a rippled efficiency curve. This phenomenon is known as valve-point effect. In this research, valve-point effect is considered as a practical operation constraint of generator. Considering valve-point effect helps to model ELD problem more accurately and closer to actual power generation system at the cost of adding extra complexities in the system.

Traditional methods like Newton-Raphson (Lin, Chen, & Huang, 1992), linear and nonlinear programming techniques (Momoh, El-Hawary, & Adapa, 1999) were used to solve ELD problem, where the ELD problem is represented using linear quadratic function. They proved to be fast and reliable against linear ELD problem. But, when considering the nonlinear characteristics of power system like consideration of valve-point effect, the traditional methods were proved to be ineffective and inefficient (Chen & Wang, 1993). They are prone to trap into the local optima and have sensitivity to the initial point (Mahdi, Vasant, Kallimani, Watada, et al., 2017).

Different heuristic and metaheuristic techniques have later used to overcome the shortcomings of the traditional methods to solve nonlinear ELD problem. Genetic algorithm (GA) (Walters & Sheble, 1993), simulated annealing (SA) (Wong & Fung, 1993), evolutionary programming (EP) (Yang, Yang, & Huang, 1996), tabu search (TS) (Lin, Cheng, & Tsay, 2002), enhanced Lagrangian artificial neural network (ELANN) (S. C. Lee & Kim, 2002), generalized ant colony optimization (GACO) (Hou, Wu, Lu, & Xiong, 2002), improved fast evolutionary program (IFEP) (Chakrabati, Choudhury, Chattopadhyay, Sinha, & Ravi, 2003), particle swarm optimization (PSO) (Park, Lee, Shin, & Lee, 2005), pattern search (PS) method (Al-Sumait, Al-Othman, & Sykulski, 2007), Biogeography based optimization (BBO) (Roy, Ghoshal, & Thakur, 2009), improved harmony search (IHS) (Coelho & Mariani, 2009b), chaotic artificial immune network (CAIN) (Coelho & Mariani, 2009a), bat algorithm (BA) (Sakthivel, Natarajan, & Gurusamy, 2013), chaotic teaching-learning-based optimization with Lévy flight (CTLBO) (X. He, Rao, & Huang, 2016) and swarm based mean-variance mapping optimization (MVMOS) (Khoa,

Vasant, Singh, & Dieu, 2017) are some of the techniques used for solving nonlinear ELD problem. These methods can provide global or near global solutions (Meng, Wang, Dong, & Wong, 2010). However, they cannot always guarantee finding global solutions in finite computational time and many problem specific parameters to tune.

Researchers propose and develop hybrid methods to avoid the problems found in the conventional and stand-alone heuristic/metaheuristic methods. They start with PSO-EP (Sinha & Purkayastha, 2004), PSO-sequential QP (SQP) (Victoire & Jeyakumar, 2005), chaotic differential evolution (CDE)-quadratic programming (QP) (dos Santos Coelho & Mariani, 2006), GA-SQP (He, Wang, & Mao, 2008), chaotic PSO-implicit filtering local search (IFLS) method (Coelho & Mariani, 2009c), variable scaling hybrid differential evolution (VSHDE) (Chiou, 2009), GA-PSO (Jiang, Xu, Gong, & Chen, 2009) and GA-PS-SQP (Alsumait, Sykulski, & Al-Othman, 2010), and finished with fuzzy adaptive PSO-Nelder Mead (FAPSO-NM) (Niknam, 2010), cultural algorithm- self-organizing migrating algorithm (CSOMA) (L. D. S. Coelho & Mariani, 2010), interior point method (IPM)-DE (Duvvuru & Swarup, 2011), a hybrid particle swarm optimization with time-varying acceleration coefficients- bacteria foraging algorithm (HPSOTVAC-BFA) (Abedinia, Amjady, Ghasemi, & Hejrati, 2013), hybrid grey wolf optimizer (HGWO) (Jayabarathi, Raghunathan, Adarsh, & Suganthan, 2016) and hybrid Big Bang-Big Crunch Algorithm (HBB-BC) (Shahinzadeh, Fathi, Moazzami, & Hosseinian, 2017). Hybrid methods are quite successful than stand-alone metaheuristic techniques to achieve global solutions. However, they often add complexities in the algorithm with long computational time, which make them computationally inefficient and hard to implement.

The use of quantum computing (QC) inspired metaheuristic techniques is popular current trend to solve optimal power dispatch problem. They provide excellent strategy to solve nonlinear and nonconvex optimization problem in a very fast and efficient way. Quantum inspired evolutionary algorithm (QEA) (Vlachogiannis & Lee, 2008), quantum inspired GA (QGA) (Lee, Lin, Liao, & Tsao, 2011) and quantum inspired PSO (QPSO) (Meng et al., 2010) are so far used to solve ELD problem. Meng et al. (Meng et al., 2010) in their research showed that QPSO successfully outperformed different versions of EP and PSO techniques. The use of quantum inspired methods in similar power dispatch problem is addressed in (Mahdi et al., 2016; Mahdi, Vasant, Kallimani, Abdullah-Al-Wadud, & Watada, 2017).

In this paper, a novel approach is followed using quantum-behaved bat algorithm (QBA) to solve ELD problem considering valve-point effect. QBA is a modified and upgraded version of BA. It considers the behavior of bat in a structured way and thus, effectively overcome the limitations of the original BA. QBA is found to produce better results than its predecessors PSO and GA. The main contribution of this paper is to investigate the feasibility of using recent advanced quantum computing powered technique like bat algorithm in solving nonlinear optimization problem like ELD with valve-point effect. QBA is applied to three different kind of systems with different load demands to assess the possibility of using such technique in real-world scenario. This research also tries to answer the effectiveness of QBA in handling power generation system of different sizes and load demands. The next section presents the mathematical formulation of ELD considering valve-point effect. Methodology section provides brief description on BA and QBA algorithms with necessary equations and pseudo code. Result and analysis section shows the obtained simulation results with comparison and short analysis. Finally, the paper is concluded with conclusion section that describes the gist of the paper with some future research directions.

PROBLEM FORMULATION

The main objective of ELD problem is to find an optimal combination of power generation in order to minimize the total fuel cost of the system, while satisfying all other constraints. ELD is considered here as a nonlinear single objective optimization problem. It can be represented using quadratic function as below:

$$F(P) = \sum_{i=1}^n a_i P_i^2 + b_i P_i + c_i \quad (1)$$

where:

$F(P)$ = fuel cost function (in \$)

n = total number of generating units

P_i = real output power of i^{th} generating unit

$a_i, b_i,$ and c_i = cost coefficients of the generating unit i

A rippling effect is produced in the heat rate function (Abdullah, Bakar, Rahim, Jamian, & Aman, 2012), when steam valves in a turbine of thermal generator start to open. This rippling effect makes the cost function highly nonlinear. This is known as a valve-point effect. In this research, valve-point effect is considered, which makes the model closer to the actual power generation system, while making the cost function highly nonlinear and complex. The ELD problem with valve-point effect can be written as:

$$F(P) = \sum_{i=1}^n a_i P_i^2 + b_i P_i + c_i + \left| d_i \times \sin \left(e_i \times \left(P_{i,\min} \right) \right) \right| \quad (2)$$

where:

d_i and e_i = fuel cost coefficients of i^{th} generating unit with valve-point effect

$P_{i,\min}$ = minimum power output of generating unit i

Two constraints i.e. power balance constraints and generation limit constraints have been considered in this research. The constraints are given below:

$$\begin{aligned} P &= \sum_{i=1}^n P_i = P_D + P_L \\ P_L &= \sum_{i=1}^N \sum_{j=1}^N P_{gi} B_{ij} P_{gj} \end{aligned} \quad (3)$$

Quantum-Behaved Bat Algorithm for Solving the Economic Load Dispatch Problem

$$P_{i,min} \leq P_i \leq P_{i,max} \quad (4)$$

where:

P = total generated power (in MW) in all generating units

P_D = total power demand (in MW)

P_L = total loss (in MW)

B_{ij} = a square matrix that is also known as a transmission loss coefficient

$P_{i,max}$ = maximum power output of generating unit i

METHODOLOGY

QBA is an extension of BA into the domain of quantum computing. BA is relatively a new nature-inspired metaheuristic algorithm based on the echolocation characteristics of bats. BA shows better performance than most other heuristic algorithms like GA and PSO (Yang, 2010). It utilizes the major advantages of its predecessor i.e. GA and PSO in a structured way (Yang & Hossein Gandomi, 2012).

The original BA is based on three idealized rules: (i) echolocation technique of bats to sense distance and to calculate difference between their prey and background barriers; (ii) bats vary their wavelength (λ_0) and loudness (A_0) to search for their prey. They also regulate frequency and rate of their emitted pulses, depending on the distance of their prey; (iii) assuming that the loudness is varied from a large (A_0) value to a minimum constant value (A_{min}). The positions (x_i) and velocities (v_i) of the virtual bats are updated using the following equations:

$$f_i = f_{min} + (f_{max} - f_{min})\alpha \quad (5a)$$

$$v_i^t = v_i^{t-1} + (x_i^t - g^t) f_i \quad (5b)$$

$$x_i^t = x_i^{t-1} + v_i^t \quad (5c)$$

where:

α = random vector in the range of [0, 1]

f_i = frequency of pulse

f_{min} = minimum frequency

f_{max} = maximum frequency

v_i^t = velocity of i^{th} bat at iteration t

v_i^{t-1} = velocity of i^{th} bat at iteration $(t-1)$

x_i^t = position of i^{th} bat at iteration t

x_i^{t-1} = position of i^{th} bat at iteration $(t-1)$

g^t = current best global location found by the bats

In QBA, new position (solution) of bat is updated using the following equation:

$$\begin{aligned} x_{id}^{t+1} &= g^t \times \left[1 + j(0, \sigma^2) \right] \\ \sigma^2 &= \left| A_i^t - A^t \right| + \varepsilon \end{aligned} \tag{6}$$

where:

$j(0, \sigma^2)$ = Gaussian distribution with mean 0 and standard deviation σ^2

x_{id}^{t+1} = the position of i^{th} bat at iteration $t+1$

A^t = average loudness of all bats at iteration t

A_i^t = loudness of i^{th} bat at iteration t

ε = a constant, integrated here to ensure the standard deviation σ^2 remains positive

The loudness A_i and pulse emission rate r_i are updated in each iteration using the following equations:

$$\begin{aligned} A_i^{t+1} &= \delta A_i^t \\ r_i^{t+1} &= r_i^0 \left[1 - \exp(-\gamma t) \right] \end{aligned} \tag{7}$$

where:

A_i^t = loudness of i^{th} bat at iteration t

A_i^{t+1} = loudness of i^{th} bat at iteration $t+1$

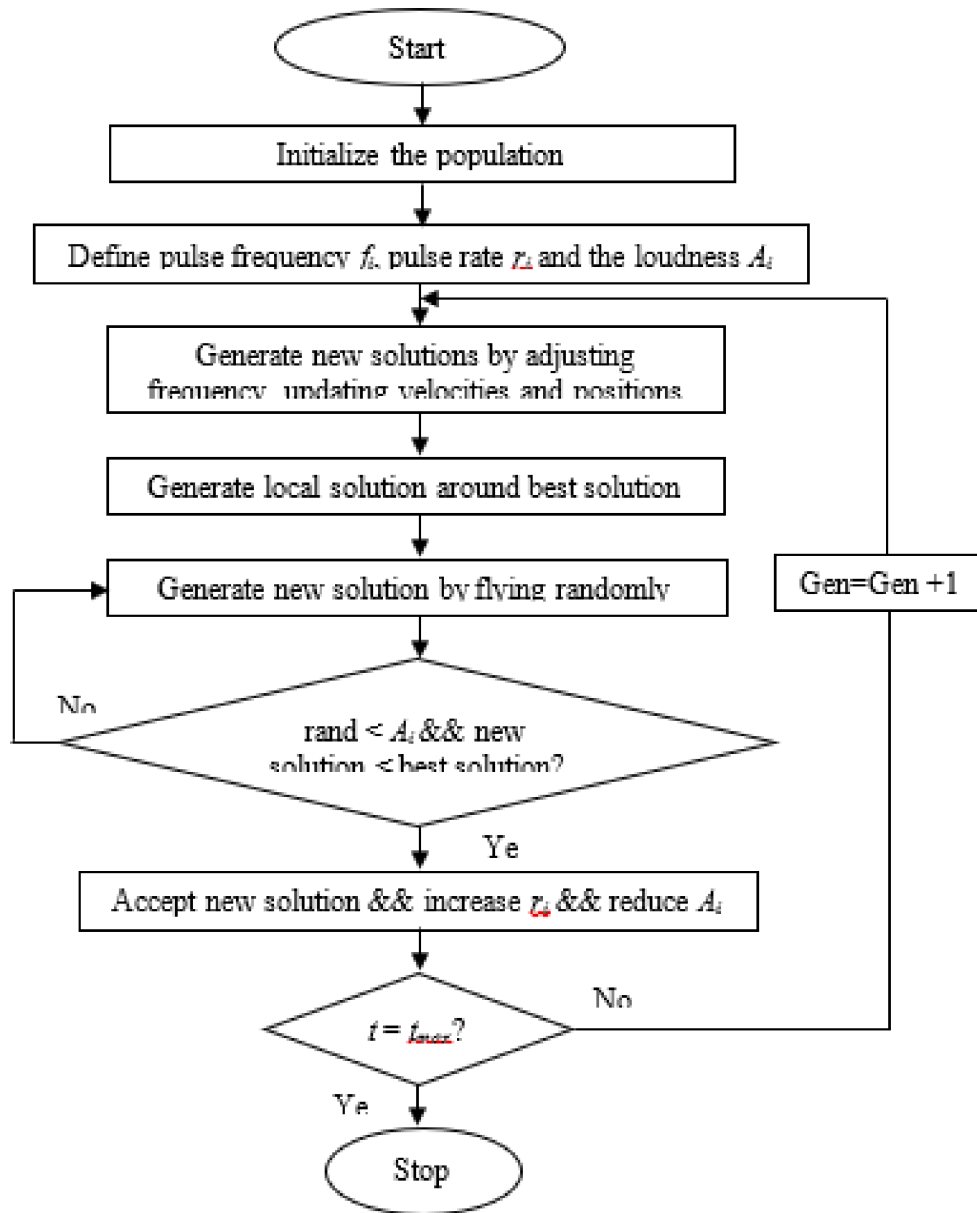
Quantum-Behaved Bat Algorithm for Solving the Economic Load Dispatch Problem

r_i^o = initial pulse emission rate of i^{th} bat

r_i^{t-1} = pulse emission rate of i^{th} bat at iteration $t+1$

δ and γ = constants whose range are $[0,1]$ and greater than 0 ($\gamma > 0$), respectively

Figure 1. Flowchart of QBA



Quantum-Behaved Bat Algorithm for Solving the Economic Load Dispatch Problem

To make the algorithm more similar to the actual scenario of bats and thus, make it more efficient, two more idealized rules have been considered along with the three idealized rules (X.-S. Yang, 2010) found in the original BA. They are: (1) bats have different foraging habitats rather than one single foraging habitat that depends on a stochastic selection, (2) bats have the self-adaptive capability to compensate for Doppler Effect in echoes. In QBA, quantum behaving virtual bats position can be defined using the equation below:

$$x_{id}^t = g_d^t + \beta |mbest_d - x_{id}^t| \ln\left(\frac{1}{u}\right), u(0,1) < 0.5 \quad (8a)$$

$$x_{id}^t = g_d^t - \beta |mbest_d - x_{id}^t| \ln\left(\frac{1}{u}\right), u(0,1) \geq 0.5 \quad (8b)$$

where:

x_{id}^t = position of i^{th} bat in dimension d at iteration t

u = random number in the range of $[0,1]$

$mbest$ = the average best location

Consideration of bats self-adaptive compensation for Doppler effect changes the updating formulas as mentioned in Equation 5. The equations can be rewritten as below:

$$f_{id} = \frac{(340 + v_i^{t-1})}{(340 + v_g^{t-1})} \times f_{id} \times \left[1 + C_i \times \frac{(g^t - x_{id}^t)}{|g^t - x_{id}^t| + \epsilon} \right] \quad (9)$$

$$v_{id}^t = (w \times v_{id}^{t-1}) + (g^t - x_{id}^t) f_{id} \quad (10)$$

$$x_{id}^t = x_{id}^{t-1} + v_{id}^t \quad (11)$$

where:

f_{id} = frequency of i^{th} bat in dimension d

v_g^{t-1} = velocity of the global best position at iteration $t-1$

C_i = positive number of i^{th} bat in the range of $[0, 1]$

Quantum-Behaved Bat Algorithm for Solving the Economic Load Dispatch Problem

For simplicity, we can assume if the value of C is 0, then bat cannot compensate for Doppler Effect in echoes and if $C=1$, it means bat can fully compensate for Doppler Effect in echoes. Inertia weight w is introduced here to update the velocity and has similar characteristics like the inertia weight found in PSO (Shi & Eberhart, 1998). Pseudo code and flowchart of QBA is given below in Algorithm 1 and Figure 1, respectively.

Algorithm 1: Quantum-Behaved Bat Algorithm

Define basic BA parameters: α , γ , f_{\min} , f_{\max} , A_0 and r_0 ;

Initialize the number of individuals (N) contained by the population, iterations (t_{\max}), probability of habitat selection (P), inertia weight (w), compensation rates for Doppler Effect in echoes (C), contraction/expansion coefficient (β), the frequency of updating the loudness and emission pulse rate (G);

Evaluation of objective function value for each individual.

```
while (iteration <  $t_{\max}$ )
if (rand(0,1) < P)
generate new solutions using equations in 8
else
generate new solutions using equations 5 and 9-11
end if
if (rand(0,1) >  $r_i$ )
generate a local solution around the selected best solution using equation 6
end if
evaluate the objective function value of each individual.
update solutions, the loudness and emission pulse rate using equations 7
rank the solutions and find the current best  $g^*$ 
if  $g^*$  does not improve in  $G$  time step.
re-initialize the loudness  $A_i$  and set temporary pulse rates  $r_i$  [0.85-0.9]
end if
t=t+1;
end while
```

RESULT AND ANALYSIS

In this paper, QBA is applied in 3-unit, 10-unit and 40-unit systems for solving ELD problem considering valve-point effect, where the load demand is 850 MW, 2000 MW and 10500 MW, respectively. All the simulations are done using MATLAB R2015a and executed with core i5-M 480 CPU @ 2.67 GHz (4 CPUs), ~2.7 GHz and 4GB RAM laptop. Table 1 shows the parameter settings of QBA for solving ELD problem. The standard parameter settings of QBA (Meng et al., 2010) is considered here. However, the population size and number of iterations are considered through trial and error method. Population size in 3-unit system does not need to be as large as 2000, rather it converges to the desired value with the population size as low as 500. However, in order to set a common parameter for all the three systems, the authors have considered population size 2000. All the data for 3-unit system are collected from (Sinha,

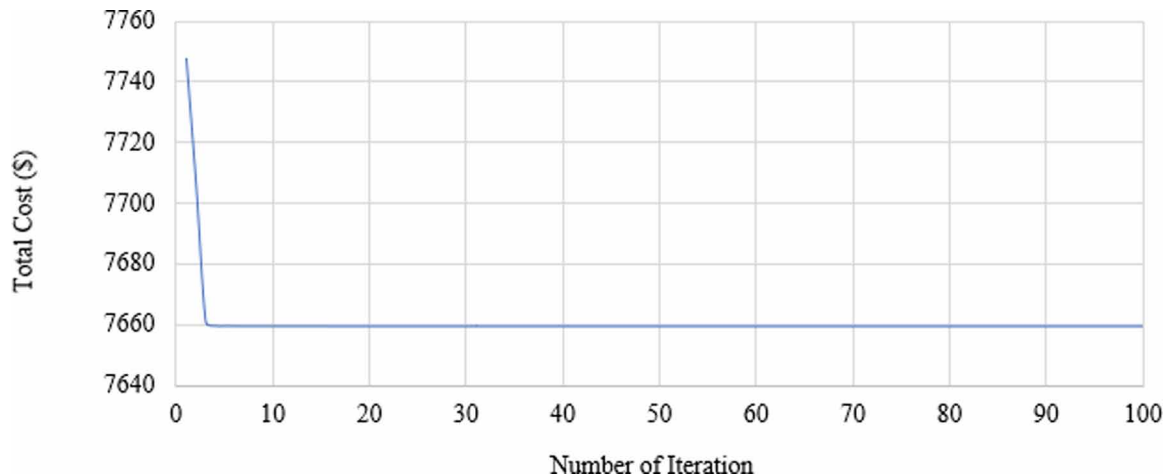
Chakrabarti, & Chattopadhyay, 2003), whereas the data for 10-unit and 40-unit systems are collected from (Basu, 2011a). A total of 30 runs are considered and the average of the runs are reported in this section.

Table 2 shows the comparative results among various types of techniques to solve ELD problem in 3-unit system considering nonlinear valve-point effect. From this table, it can be seen that the best result of QBA is much better than all other methods reported in the literature such as classical EP (CEP), fast EP (FEP), improved FEP (IFEP) (Sinha et al., 2003), fuzzy self-adaptive immune algorithm (FIA) (Meng, 2007) and QPSO (Meng et al., 2010). Again, the best average result also comes from QBA. Therefore, it can be concluded that the idea of integrating quantum-computing phenomenon with other nature inspired optimization techniques like BA provides improved and robust results. Figures 2-4 show the convergence graphs of QBA for 3, 10 and 40-unit system, respectively.

Table 1. Parameter settings of QBA for ELD problem with valve-point effect

Parameters	Values
Maximal generations (iterations)	100
Population size	2000
The maximal and minimal pulse rate	1 and 0, respectively
The maximal and minimal frequency (n_{max} and n_{min})	1.5 and 0, respectively
The maximal and minimal loudness	2 and 1, respectively
Delta, δ	0.9
Gamma, γ	0.9
The frequency of updating the loudness and emission pulse rate, G	10
The maximum and minimum probability of habitat selection	0.9 and 0.6, respectively
The maximum and minimum compensation rate for Doppler Effect (C_{max} and C_{min})	0.9 and 0.1, respectively
The maximum and minimum contraction expansion coefficient (β_{max} and β_{min})	1 and 0.5, respectively
The maximum and minimum inertia weight (w_{max} and w_{min})	0.9 and 0.5, respectively

Figure 2. Convergence graph of QBA for solving ELD problem in 3-unit system ($P_D = 850$)



Quantum-Behaved Bat Algorithm for Solving the Economic Load Dispatch Problem

Table 2. Comparison of results among different approaches to solve 3-unit ELD problem with valve-point effect

Algorithms	Best Result (\$)	Average Result (\$)
CEP	8234.07	8235.97
FEP	8234.07	8234.24
MFEP	8234.08	8234.71
IFEP	8234.07	8234.16
EGA	8234.07	8234.41
FIA	8234.07	8234.26
SPSO	8234.07	8234.18
QPSO	8234.07	8234.10
QBA	7659.29	7684.63

In the second case, QBA is applied to 10-unit power generating system. Table 3 shows the comparative results for 10-unit system among hybrid artificial bee colony-particle swarm optimization (ABC_PSO) (Mantaw & Otero, 2012), differential evolution (DE) (Basu, 2011b), simulated annealing (SA) (Ziane, Benhamida, & Graa, 2016) and QBA. The table also mention the optimized dedicated generations (in MW) in each of the generating units. The comparison of the result i.e. total cost (in \$) show that QBA outperforms other methods by calculating least amount of cost for nonlinear ELD problem. However, transmission loss is found to be little higher in QBA than SA and ABC_PSO. These two investigations confirm the feasibility of using QBA in small and medium-ranged power generating units.

Table 3. Comparison of results among different approaches to solve 10-unit ELD problem with valve-point effect

$P_D = 2000$ MW	ABC_PSO	DE	SA	QBA
P_1 (MW)	55	55	54.9999	54.9931
P_2 (MW)	80	79.89	80	80
P_3 (MW)	106.93	106.8253	107.6363	107.7993
P_4 (MW)	100.5668	102.8307	102.5948	99.8801
P_5 (MW)	81.49	82.2418	80.7015	83.2628
P_6 (MW)	83.011	80.4352	81.1210	81.9051
P_7 (MW)	300	300	300	300
P_8 (MW)	340	340	340	340
P_9 (MW)	470	470	470	470
P_{10} (MW)	470	469.8975	470	470
Losses (MW)	87.0344	-	87.04	87.84
Fuel cost (\$/hr)	111500	111500	111498.66	111310.7

In third and last case, QBA is applied to 40-unit power generation system in order to verify its effectiveness in handling large number of generating units of a power generation system. The authors do not consider transmission loss for this case. The obtained result is accumulated and compared with DE (Basu, 2011b), which is the only method found previously applied in 40-unit system considering valve-point effect. The table also provides optimized dedicated generations (in MW) for each of the 40 units. The comparison of result demonstrates that QBA effectively outperforms DE in 40-unit system. Therefore, in all three cases, whether small, medium or large generation system, QBA performs better than any other existing method found in the literature. Table 4 has a Comparison of results among different approaches to solve 10-unit ELD problem with valve-point effect

Figure 3. Convergence graph of QBA for solving ELD problem in 10-unit system ($P_D=2000$)

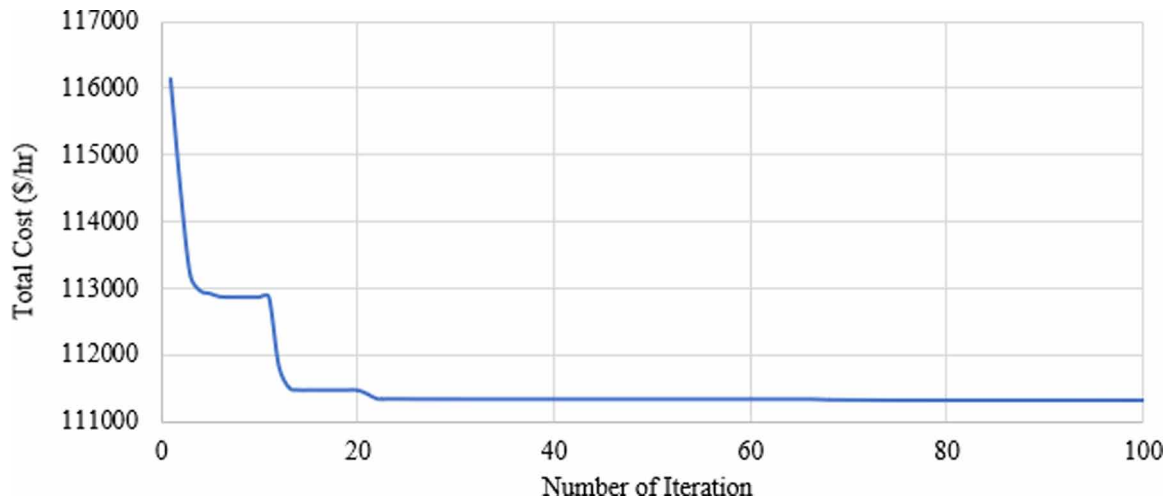
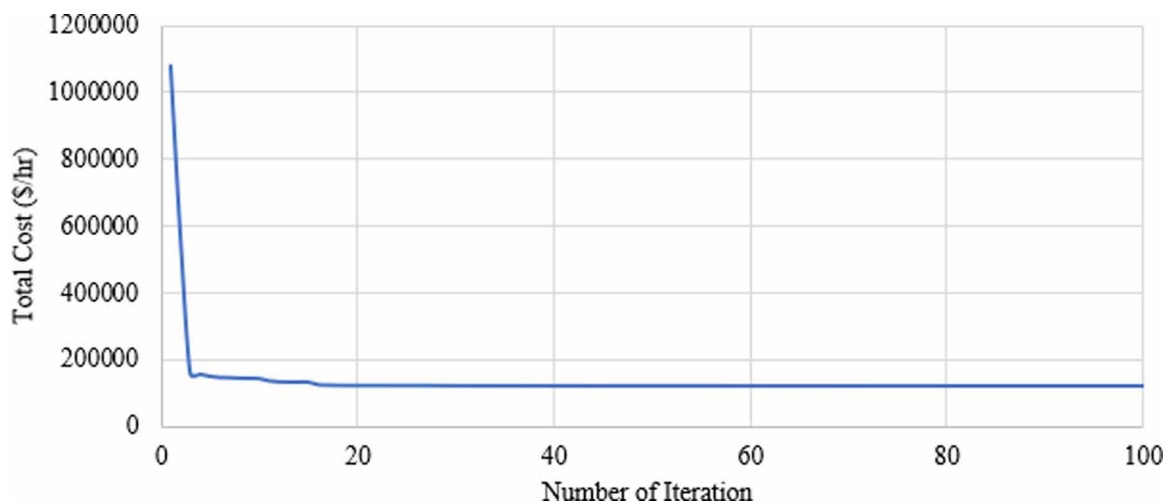


Figure 4. Convergence graph of QBA for solving ELD problem in 40-unit system ($P_D=10500$)



Quantum-Behaved Bat Algorithm for Solving the Economic Load Dispatch Problem

Table 4. Comparison of results among different approaches to solve 10-unit ELD problem with valve-point effect

$P_D=2000$ MW	DE	QBA
P_1 (MW)	110.9515	113.9687
P_2 (MW)	113.2997	114
P_3 (MW)	98.6155	120.0000
P_4 (MW)	184.1487	97.0000
P_5 (MW)	86.4013	140.0000
P_6 (MW)	140.0000	300.0000
P_7 (MW)	300.0000	300.0000
P_8 (MW)	285.4556	300.0000
P_9 (MW)	297.5110	300.0000
P_{10} (MW)	130.0000	272.5902017
P_{11} (MW)	168.7482	122.8924129
P_{12} (MW)	95.6950	172.2595563
P_{13} (MW)	125.0000	500
P_{14} (MW)	394.3545	500
P_{15} (MW)	305.5234	173.2148741
P_{16} (MW)	394.7147	452.7186369
P_{17} (MW)	489.7972	500
P_{18} (MW)	489.3620	296.2040981
P_{19} (MW)	520.9024	550
P_{20} (MW)	510.6407	489.1801605
P_{21} (MW)	524.5336	550
P_{22} (MW)	526.6981	316.2507976
P_{23} (MW)	530.7467	487.0302724
P_{24} (MW)	526.3270	550
P_{25} (MW)	525.6537	550
P_{26} (MW)	522.9497	11.67802064
P_{27} (MW)	10.0000	18.77386762
P_{28} (MW)	11.5522	17.00767457
P_{29} (MW)	10.0000	97
P_{30} (MW)	89.9076	190
P_{31} (MW)	190.0000	190
P_{32} (MW)	190.0000	101.5924418
P_{33} (MW)	190.0000	136.6382606
P_{34} (MW)	198.8403	200
P_{35} (MW)	174.1783	200
P_{36} (MW)	197.1598	110
P_{37} (MW)	110.0000	110

continues on following page

Table 4. Continued

$P_D=2000$ MW	DE	QBA
P_{38} (MW)	109.3565	110
P_{39} (MW)	110.0000	550
P_{40} (MW)	110.9515	272.5902017
Fuel cost \$/hr ($\times 10^5$)	1.2184	1.2093

The vertical axis describes the total cost (in \$), whereas the horizontal axis describes the number of iterations. The figures verify and demonstrate QBA's powerful computational and convergence characteristics. QBA takes around 20 iterations for 10-unit system, whereas takes less than 10 iterations for 3-unit and 40-unit systems. From the figures, authors conclude that QBA converges very quickly and thus can be said that this method is computationally powerful and efficient. Although, the population size of 3-unit system is taken similar as for the other systems to make a fair comparison, it does not require that much of population size. Furthermore, QBA successfully provides solutions without trapping into the local optima, which is a major problem for many of the existing methods when dealing with nonlinear optimization problem. The consideration of self-adaptive capability and multiple foraging habitats play a pivotal role for such well distributed and stronger searching performance of QBA in solving such nonlinear power dispatch problem.

CONCLUSION

In this research, QBA is successfully applied to solve ELD problem considering valve-point effect for 3-unit, 10-unit and 40-unit power generation systems for 850 MW, 2000 MW and 105000 MW loads, respectively. The comparison of the obtained results with other well-known methods verifies that QBA is more powerful in solving nonlinear optimization problem like ELD than other reported methods in the literature in terms of solution quality, computational efficiency and convergence characteristics. The successful implementation of QBA in 40-unit system verifies QBA's effectiveness in large power generation system. It largely overcomes the limitations found in other methods found in the literature. The main achievement of this research is to justify the feasibility of using quantum computing based traditional nature inspired metaheuristic algorithm like bat algorithm in solving nonlinear optimization problem. The obtained results verify that QBA can be implemented in power generation system of different sizes and loads. Therefore, the method can be used as a useful tool in real-world nonlinear optimization problem like dispatch and unit commitment problem of power generation system.

One of the disadvantages of QBA is that it has many parameters to tune. Efforts should be made to reduce parameters in QBA. In future, QBA should be applied with other real-world objectives such as environmental dispatching and reliability, and constraints like prohibited operating zones, ramp-rate limit and dynamic dispatching to make it more implement friendly technique in modern power generation system. In addition, renewable energy technologies should be considered along with this power dispatch problem to make it more environmentally friendly, long lasting and economically viable. Other advanced quantum computing powered metaheuristic techniques like quantum cuckoo search (QCS) algorithm

should be explored to solve this power dispatch problem. CS algorithm utilizes Levy flight technique that could be useful to solve such nonlinear optimization problem.

ACKNOWLEDGMENT

Centre of Graduate Studies (CGS) with the support of the Department of Fundamental & Applied Sciences, Universiti Teknologi PETRONAS sponsors this research work.

REFERENCES

- Abdullah, M. N., Bakar, A. H. A., Rahim, N. A., Jamian, J. J., & Aman, M. M. (2012). Economic dispatch with valve point effect using iteration particle swarm optimization. *Paper presented at the 2012 47th International Universities Power Engineering Conference (UPEC)*. Academic Press.
- Abedinia, O., Amjady, N., Ghasemi, A., & Hejrati, Z. (2013). Solution of economic load dispatch problem via hybrid particle swarm optimization with time-varying acceleration coefficients and bacteria foraging algorithm techniques. *International Transactions on Electrical Energy Systems*, 23(8), 1504–1522. doi:10.1002/etep.1674
- Al-Sumait, J. S., Al-Othman, A. K., & Sykulski, J. K. (2007). Application of pattern search method to power system valve-point economic load dispatch. *International Journal of Electrical Power & Energy Systems*, 29(10), 720–730. doi:10.1016/j.ijepes.2007.06.016
- Alsumait, J. S., Sykulski, J. K., & Al-Othman, A. K. (2010). A hybrid GA-PS-SQP method to solve power system valve-point economic dispatch problems. *Applied Energy*, 87(5), 1773–1781. doi:10.1016/j.apenergy.2009.10.007
- Basu, M. (2011a). Economic environmental dispatch of fixed head hydrothermal power systems using nondominated sorting genetic algorithm-II. *Applied Soft Computing*, 11(3), 3046–3055. doi:10.1016/j.asoc.2010.12.005
- Basu, M. (2011b). Economic environmental dispatch using multi-objective differential evolution. *Applied Soft Computing*, 11(2), 2845–2853. doi:10.1016/j.asoc.2010.11.014
- Chakrabati, R., Choudhury, S., Chattopadhyay, P. K., Sinha, N., & Ravi, G. (2003). Improved fast evolutionary algorithm for security constrained nonconvex economic load dispatch. *Paper presented at the IPEC 2003 - 6th International Power Engineering Conference*. Academic Press.
- Chen, C.-L., & Wang, S.-C. (1993). Branch-and-bound scheduling for thermal generating units. *IEEE Transactions on Energy Conversion*, 8(2), 184–189.
- Chiou, J. P. (2009). A variable scaling hybrid differential evolution for solving large-scale power dispatch problems. *IET Generation, Transmission & Distribution*, 3(2), 154–163. doi:10.1049/iet-gtd:20080262
- Coelho, L. D. S., & Mariani, V. C. (2010). An efficient cultural self-organizing migrating strategy for economic dispatch optimization with valve-point effect. *Energy Conversion and Management*, 51(12), 2580–2587. doi:10.1016/j.enconman.2010.05.022

- Coelho, L. S., & Mariani, V. C. (2009a). Chaotic artificial immune approach applied to economic dispatch of electric energy using thermal units. *Chaos, Solitons, and Fractals*, 40(5), 2376–2383. doi:10.1016/j.chaos.2007.10.032
- Coelho, L. S., & Mariani, V. C. (2009b). An improved harmony search algorithm for power economic load dispatch. *Energy Conversion and Management*, 50(10), 2522–2526. doi:10.1016/j.enconman.2009.05.034
- Coelho, L. S., & Mariani, V. C. (2009c). A novel chaotic particle swarm optimization approach using Hénon map and implicit filtering local search for economic load dispatch. *Chaos, Solitons, and Fractals*, 39(2), 510–518. doi:10.1016/j.chaos.2007.01.093
- dos Santos Coelho, L., & Mariani, V. C. (2006). Combining of chaotic differential evolution and quadratic programming for economic dispatch optimization with valve-point effect. *IEEE Transactions on Power Systems*, 21(2), 989–996. doi:10.1109/TPWRS.2006.873410
- Duvvuru, N., & Swarup, K. S. (2011). A Hybrid Interior Point Assisted Differential Evolution Algorithm for Economic Dispatch. *IEEE Transactions on Power Systems*, 26(2), 541–549. doi:10.1109/TPWRS.2010.2053224
- He, D., Wang, F., & Mao, Z. (2008). Hybrid genetic algorithm for economic dispatch with valve-point effect. *Electric Power Systems Research*, 78(4), 626–633. doi:10.1016/j.epsr.2007.05.008
- He, X., Rao, Y., & Huang, J. (2016). A novel algorithm for economic load dispatch of power systems. *Neurocomputing*, 171, 1454–1461. doi:10.1016/j.neucom.2015.07.107
- Hou, Y. H., Wu, Y. W., Lu, L. J., & Xiong, X. Y. (2002). Generalized ant colony optimization for economic dispatch of power systems. *Paper presented at the PowerCon 2002 - 2002 International Conference on Power System Technology*. Academic Press.
- Jayabarathi, T., Raghunathan, T., Adarsh, B. R., & Suganthan, P. N. (2016). Economic dispatch using hybrid grey wolf optimizer. *Energy*, 111, 630–641. doi:10.1016/j.energy.2016.05.105
- Jiang, X. J., Xu, M. Q., Gong, X. H., & Chen, L. (2009). Hybrid particle swarm optimization for economic dispatch with valve-point effect. *Dianli Xitong Baohu yu Kongzhi [Power System Protection and Control]*, 37(8), 10-13.
- Khoa, T. H., Vasant, P. M., Singh, M. S. B., & Dieu, V. N. (2017). Swarm based mean-variance mapping optimization for convex and non-convex economic dispatch problems. *Memetic Computing*, 9(2), 91–108. doi:10.1007/12293-016-0186-1
- Lee, J.-C., Lin, W.-M., Liao, G.-C., & Tsao, T.-P. (2011). Quantum genetic algorithm for dynamic economic dispatch with valve-point effects and including wind power system. *International Journal of Electrical Power & Energy Systems*, 33(2), 189–197. doi:10.1016/j.ijepes.2010.08.014
- Lee, S. C., & Kim, Y. H. (2002). An enhanced Lagrangian neural network for the ELD problems with piecewise quadratic cost functions and nonlinear constraints. *Electric Power Systems Research*, 60(3), 167–177. doi:10.1016/S0378-7796(01)00181-X
- Lin, C. E., Chen, S. T., & Huang, C.-L. (1992). A direct Newton-Raphson economic dispatch. *IEEE Transactions on Power Systems*, 7(3), 1149–1154. doi:10.1109/59.207328

Quantum-Behaved Bat Algorithm for Solving the Economic Load Dispatch Problem

Lin, W.-M., Cheng, F.-S., & Tsay, M.-T. (2002). An improved tabu search for economic dispatch with multiple minima. *IEEE Transactions on Power Systems*, 17(1), 108–112. doi:10.1109/59.982200

Mahdi, F. P., Vasant, P., Kallimani, V., & Abdullah-Al-Wadud, M. (2016). A review on economic emission dispatch problems using quantum computational intelligence. *AIP Conference Proceedings*, 1787(1), 020002. doi:10.1063/1.4968051

Mahdi, F. P., Vasant, P., Kallimani, V., Abdullah-Al-Wadud, M., & Watada, J. (2017). Quantum-Inspired Computational Intelligence for Economic Emission Dispatch Problem. In K. S. Shishir, S. Smita, D. K. Sum, & K. N. Atulya (Eds.), *Handbook of Research on Soft Computing and Nature-Inspired Algorithms* (pp. 445–468). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-2128-0.ch015

Mahdi, F. P., Vasant, P., Kallimani, V., Watada, J., Fai, P. Y. S., & Abdullah-Al-Wadud, M. (2017). A holistic review on optimization strategies for combined economic emission dispatch problem. *Renewable & Sustainable Energy Reviews*. doi:10.1016/j.rser.2017.06.111

Manteaw, E. D., & Odero, N. A. (2012). Combined Economic and Emission Dispatch solution using ABC_PSO Hybrid algorithm with valve point loading effect. *International Journal of Scientific and Research Publications*, 2(12), 1–9.

Meng, K. (2007). *Research of fuzzy self-adaptive immune algorithm and its application. (M.E.)*. Shanghai, China: East China University of Science and Technology.

Meng, K., Wang, H. G., Dong, Z., & Wong, K. P. (2010). Quantum-Inspired Particle Swarm Optimization for Valve-Point Economic Load Dispatch. *IEEE Transactions on Power Systems*, 25(1), 215–222. doi:10.1109/TPWRS.2009.2030359

Momoh, J. A., El-Hawary, M., & Adapa, R. (1999). A review of selected optimal power flow literature to 1993. II. Newton, linear programming and interior point methods. *IEEE Transactions on Power Systems*, 14(1), 105–111. doi:10.1109/59.744495

Niknam, T. (2010). A new fuzzy adaptive hybrid particle swarm optimization algorithm for non-linear, non-smooth and non-convex economic dispatch problem. *Applied Energy*, 87(1), 327–339. doi:10.1016/j.apenergy.2009.05.016

Park, J. B., Lee, K. S., Shin, J. R., & Lee, K. Y. (2005). A particle swarm optimization for economic dispatch with nonsmooth cost functions. *IEEE Transactions on Power Systems*, 20(1), 34–42. doi:10.1109/TPWRS.2004.831275

Roy, P. K., Ghoshal, S. P., & Thakur, S. S. (2009). Biogeography based optimization to solve economic load dispatch considering valve point effects. *Paper presented at the 2009 World Congress on Nature and Biologically Inspired Computing NABIC 2009*. Academic Press. 10.1109/NABIC.2009.5393790

Sakthivel, S., Natarajan, R., & Gurusamy, P. (2013). Application of bat optimization algorithm for economic load dispatch considering valve point effects. *International Journal of Computers and Applications*, 67(11).

- Shahinzadeh, H., Fathi, S. H., Moazzami, M., & Hosseinian, S. H. (2017). Hybrid Big Bang-Big Crunch Algorithm for solving non-convex Economic Load Dispatch problems. *Paper presented at the 2nd Conference on Swarm Intelligence and Evolutionary Computation CSIEC 2017*. Academic Press. 10.1109/CSIEC.2017.7940156
- Shi, Y., & Eberhart, R. C. (1998). Parameter selection in particle swarm optimization. In V. W. Porto, N. Saravanan, D. Waagen, & A. E. Eiben (Eds.), *Evolutionary Programming VII: 7th International Conference, EP98, San Diego, CA* (pp. 591-600). Springer.
- Sinha, N., Chakrabarti, R., & Chattopadhyay, P. (2003). Evolutionary programming techniques for economic load dispatch. *IEEE Transactions on Evolutionary Computation*, 7(1), 83–94.
- Sinha, N., & Purkayastha, B. (2004). PSO embedded evolutionary programming technique for nonconvex economic load dispatch. *Paper presented at the Power Systems Conference and Exposition*. Academic Press.
- Victoire, T. A. A., & Jeyakumar, A. E. (2005). Reserve constrained dynamic dispatch of units with valve-point effects. *IEEE Transactions on Power Systems*, 20(3), 1273–1282. doi:10.1109/TPWRS.2005.851958
- Vlachogiannis, J. G., & Lee, K. Y. (2008). Quantum-Inspired Evolutionary Algorithm for Real and Reactive Power Dispatch. *IEEE Transactions on Power Systems*, 23(4), 1627–1636. doi:10.1109/TPWRS.2008.2004743
- Walters, D. C., & Sheble, G. B. (1993). Genetic algorithm solution of economic dispatch with valve point loading. *IEEE Transactions on Power Systems*, 8(3), 1325–1332. doi:10.1109/59.260861
- Wong, K. P., & Fung, C. C. (1993). Simulated annealing based economic dispatch algorithm. *IEE Proceedings C - Generation, Transmission and Distribution*, 140(6), 509-515. doi:10.1049/ip-c.1993.0074
- Wood, A. J., & Wollenberg, B. F. (2012). *Power generation, operation, and control*. John Wiley & Sons.
- Yang, H.-T., Yang, P.-C., & Huang, C.-L. (1996). Evolutionary programming based economic dispatch for units with non-smooth fuel cost functions. *IEEE Transactions on Power Systems*, 11(1), 112–118. doi:10.1109/59.485992
- Yang, X.-S. (2010). A new metaheuristic bat-inspired algorithm. *Proceedings of the Nature inspired cooperative strategies for optimization (NICSO 2010)* (pp. 65-74). Springer. doi:10.1007/978-3-642-12538-6_6
- Yang, X.-S., & Hossein Gandomi, A. (2012). Bat algorithm: A novel approach for global engineering optimization. *Engineering Computations*, 29(5), 464–483. doi:10.1108/02644401211235834
- Ziane, I., Benhamida, F., & Graa, A. (2016). Economic/Emission dispatch Problem with Valve-Point Effect. *Revue Roumaine des Sciences Techniques-Serie Electrotechnique et Energetique*, 61(3), 269–272.

This research was previously published in the International Journal of Applied Metaheuristic Computing (IJAMC), 11(3); pages 41-57, copyright year 2020 by IGI Publishing (an imprint of IGI Global).

Chapter 5

Design and Performance Evaluation of Smart Job First Multilevel Feedback Queue (SJFMLFQ) Scheduling Algorithm With Dynamic Smart Time Quantum

Amit Kumar Gupta

Suresh Gyan Vihar University, Jaipur, India

Narendra Singh Yadav

JECRC University, Jaipur, India

Dinesh Goyal

Suresh Gyan Vihar University, Jaipur, India

ABSTRACT

Multilevel feedback queue scheduling (MLFQ) algorithm is based on the concept of several queues in which a process moves. In earlier scenarios there are three queues defined for scheduling. The two higher level queues are running on Round Robin scheduling and last level queue is running on FCFS (First Come First Serve). A fix time quantum is defined for RR scheduling and scheduling of process depends upon the arrival time in ready queue. Previously a lot of work has been done in MLFQ. In our propose algorithm Smart Job First Multilevel feedback queue (SJFMLFQ) with smart time quantum (STQ), the processes are arranged in ascending order of their CPU execution time and calculate a Smart Priority Factor SPF on which processes are scheduled in queue. The process which has lowest SPF value will schedule first and the process which has highest SF value will schedule last in queue. Then a smart time quantum (STQ) is calculated for each queue. As a result, we found decreasing in turnaround time, average waiting time and increasing throughput as compared to the previous approaches and hence increase in the overall performance.

DOI: 10.4018/978-1-7998-8593-1.ch005

INTRODUCTION

A multiprogramming system in which multiple programs can be execute simultaneously. So the scheduling algorithms which decide which process will acquire the CPU at particular instance have a very crucial role for effecting the performance and efficiency of computer system. The scheduling algorithm is basically installed in the short term schedulers who select the process from the ready queue as per the guideline of scheduling algorithm and allocate it to the CPU for execution. There are many CPU scheduling algorithms exist like First Come First Serve (FCFS), Shortest Job First (SJF), Shortest Remaining Time First (SRTF), Priority scheduling, Round Robin Scheduling, Multilevel Queue Scheduling (MLQ) and Multilevel Feedback Queue Scheduling. The multilevel feedback queue scheduling is implemented with several queues in which processes are switches among several queues. Previously it is working on two scheduling algorithms in which the higher level queue is working on RR scheduling and last level queue is working on FCFS scheduling. These scheduling Algorithms are used to optimize the turnaround time, response time, waiting time and no of context switching. There are some scheduling criteria exist, on the behalf of these criteria the researcher analysis and determine which scheduling algorithm is perform better in terms of optimizing the performance matrices (D.M. Dhamdhare, 2006; Silberchatz et al, 2003).

SCHEDULING CRITERIA

There are many CPU scheduling algorithm is defined in operating system. Now choose of particular scheduling algorithm is become very challenging task. So, which algorithm have the best property or best for schedule the process the researcher has consider the properties of scheduling algorithm. There are number of criteria are defined to judge which scheduling algorithm is best in operating system. These criteria basically characterize the scheduling algorithm for performances wise difference in the scheduling algorithm. Here the researcher has described each and every criterion in detail, which is followings: (D.M. Dhamdhare, 2006; Silberchatz et al, 2003)

- **Context Switch:** A context switch occur when a process interrupt the normal execution sequence of another process. The CPU stores all relevant information of interrupted process in Task Control Box (TCB). The context switch degrades the system performances due to scheduling overhead. So scheduling algorithm is designed in such way that it can minimize the number of context switches.
- **Throughput:** This term is defined as number of process finished their execution in per unit time. So scheduling algorithm is designed in such way that it can maximise the throughput.
- **CPU Utilization:** From the performance wise concern the CPU cannot be sit ideal. So, scheduling algorithm is designed in such way that it cans maximum use of CPU as achievable.
- **Turnaround Time:** It represents the duration of time from at which a particular process becomes ready for execution and at which it completed its whole execution time.
- **Waiting Time:** It represents the duration of time for which the process has wait for acquiring the CPU for completing its execution time.
- **Response Time:** It represents the instance of time at which the CPU is assigned to the process first time.

LITERATURE SURVEY

Multilevel Feedback Queue Scheduling (MLFQ)

(Silberchatz et al, 2003) defines the MLFQ in which processes can be switches between queues. It defines that the last level queue will be implemented on FCFS and higher level queue will be implemented on the RR scheduling algorithm. The idea is behind on this concept is that to break up process with different CPU burst characteristics. If the execution time of a process is higher than the higher queue time quantum then it will be migrated to the lower queue. Similarly, the waiting time of any process which is situated in lower queue is becomes very high then it will be migrated to higher queue. This phenomenon is basically known as aging and it is used to escaping from the starvation.

(Rakesh Kumar Yadav et al, 2012) have proposed a scheduling algorithm which has mixed the working principles of MLFQ, SJF and improved round robin scheduling algorithm. They have defined his algorithm as Step 1: They have taken three queues as in consideration. The first two queues have RR scheduling and last one has FCFS scheduling. Step 2: sort all the processes and arrange all the process in increasing order of their burst time. Step 3: on the completion of step2 apply the round robin (RR) scheduling algorithm with fix time quantum in first queue. Step 4: As per MLFQ scheduling the processes which did not complete its execution are moved in second queue. The processes are scheduled as per RR Scheduling with static time quantum. Step 5: After the completion of step 4, all the process which have not completed their execution in second queue will be move in third queue where, FCFS scheduling will be implemented.

(Behera et al., 2012) have proposed Improved Multilevel Feedback Queue Scheduling Using Dynamic Time Quantum and Its Performance Analysis. In this paper, they have used five queues for scheduling. The RR scheduling algorithm will be implemented on all five queues (Q1, Q2, Q3, Q4, and Q5) with the use of dynamic time quantum. They have calculated the dynamic time quantum (TQ) is for every queue by calculating the mean and median of execution time of the processes. The difference value of mean and median which is divided by 3 is taken as the time quantum for the first queue (Q1). The time quantum for remaining queue is calculated as $t_{q_{i+1}} = t_{q_i} * 2$ where $i = 1, 2, 3, 4$.

The scheduling is defined as:

1. The processes are sorted in ascending order of CPU execution time of processes.
2. Then the processes are scheduled on queue Q1 with the calculated time quantum t_{q_1} in RR manner.
3. The processes which have not completed their execution will be moved in queue Q2 and schedule with t_{q_2} . Then move processes in queue Q3, Q4 and Q5 and schedule the process with time quantum t_{q_3} , t_{q_4} and t_{q_5} .
4. If the processes have not completed their remaining burst time in queue Q5 then all the processes are dispatched to higher queue as per their remaining burst time. The least remaining burst time process will be dispatch to Q1, next least to Q2 and at most remaining burst time process to Q5. This process is repeated until all the processes complete their execution.

They have analyzed their proposed algorithm Power MLFQ and EMLFQ algorithm and found better result in terms of decreasing average waiting time, average turnaround time than MLFQ and EMLFQ algorithm.

(Iqra Sattar et al., 2014) have proposed Multi-Level Queue with Priority and Time Sharing for Real Time Scheduling. In this algorithm, all the tasks are inserted in a list. Then the priority levels for all tasks are defined on the basis of tasks deadline, turnaround time and the waiting time of task. Once the priority level has been decided the tasks are divided in to the multiple queues and each queue define a particular priority level. Each queue having a specific time quantum known as queue execution time which will be varies queue by queue. The queue which has highest priority level will have the more amount of time for executing its task on CPU. After one cycle the priority level for the task which has not completed its execution will again calculated and whole process will be repeated until all the tasks are completely scheduled.

(Ayan Bhunia, 2011) has proposed Enhancing the Performance of Feedback Scheduling. In this paper he has implemented the concept of MLFQ with five queues. The process which is ready to execute, dispatch to the queue 1 and if it is not finished their execution in queue 1 then it will be transferred to the lower priority queues until it finished their execution. The time quantum of each queue is doubled from upper to lower. The processes are scheduled first in queue 1 with a time quantum say k units. Then processes will be switches in second queue if they have not completed with time quantum doubled from the queue 1. Then they will be dispatched to queue 3, queue 4 and queue 5 with time quantum four times, eight times and sixteen times respectively from the time quantum of queue 1. If the processes have not finished their execution after the completion of the last queue then they again the processes are sorted ascending order of their remaining burst time. Then the process which has minimum remaining burst time process will be dispatched to first queue and at most remaining burst time process will be dispatched to lowest queue. He has analyzed their proposed algorithm Power MLFQ and EMLFQ algorithm and found better result in terms of decreasing average waiting time, average turnaround time than MLFQ and EMLFQ algorithm.

(H.S.Behera et. al., 2012) have proposed a new Hybridized Multilevel Feedback Queue Scheduling with Intelligent Time Slice and its Performance Analysis. In this paper, they have defined multilevel feedback queue algorithm with five queues (Q1, Q2, Q3, Q4 and Q5) in consideration and calculate dynamic ITS (Intelligent Time Slice) for each queue. The ITS is calculated as follows:

1. $\text{Range} = \frac{\text{Max burst time} + \text{Min burst time}}{\text{Max burst time} - \text{Min burst time}}$
2. $\text{OTS} = \text{Range} + \text{no. of processes} + \text{priority of current process}$
3. To calculate ITS the formula used is
 - a. $\text{ITS} = \text{OTS} + (\text{total no. of processes}) + (\text{priority of current process})$.
4. The various ITS for each queue is calculated as follows;
 - a. $\text{ITS1} = \text{ITS}$, $\text{ITS2} = 2 * \text{ITS1}$, $\text{ITS3} = 2 * \text{ITS2}$, $\text{ITS4} = 2 * \text{ITS3}$, $\text{ITS5} = 2 * \text{ITS4}$

From the above they have scheduled the processes in Q1 with time slice ITS1 using RR scheduling. Then the processes are transferred in Queue Q2, Q3, Q4 and Q5. If any process does not finish their execution in Q5 then the all the processes which have remaining burst time is greater than zero are to be rescheduled in their respective queues. The processes are sorted in ascending order of their burst time and dispatched them to their respective queues. The process which has least burst time is dispatched to Q1 and next process to Q2 and in the similar manner the processes are dispatched up to Q5 so that Q5 can be assigned the process with at most remaining burst time. The same procedure repeated until all the processes have completed their execution time. They have analyzed their proposed algorithm Power

MLFQ and EMLFQ algorithm and found better result in terms of decreasing average waiting time, average turnaround time than MLFQ and EMLFQ algorithm

PROPOSED PLAN

The proposed algorithm, Smart Job First Multilevel feedback queue (SJFMLFQ) scheduling algorithm with smart dynamic time quantum is based on the smart factor (SF) and dynamically calculated smart time quantum (STQ). Assume that the arrival time of all process is zero. The algorithm is defined as:

Step 1

Divide the memory into three queues (Q1, Q2, and Q3). Each queue has SJFDRR scheduling algorithm. The SJFDRR scheduling algorithm is defined as: In this algorithm, first we will calculate a smart priority factor 'SPF' is for every process. The process which has smallest 'SPF' value will be scheduled first. In this work every process has two types of priority one is user priority which is given by user itself (PRU) and second is the system priority which is defined by scheduling system in such a way that lowest burst time has highest system priority (PRS). The two important factors are also taken for calculating smart priority factor (SPF) which is user priority ratio (UPR) and system priority ratio (SPR). The user priority has more importance so the user priority ratio is given 55% weight and system priority ratio is given 45% weight. Assume that all the processes become ready for execution at same time i.e. arrival time = 0. Then Smart Priority Factor 'SPF' is calculated as:

$$SPF = PRU * UPR + PRS * SPR \quad (1)$$

So, we calculate SPF for every process and decide which process will schedule first on the basis of SPF value.

Step 2

Define the smart time quantum (STQ) for first queue as given below:

- First calculate median for the set of processes in ready queue by given formula as given below:

$$\text{Median}(M) = \begin{cases} \frac{Y_{\frac{n+1}{2}}}{2} & \text{if } n \text{ is odd} \\ \frac{1}{2} \left(Y_{\frac{n}{2}} + Y_{\frac{n}{2}+1} \right) & \text{if } n \text{ is even} \end{cases}$$

where, M = median, Y = Burst time of Process which is situated in the mid of process after the processes are sorted and arranged in the increasing order of their burst time and n = number of processes:

- Then, the smart time quantum is calculated as follows:

$$\text{Smart Time Quantum (STQ)} = \text{Ceiling } (((Bt_{\max} + M) / 2) / n) \quad (2)$$

where Bt_{\max} is maximum burst time among all the process in ready queue.

Step 3

The smart time quantum STQ1, STQ2 and STQ3 is defined for queues Q1, Q2 and Q3 respectively as follows:

$$STQ_i = STQ, STQ_{i+1} = 2 * STQ_i$$

where STQ_i is Smart Time Quantum for i^{th} Queue and STQ_{i+1} is Smart Time Quantum for $(i+1)^{\text{th}}$ Queue.

Step 4

If any process does not finish their execution up to the last queue i.e. Q3. Then all the processes having remaining burst time is greater than zero are again sorted and arranged in the increasing order of their burst time and dispatched them to their concern queues. The process which has least remaining burst time will be dispatched to Queue Q1 and next process to queue Q2 and in the similar manner processes are dispatched to queue Q3 so that queue Q3 must received the process with at most remaining burst time. The similar method repeats until all the processes have completed their execution.

RESULT AND ANALYSIS

Here in this paper the Case 1 and Case 2 data has been opted from the paper (Rakesh Kumar Yadav et al, 2012) for the comparison of new proposed algorithm and fresh loom MLFQ.

Case 1

The processes with their data is shown in Table 1. In the Table 2 processes are arranged in ascending order of their burst time. The Table 3 shows the output using fresh loom of MLFQ algorithm and our new proposed algorithm SJFMLFQ with smart time quantum. See also Figure 3. Figure 1 and Figure 2 show Gantt chart for fresh loom of MLFQ algorithm and our proposed algorithm respectively. The STQ for SJFMLFQ as follows:

$$\text{Median (M)} = 6.5, \text{STQ} = \text{Ceiling } (((6.5+11)/2)/6) = 2, \text{The STQ1} = 2 \text{ for Queue1, STQ2} = 4 \text{ for Queue2, STQ3} = 8 \text{ for Queue3}$$

Table 1. Processes with Burst Time and Priority

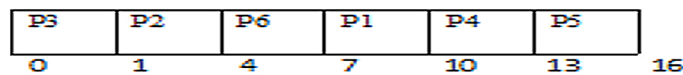
Processes	Arrival Time	Burst Time	User Priority
P1	0	8	3
P2	0	4	2
P3	0	1	1
P4	0	10	5
P5	0	11	6
P6	0	5	4

Table 2. Processes are arranged in ascending order of their Burst Time

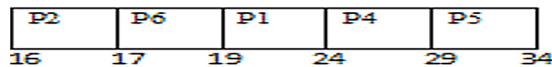
Processes	Arrival Time	Burst Time	User Priority
P3	0	1	1
P2	0	4	2
P6	0	5	3
P1	0	8	4
P4	0	10	5
P5	0	11	6

Figure 1. Gantt chart using Fresh loom of Multilevel Feedback Queue

(i) First Queue with time Quantum =3



(ii) Second Queue with time Quantum =5



(iii) Third Queue with FCFS

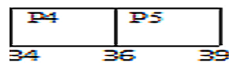
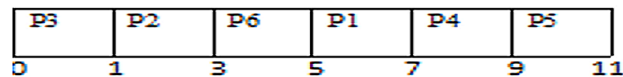
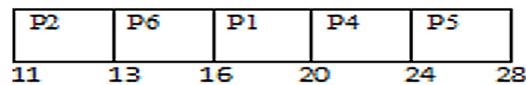


Figure 2. Gantt Chart Using SJFMLFQ

(i) First Queue with smart time Quantum =2



(ii) Second Queue with smart time Quantum =4



(iii) Third Queue with smart time Quantum =8

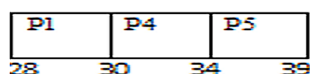
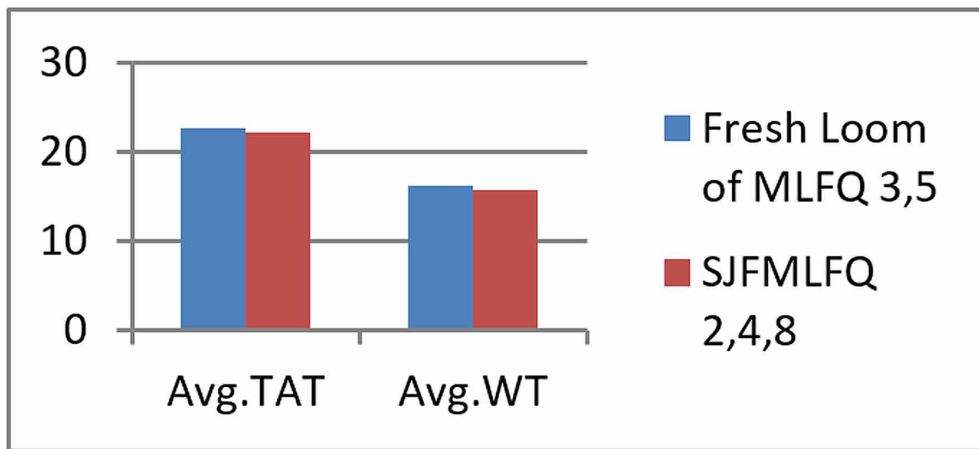


Table 3. Comparison table

Algorithm	Time Quantum	Avg.TAT	Avg.WT
Fresh Loom of MLFQ	3,5	22.16	16.16
SJFMLFQ	2,4,8	22.16	15.66

Figure 3. Comparison graph between Fresh loom of Multilevel Feedback Queue and SJFMLFQ



Case 2

The processes with their data as shown in Table 4. In the Table 5 processes are arranged in ascending order of their burst time. The Table 6 shows the output using fresh loom of MLFQ algorithm and our new proposed algorithm SJFMLFQ with smart time quantum. See also Figure 6. Figure 4 and Figure 5 show Gantt chart for fresh loom of MLFQ algorithm and our proposed algorithm respectively. The STQ for SJFMLFQ as follows: Median (M) = 13, STQ = Ceiling $\left(\frac{(13+22)}{2}\right)/6 = 3$, The STQ1 = 3 for Queue1, STQ2 = 6 for Queue2, STQ3 = 12 for Queue3.

Table 4. Processes with Burst Time and Priority

Processes	Arrival Time	Burst Time	User Priority
P1	0	16	3
P2	0	8	2
P3	0	2	1
P4	0	20	5
P5	0	22	6
P6	0	10	4

Table 5. Processes are arranged in ascending order of their Burst Time

Processes	Arrival Time	Burst Time	User Priority
P3	0	2	1
P2	0	8	2
P6	0	10	3
P1	0	16	4
P4	0	20	5
P5	0	22	6

Figure 4. Gantt chart using Fresh loom of Multilevel Feedback Queue

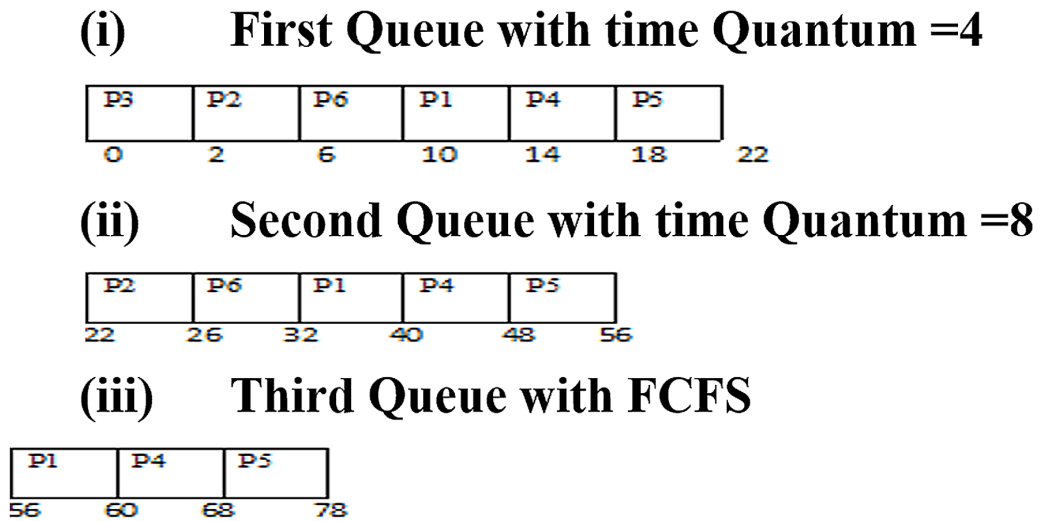


Figure 5. Gantt Chart Using SJFMLFQ

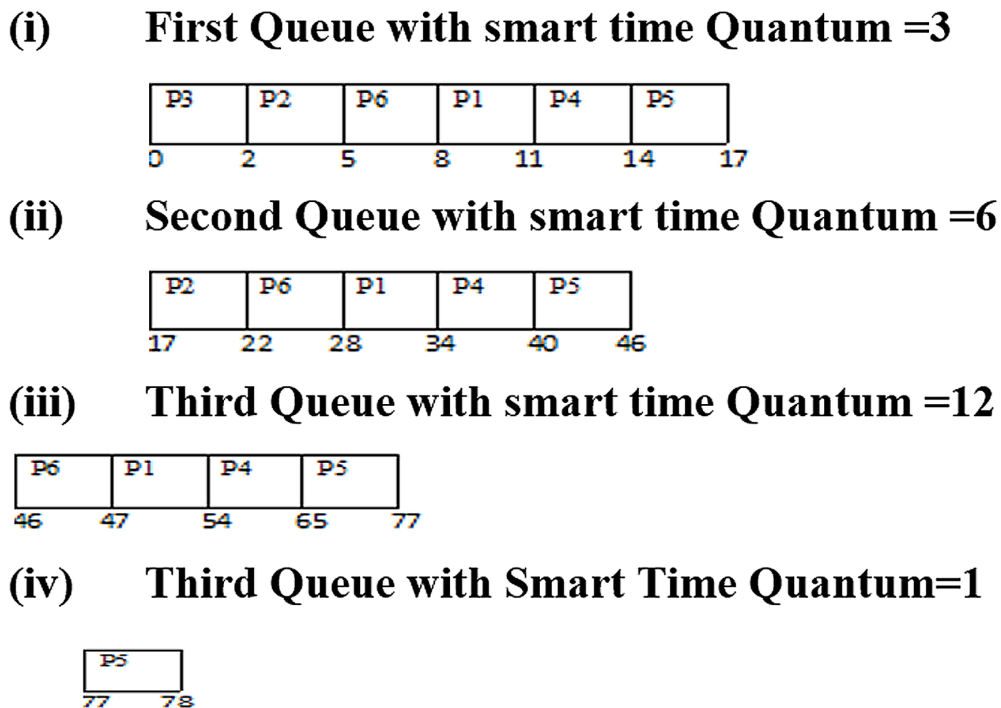
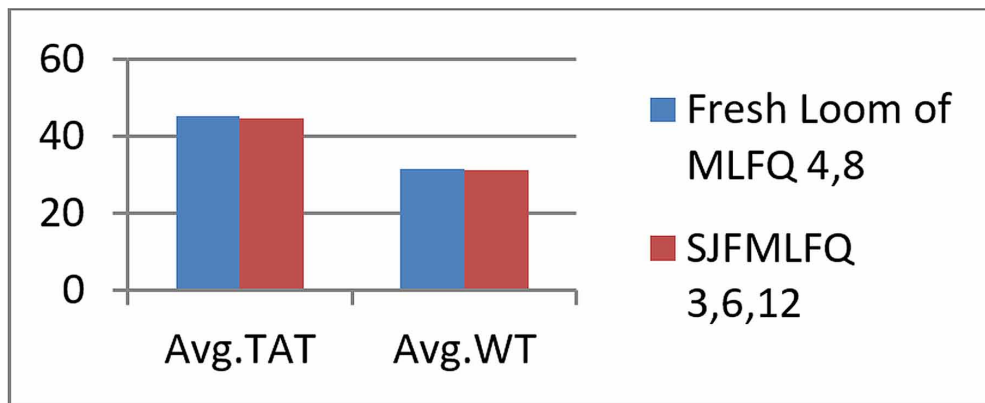


Table 6. Comparison table

Algorithm	Time Quantum	Avg.TAT	Avg.WT
Fresh Loom of MLFQ	4,8	45.33	31.66
SJFMLFQ	3,6,12	44.66	31.33

Figure 6. Comparison graph between Fresh loom of Multilevel Feedback Queue and SJFMLFQ



It is evaluated that average waiting time, average turnaround time and number of context switches are minimizing with our new approach SJFMLFQ with smart time quantum. The minimization of average waiting time, average turnaround time and number of context switches shows maximizing CPU utilization and response time. Therefore, our approach is more efficient compare than a fresh loom of multilevel feedback queue scheduling approach.

SIMULATION RESULT

The researcher has designed a simulator in .net Framework which gives the comparison result of SJFMLFQ with Dynamic Smart Time Quantum and Fresh Loom MLFQ. Here in this paper researcher has included some result on randomly generated process in Figures 7, 8, 9, 10, 11, and 12. The number of process is taken 25, 10, 20, 35, 40 and 50. The Figures 13, 14, 15, 16, 17 and 18 show the comparison graph. The simulation result gives that SJFMLFQ with Dynamic Smart Time Quantum is perform better in terms of decreasing the average waiting time and average turnaround time.

CONCLUSION

From the analysis and simulation result, it is founded that our proposed algorithm SJFMLFQ (Smart Job First Multilevel Feedback Queue Scheduling) with smart time Quantum performs better than the Fresh Loom MLFQ in terms of decreasing average waiting time and average turnaround time. But this work limited only for when arrival time of all process are zero. So, the enhancement will in this algorithm 1) research work for use different arrival time for the processes and 2) even the time quantum is high than also result may be affected.

Design and Performance Evaluation of SJFMLFQ Scheduling Algorithm With Dynamic Smart Time Quantum

Figure 7 Simulation Result (No of Process = 25)

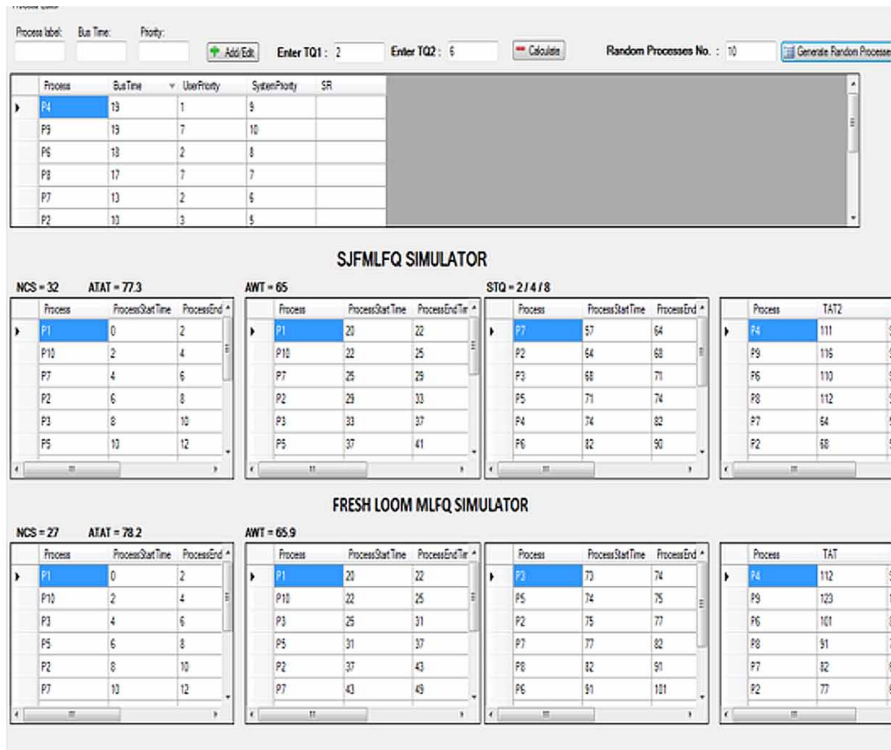
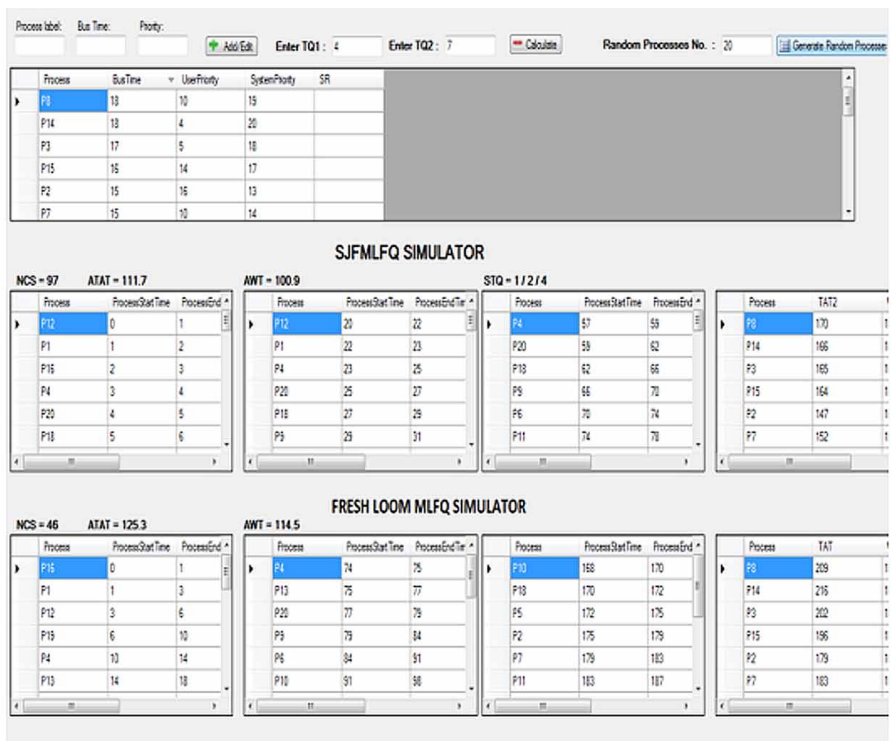


Figure 8 Simulation Result (No of Process = 10)



Design and Performance Evaluation of SJFMLFQ Scheduling Algorithm With Dynamic Smart Time Quantum

Figure 9 Simulation Result (No of Process = 20)

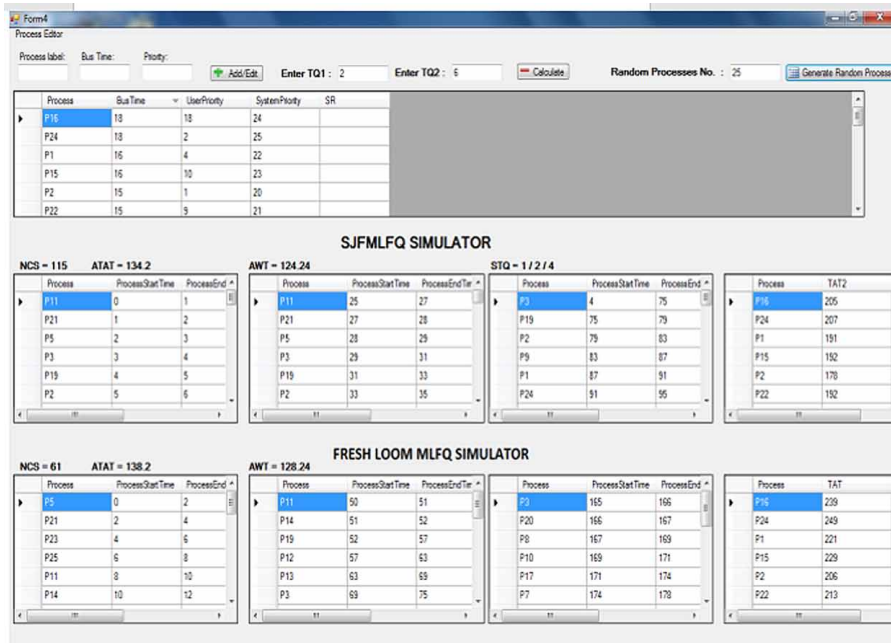
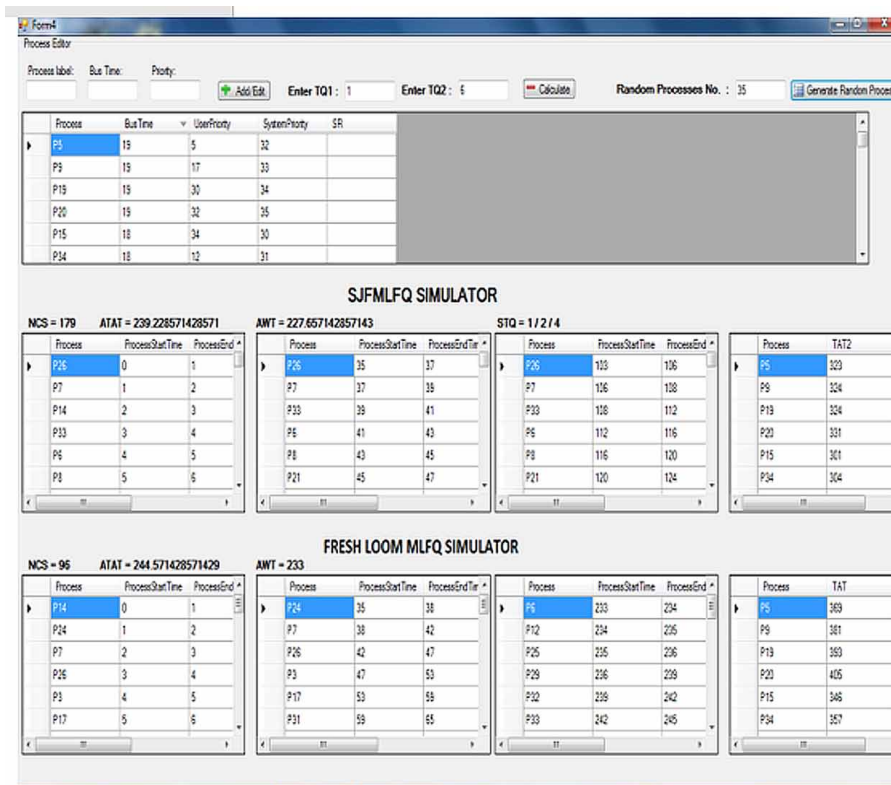


Figure 10 Simulation Result (No of Process = 35)



Design and Performance Evaluation of SJFMLFQ Scheduling Algorithm With Dynamic Smart Time Quantum

Figure 11 Simulation Result (No of Process = 40)

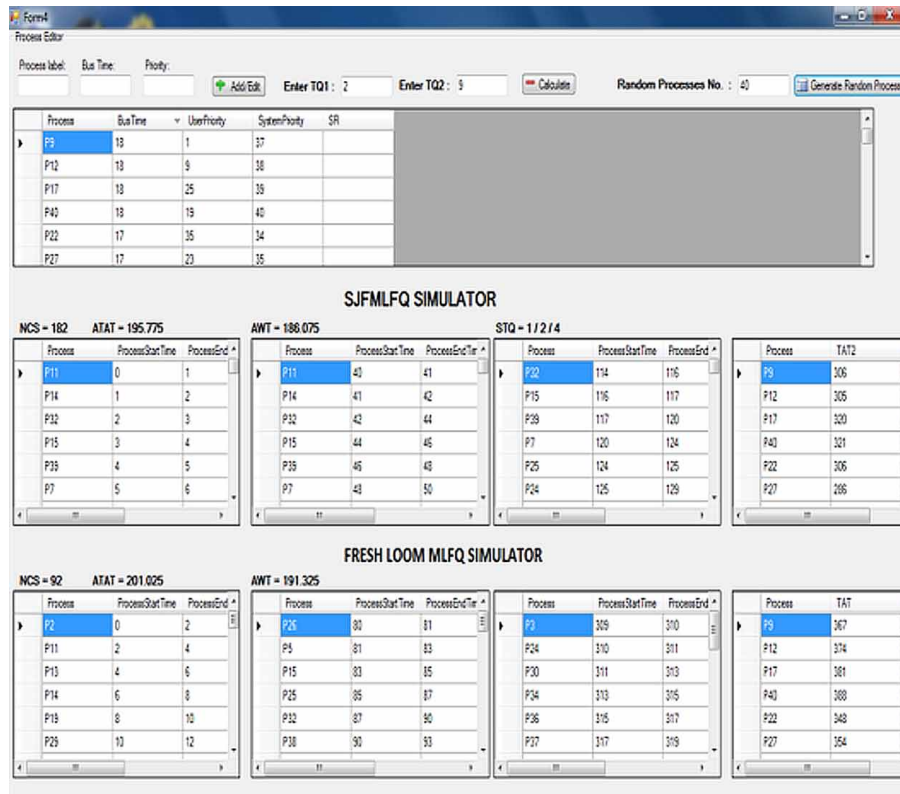


Figure 12 Simulation Result (No of Process = 50)

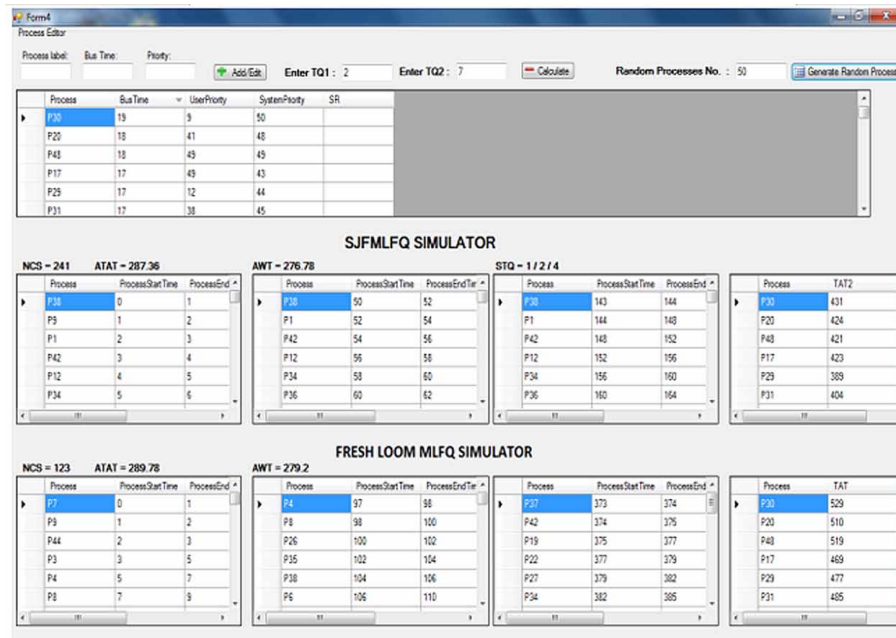


Figure 13 Comparison Graph (No of Process = 25)

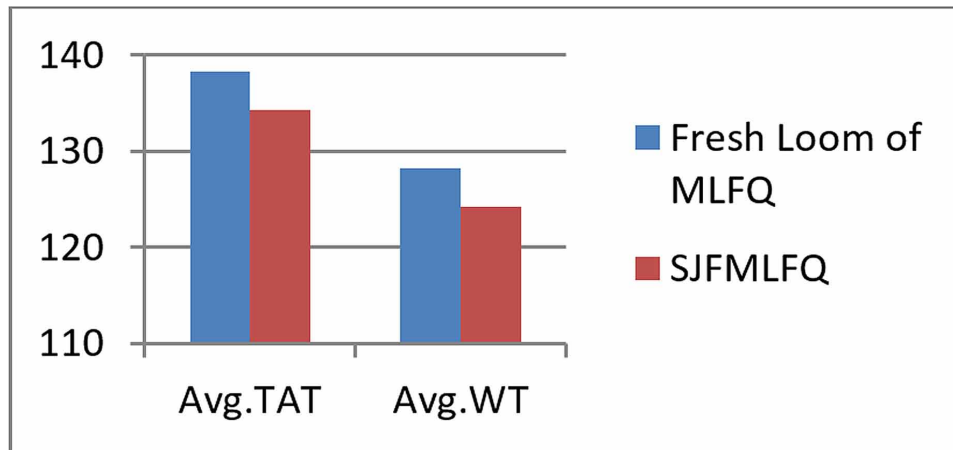


Figure 14 Comparison Graph (No of Process = 10)

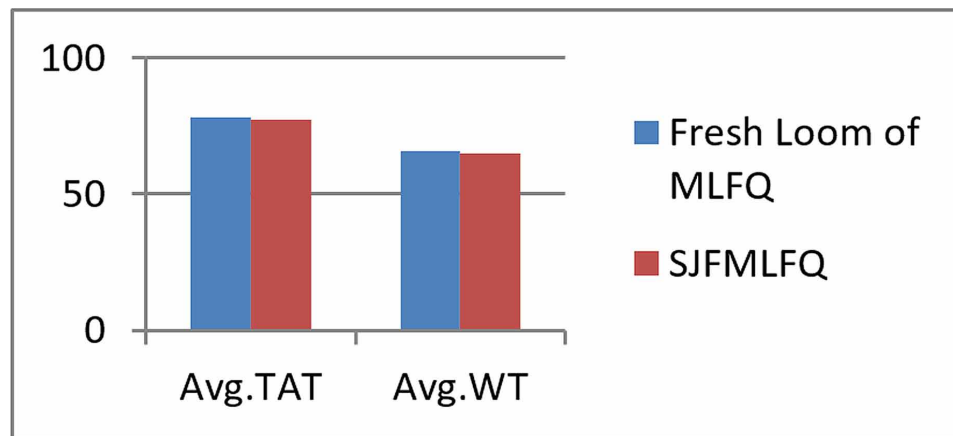


Figure 15 Comparison Graph (No of Process = 20)

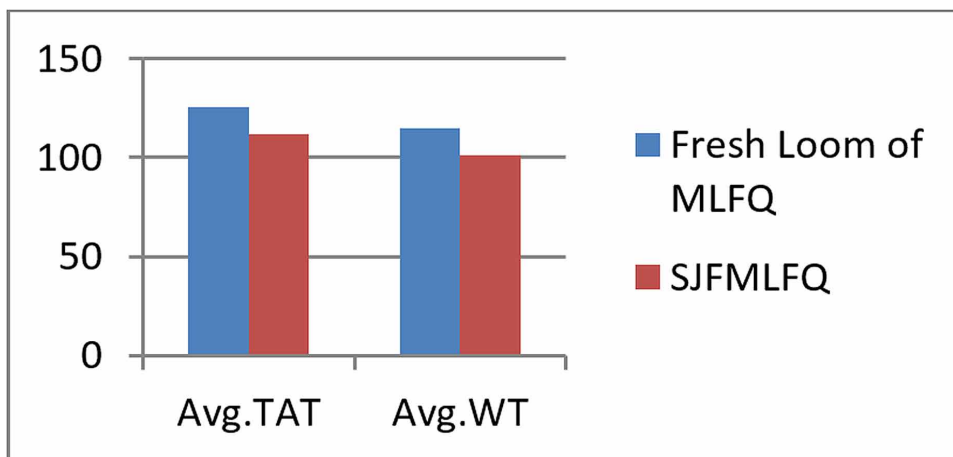


Figure 16 Comparison Graph (No of Process = 35)

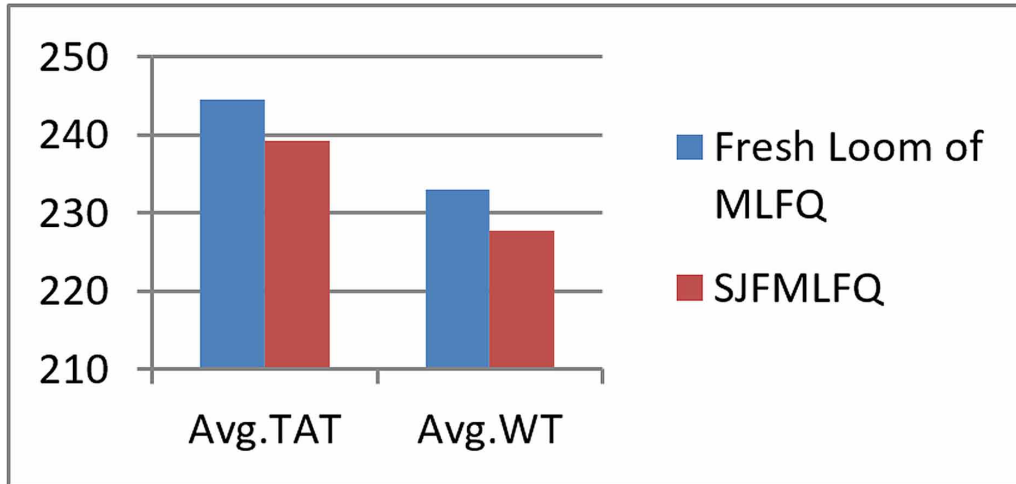


Figure 17 Comparison Graph (No of Process = 40)

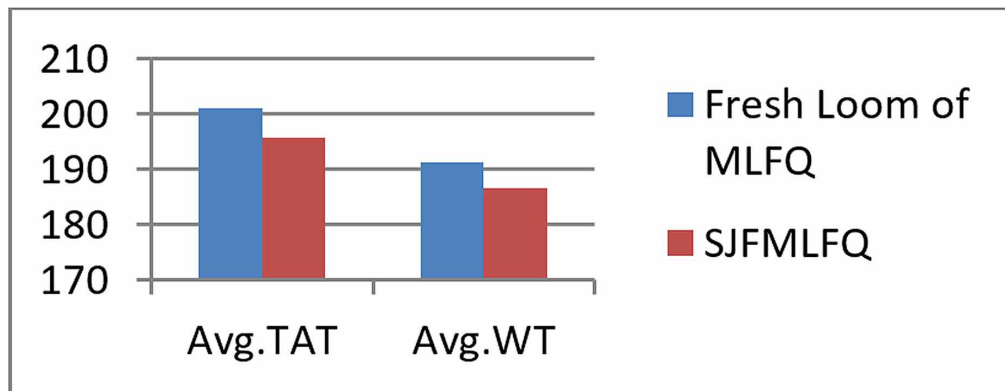
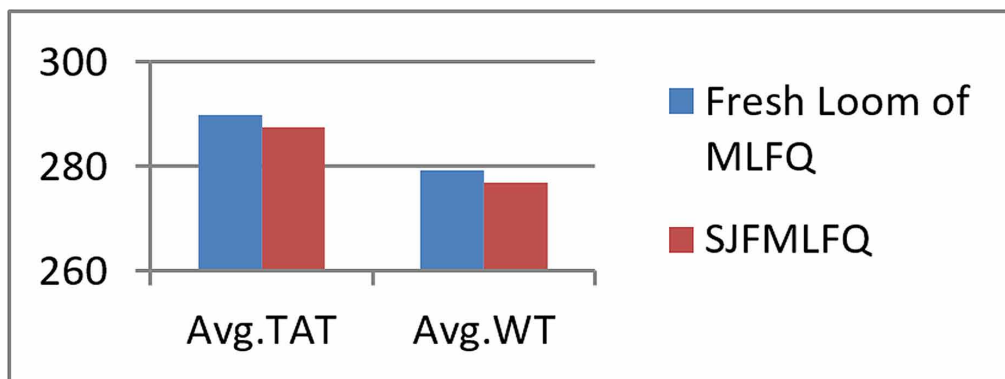


Figure 18 Comparison Graph (No of Process = 50)



REFERENCES

- Al-Husainy, M. A. F. Mohammed A.F. Al-Husainy. (2007). Best-job-first CPU scheduling algorithm. *Inform Technol. J.*, 6(2), 288–293. doi:10.3923/itj.2007.288.293
- Arora, H., Arora, D., & Jain, P. (2013). An Improved CPU Scheduling Algorithm. *International Journal of Applied Information Systems*, 6(6).
- Behera, H.S. (2011). Design and Performance Evaluation of Multi Cyclic Round Robin (MCCR) Algorithm using Dynamic Time Quantum. *Journal of Global Research in Computer Science*, 2(2), 48-53.
- Behera, H. S. (2011). Experimental Analysis of A New Fair Share Weighted Time Slice (FSWTS) Scheduling Algorithm for Real Time Systems. *Journal of Global Research in Computer Science*, 2(2), 54-60.
- Behera, H. S., Patel, S., & Panda, B. (2011). A New Dynamic Round Robin and SRTN Algorithm with Variable Original Time Slice and Intelligent Time Slice for Soft Real Time Systems. *International Journal of Computers and Applications*, 16(1), 54–60. doi:10.5120/2037-2648
- Behera, H.S., Naik, R.K., & Parida, S. (2012). A new Hybridized Multilevel Feedback Queue Scheduling with Intelligent Time Slice and its Performance Analysis. *International Journal of engineering research and technology*.
- Behera, H.S., Naik, R.K., & Parida, S. (2012). Improved Multilevel Feedback Queue Scheduling Using Dynamic Time Quantum and Its Performance Analysis. *International Journal of Computer Science and Information Technologies*, 3.
- Bhunia, A. (2011). Enhancing the Performance of Feedback Scheduling. *International Journal of Computer Applications*, 18(4).
- Dhamdhere, D. M. (2006). *Operating Systems A Concept Based Approach* (2nd ed.). Tata: McGraw-Hill.
- Mohanty, R., Behera, H. S., Patwari, K., Dash, M., & Prasanna, M. L. (2011). Priority Based dynamic Round Robin (PBDRR) Algorithm with Intelligent Time Slice for Soft Real Time System. *International Journal of Advanced Computer Science and Application*, 2(2).
- Rakesh Mohanty, H. S. Behera, Khusbu Patwari, Monisha Dash (2010). Design and Performance Evaluation of a New Proposed Shortest Remaining Burst Round Robin (SRBRR) Scheduling Algorithm. *Proceedings of International Symposium on Computer Engineering & Technology (ISCET)* (Vol 17).
- Sattar, I., Shahid, M., & Yasir, N. (2014). Multi-Level Queue with Priority and Time Sharing for Real Time Scheduling. *International Journal of Multidisciplinary Sciences and Engineering*, 5(8).
- Silberschatz, A., Galvin, P.B., & Gagne, G. (2003). *Operating systems concepts* (5th ed.). Wiley.
- Yadav, R.K., & Upadhayay, A. (2012). A Fresh Loom for Multilevel Feedback Queue Scheduling Algorithm. *International Journal of Advances in Engineering Sciences*, 2(3).
- Yadav, R.K., Mishra, A.K., Prakash, N., & Sharma, H. (2010). An Improved Round Robin Scheduling Algorithm. *International Journal on Computer Science and Engineering*, 2(4), 1064–1066.

This research was previously published in the International Journal of Multimedia Data Engineering and Management (IJM-DEM), 8(2); pages 50-64, copyright year 2017 by IGI Publishing (an imprint of IGI Global).

Chapter 6

Hardware Implementation of a Visual Image Watermarking Scheme Using Qubit/Quantum Computation Through Reversible Methodology

Subhrajit Sinha Roy

Global Institute of Management and Technology, India

Abhishek Basu

RCC Institute of Information Technology, India

Avik Chattopadhyay

University of Calcutta, India

ABSTRACT

In this chapter, hardware implementation of an LSB replacement-based digital image watermarking algorithm is introduced. The proposed scheme is developed in spatial domain. In this watermarking process, data or watermark is implanted into the cover image pixels through an adaptive last significant bit (LSB) replacement technique. The real-time execution of the watermarking logic is developed here using reversible logic. Utilization of reversible logic reduces the power dissipation by means of no information loss. The lesser power dissipation enables a faster operation as well as holds up Moore's law. The experimental results confirm that the proposed scheme offers high imperceptibility with a justified robustness.

DOI: 10.4018/978-1-7998-8593-1.ch006

INTRODUCTION

New age digital data communication offers easy access over data processing. So, Data security is essential to put off illegitimate copying or forgery attempts over transmission channel. The increasing consumer number proportionally causes a huge data augmentation which is easily performed in digital domain. But the possessor demands a copyright protection to their belongings multimedia data so that the information remains tenable. Thus the copyright protection has become a challenging research point in this rapidly developing multimedia communication domain. A good number of secured data transmission methods are invented in terms of cryptography, steganography, digital watermarking etc. during last few decades.

In cryptography the message itself converted into a distinct and unreadable form and transmitted through a secret channel. Cryptographic systems are unable to provide enough protection and reliability for data authentication. Moreover the cryptographic techniques are not reversible in nature which causes data loss. Steganography is a point to point data transmitting process where the message is made imperceptible in a cover object. The message may have nothing to do with the cover as the cover is required only to serve the purpose of concealment. On the other hand digital watermarking is the process to embed a unique code (may be in form of text or image or any multimedia object), said watermark into a cover object to make an assertion on it. Being offering a one-to-many communication without any type of secret channel or encryption, watermarking is preferred for copyright protection.

A good number of digital watermarking algorithms have been developed to reach the maximum rate of efficiency in terms of three exigent qualities of – robustness, imperceptibility and payload capacity. The software logic level development for insertion process can be performed in spatial or frequency domain. Though the frequency domain provides robustness, spatial domain is chosen for effective real time hardware implementation.

Field programmable gate array (FPGA) is one of the most intended tools for hardware execution but the more alarming issue of modern VLSI industry is power dissipation. The exponential growth of transistors within an IC causes generation of heat which results into information loss. Therefore supporting the pace of Moore's law has become gradually more complicated over modern systems. The solution was received from the new age quantum computation. The development of quantum hardware also defines the hardware software co-simulation. This quantum computation can be performed through Reversible circuits of which logic operations theoretically ensure zero percent computational data loss and thus the inputs could be recovered from the outputs. This property can be fully utilized in designing the hardware architecture of an effective watermarking embedding and extracting model with minimum power dissipation.

DIGITAL WATERMARKING

Watermarking is the process of inserting a mark into a multimedia object to make an assertion on the owner or the originality of the object. The use of watermark is an old age art. It began after a little time span of invention of paper manufacturing procedure. At that time, to manufacture paper, a semi liquid mixture of fiber and water is poured in a frame of mesh and distributed throughout the frame to give a proper shape and finally by applying pressure leaving off the water the fiber is cohered. In the wet fiber a picture or text can be impressed from a negative and it left a permanent mark on the paper – fibers

when the fibers compressed and dried. As by water vaporization the mark is manufactured, it is called 'watermark', Mohanty, S.P. (1999).

In another discussion, it is noted that the watermarking mechanism was first invented about 700 years ago in Fabriano Italy, Kutter M. (1999). In this mechanism to label an article in an invincible manner a portion of the article was made slightly thin. The thinner location of the particular article could be perceived by looking at it when it is held against a strong light source. As the thinner portion looked like watery area on the article, it was called watermark.

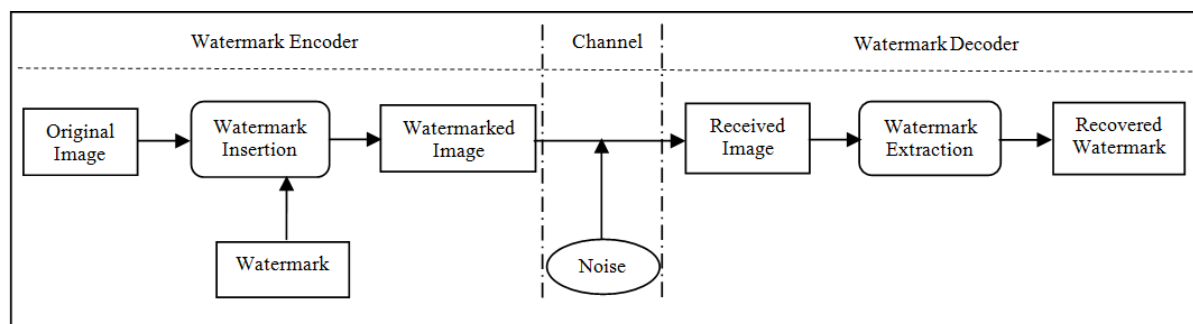
The ancient age watermark embedding process cannot sustain for the first-rate growth of modern communication technology with multimedia objects. Now a day the cover object may be audio, video, image or text which is mostly preferred in a form of digital signal. Another multimedia object should be formed as a unique mark i.e. the watermark to embed into the cover object.

Basic Operations of Digital Watermarking

Throughout the discussion, authors have chosen image as the multimedia objects to be used as cover or watermark for better comparison as most of the works have been developed using image and any image can be represented through a 2-D matrix form. Any type of digital watermarking process principally consists of three operational blocks –

1. Watermark Insertion Block
2. Transmission Block or Channel
3. Watermark Extraction Block

Figure 1. General Block Diagram of Water Encoder & Extractor



As shown in Figure 1, in the insertion block the data or watermark is injected to the cover image and the watermarked image is generated. The watermark image is transmitted over the communication channel and at the receiving end an extraction block is required. It recovers the watermark bits and reconstructs the watermark to judge the novelty by comparing with the original one. During transmission, signal processing attacks or noise can affect the cover as well as the watermark. Thus in the time of embedding a watermark, it is desired to achieve the maximum robustness as well as energy. In maximize the signal energy designer should try to decrease the error rate.

Applications and Classifications of Digital Watermarking

The application domain of digital watermarking expands as follows:

- **Copyright Protection:** The most distinct application of digital watermarking is copyright protection. As lots of multimedia objects are exchanged over insecure network every time, the copyright protection has become a vital issue. Because of availability of the images through internet, these will be used without payment of royalty. So, watermark acting as an ownership mark can restrain the redistribution of the object.
- **Content Protection:** If content (like library manuscript) stamped with a robust and visible watermark, it will indicate the ownership original. So, the content can be made available through the internet and be distributed more freely and publicly.
- **Content Labeling:** Watermark may carry more information about the object like quality, manufacturer's description etc. This is known as content labeling.
- **Authentication:** In some applications like ATM cards, ID cards, Credit cards etc., the ownership of the contain has to be verified. This quarry can be solved by embedding a watermark and in addition by providing the owner with a private key to access the message.
- **Evidence of Ownership:** Invisible watermarking may also used in copyright protection. Here it plays a roll of ownership evidence. That means the seller's watermark in the object proves that the public object is property of the seller not produced illegally or without payment of royalties by copying or editing the object.
- **Misappropriation Detection:** It may occur that someone bought a fee generating object from a license owner and sell these objects in cheap or free of cost, keeping of the revenue license owner. This type of fraudulent business can be restrained by invisible watermarking.
- **Tamper Detection:** By using the Fragile Watermarks any type of tampering on the object where the water mark was embedded, can be detected. Because, it tampering happened, the watermark will be degenerated or distorted.
- **Trustworthy Detection:** Invisible watermarking may also use in a trustworthy camera to indicate the images have been originally captured by the camera not produced by editing or falsifying any scene. Actually, at the time of capturing a picture an invisible watermark is embedded into the picture.
- **Digital Fingerprinting:** To justify the owner of as content, or to detect any alternation of object store in a digital library, it is used. Because for each party or object there should be a unique fingerprint.
- **Broadcast Monitoring:** It mainly helps the advertising companies to verify whether the advertisement broadcasted on T.V. or Radio appeared for the right duration or not.
- **Source Tracking:** Is another application of Digital Watermarking.

The dilate application field of digital watermarking has categorized this process in several ways.

1. According to the human perception watermarking can be classified in two types-
 - a. **Visible:** It is used mainly in purpose of identification of the owner. It always robust in nature.
 - b. **Invisible:** It is used for authentication and copyright protection. This section may further be divided into two types such as- Robust, Fragile.

2. Working domain of digital watermark is divided in two types-
 - a. **Spatial Domain:** In this technique randomly, selected pixels are modified.
 - b. **Frequency Domain:** In frequency domain secret data is embedded into the best frequency portions of the protected image.
3. According to application water marking is also of two types, which are-
 - a. **Source Based:** Used for ownership identification
 - b. **Destination Based:** Used to trace buyer in case of illegal reselling.

Now, invisible watermarking it is preferred that the aesthetic magnificence of the cover image should not be affected by the mark. But these two properties are opposing to each other. Moreover, to obtain a better visual transparency, payload should be reduced. To overcome this trade off a number of watermarking algorithms have been developed during last few decades.

A software algorithm deals with the challenges in terms of imperceptibility, robustness and payload capacity. Whereas in case of hardware implementation of the algorithms, the main considerations are power dissipation, energy, speed and space efficiency. In the recent years, the reversible logic has obtained immense interest in low power VLSI design because of their capability to trim down the power dissipation with a high-speed computation. Moreover, in reversible computation, the process is allowed to run both in forward and backward path i.e. the inputs can be generated from the outputs. Thus, the authors have employed reversible logic technique in hardware implementation of the proposed watermarking scheme.

LITERATURE SURVEY

Paper watermark was first brought up in Italy in late 13th century paper watermark was first introduced in Italy to be a symbol of design, class recognition and ownership proof. Very soon this technique spread over whole Europe, Emery, O. (1958), Weiner J. and Mirkes K. (1972). The paper watermarking technique is utilized in protecting legal papers, postage stamps, currencies whole over the world till now, Jaseena K.U. et al. (2011). But the concept of digital or electronic watermarking was first invented by Tanaka et al. (1990) and it was brought into use by Tirkel et al. (1993). Since that time, digital watermarking started putting on preferences as a copyright protection tool. As discussed in the earlier section, the efficiency or acceptance of any digital watermarking scheme can be measured generally through three qualities— Imperceptibility, Robustness and Payload capacity. These three features are contradictory to each other Liu N et al. (2006) & Juergen S. (2005) and a number of methods have been developed to deal with these tradeoffs among them. The watermarking techniques, developed in several ways, can be categorized principally in two domains. One is the spatial domain where the cover image pixels are directly modified by the watermark, Lin P-L, (2001), Megalingam, R.K. (2010), Mukherjee D.P. (2004) & Mohanty Saraju P. et al. (2006). And another one is frequency domain where data embedding is performed after converting the cover and watermark images into frequency domain. The frequency domain transfer operation may be performed using different transforms like discrete wavelet transform, Lalitha (2013), discrete cosine transform (DCT), Patra J. C. et al. (2010), discrete Fourier transform (DFT), Ming Li Dong (2012) etc. Although the frequency domain offers a better robustness with respect to the spatial domain techniques, but when imperceptibility is given higher preference, the spatial domain practices result superior. Moreover for real time implementation spatial domain is preferred again for its less computational cost and easy to implement feature Grgic Mislav (2009) & Maity S. P. (2009).

In this section a concise review on some recent trade of digital watermarking techniques is provided. Khandare S., and Shrawankar U. (2015) proposed a digital image watermarking algorithm for secured and classified data transmission which works on bit depth plane. The system is consists of two processes. At first the image is translated into classified information through maximum likelihood categorization and fuzzy logic. In the later process the classified image is got copyright protected by means of watermarking. Xiang-yang et al. (2015) developed a robust digital watermarking scheme based on local polar harmonic transform. The watermark inserted through this algorithm, can sustain against several signal processing noises as well as geometric distortions. Moreover the watermark does not cause any visual distortion for this embedding process. A comprehensive sensing method based watermarking method was introduced by Hong, L. et al. (2016), where the original image is encrypted with the sensing process. A Scalar-Costa algorithm is involved here to implant the watermark into the encrypted image. The study of the practice confirms supremacy in terms of robustness and hiding capacity. Hu Hwai-Tsu & Ling-Yuan Hsu (2016) used mixed modulation to develop a blind digital image watermarking scheme. Here watermark embedding is executed through Quantization index modulation and Relative modulation. This is basically a discrete cosine transfer domain based algorithm. For the transfer coefficients with small estimation differences, the relative modulation is activated for the watermark implanting process. If the estimation variation surpasses the preset boundary threshold the Quantization index modulation is drawn on. To close down the concept of verification via password, Wioletta and Ogiela (2015) projected a bimodal biometric validation based digital image watermarking scheme. In this technique a fingerprint along with iris biometrics is considered as watermark and embedded into a sovereign region of the cover image to form the watermarked image. The testing results confirm that the projected system facilitates authentication of images with a remarkable precision level. A discrete wavelet transform based digital image watermarking algorithm using probabilistic neural network was projected by AL-Nabhani et al. (2015) where robustness is considered as a top priority. In this approach a Haar filter is utilized with DWT to embed binary watermark in preferred coefficient regions of cover image. In the time of extraction of the watermark a probabilistic neural network is exploited. It is revealed from the experimental results that the method is useful to overcome the trade-off between imperceptibility and robustness. A novel color image watermarking scheme is developed in spatial domain by Thongkor Kharittha et al. (2015). This is a blind method where regularized filters are utilized to insert watermark within the blue color component of the cover image. A hologram authentication scheme using reversible fragile watermarking was developed by Chan Hao-Tang et al. (2015). In this technique watermark is embedded into hologram image in transform domain, and then the image is laid up in spatial domain. The resolution of the image is restricted to provide transparency to the watermarked image. Zhou Wujie et al. (2016) proposed a fragile watermarking scheme for stereoscopic images that could be used for authentication through tamper detection. Here the embedding process is performed using just noticeable difference technique. The results show that the projected scheme provides better security with the hiding capacity and imperceptibility being justified. Sadreazami Hamidreza et al. (2016) introduced a new watermark decoder, designed in contourlet domain. This is basically a multiplicative decoder that utilizes the standard inverse Gaussian Probability Density Functions as a prior for the contourlet coefficients of images. Digital watermarking technique using Singular Value Decomposition and Discrete Wavelet Transform is also a new trend providing higher robustness, Shah P. et al. (2015). In this approach initially both of the cover image and watermark image are decomposed in the course of Discrete Wavelet Transform followed by Singular Value Decomposition in LL band. In next phase, through a scaling operation, the watermark values are injected by detecting and replacing the singular values in every sub-band. An HVS

(human visual system) based adaptive image watermarking scheme was developed in spatial domain by Sur A. et al. (2009). In this technique watermark is embedded into the least salient regions of the cover image providing a better perceptual transparency for the watermark. A spectral residual based saliency map model was utilized in digital watermarking model was introduced by Basu A. et al. (2015). In this approach, first the cover image is segmented according the pixel saliency obtained from the saliency map. The watermark bits are adaptively embedded into the image in such a manner that the least salient regions contain maximum amount of information. The FPGA implementation of this algorithm was also developed for real time execution. In another approach by Basu A. et al. (2016) described a further saliency based algorithm where utmost data is implanted into most salient regions. The experimental results show that this technique provides a better data transparency than the previous method according to the human visual stimuli. Tsai C. et al. (2005) introduced reversible technique in data hiding process for binary images and a lossless reform of the image is done using pair-wise logical calculation. Another reversible data hiding scheme was developed by Gui X. et al. (2014) where an adaptive data embedding is performed based on generalized prediction-error expansion. This technique provides an increased payload capacity.

WATERMARK EMBEDDING AND EXTRACTING FRAMEWORK

This proposed algorithm is developed based on LSB replacement process as it is a spatial domain approach and easy to implement in hardware. Moreover through this technique the watermark can be made robust against several signal processing attacks like cropping, lossy compression or addition of any undesired noise. The watermark, being injected through replacing the LSBs, does not make any visual distortion to the cover image pixels.

The authors have chosen a gray image of size $A \times B$ as cover image and a $C \times D$ binary image as watermark to implement the algorithm of watermark insertion and extraction.

Let the cover image (I_c) and watermark (I_w) is defined by equation (1) and (2) respectively.

$$I_c = \{ i(a,b): 0 \leq a < A, 0 \leq b < B \wedge i(a,b) \in [0, 1, 2, \dots, 255] \} \quad (1)$$

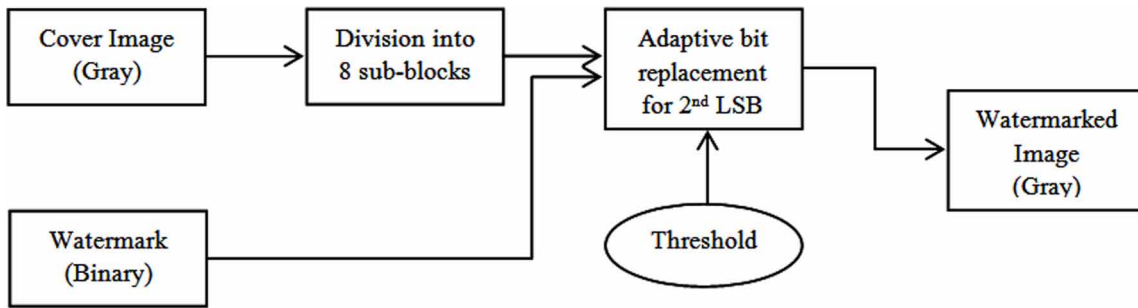
$$I_w = \{ i(c,d): 0 \leq c < C, 0 \leq d < D \wedge i(c,d) \in [0, 1] \} \quad (2)$$

Where $i(a,b)$ is any cover image pixel consists of 8 bits and $i(c,d)$ represents any watermark bit.

Watermark Insertion Procedure

The insertion or embedding process has been illustrated in Figure 2. Here first each of the cover image pixels is segmented into eight sub-blocks. Thus each block contains one bit at a time. For each cover image pixel an adaptive bit replacement is performed for the block consists of the second least significant bit. The bit is replaced with the watermark bit if the cover image pixel value satisfies a certain threshold value i_t . The value of i_t can be varied suitably within the range of 0 to 255. Bits of all other sub-blocks together with the replaced watermark bit construct the watermarked image pixel. This process continued for all the pixels and multiple insertion process can be performed for a better robustness. It is obvious that the size of the original cover image and the watermarked image are same.

Figure 2. Block Diagram for watermark insertion



If the bits in the sub-blocks for any pixel $i(a,b)$ of the cover image I_C are noted as x_0, x_1, \dots, x_7 (from LSB to MSB), then the watermarked image I_E can be defined as,

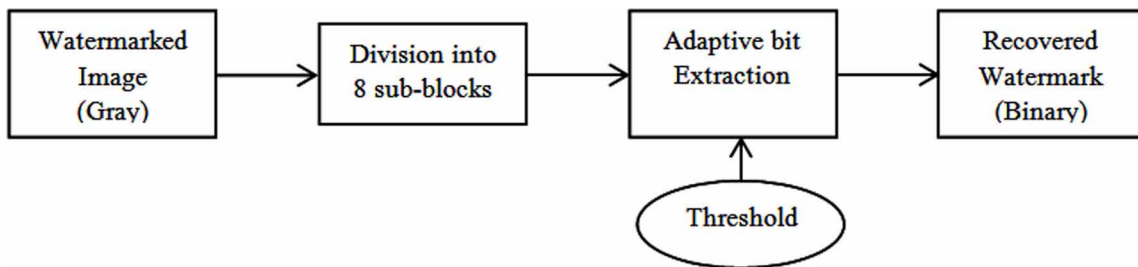
$$\begin{aligned}
 I_E &= x_0 + 10.i(c,d) + \sum_{n=2}^7 10^n x_n \text{ for } I_C \geq i_t \\
 &= \sum_{n=0}^7 10^n x_n \text{ otherwise}
 \end{aligned} \tag{3}$$

Where $i(c,d)$ is the watermark bit present in the queue at that time instant.

Watermark Extraction Procedure

Similarity of a recovered watermark to the original one defines the authentication or originality of the cover object. Watermark extraction is performed through a method just reverse to the embedding algorithm. Here first the watermarked image pixels are segmented into 8 sub-blocks in a similar manner. Then the same threshold, used in during insertion process, is applied to obtain an adaptive extraction routine. Depending on the threshold value, 2nd LSBs from the image pixels are extracted. These retrieved bits together form the watermark that shows the novelty. The block diagram for watermark extraction is shown in Figure 3.

Figure 3. Block Diagram for watermark extraction

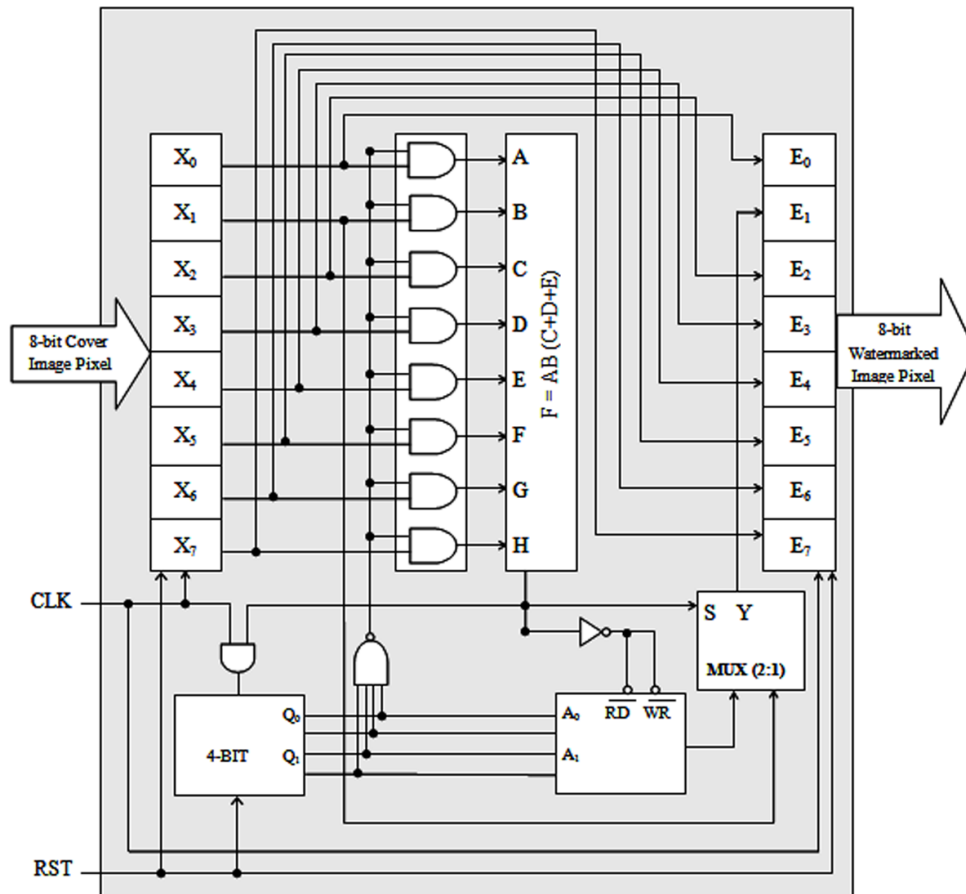


HARDWARE IMPLEMENTATION OF WATERMARK EMBEDDING AND EXTRACTING ALGORITHMS

The proposed watermarking scheme is a simple copyright protection method. It is already discussed that copyright protection is a vital issue in digital communication and digital watermarking is the best solution to serve the purpose. So, this proposed methodology can be very useful to the owners willing to set copyright to their digital properties. For the software execution a system set-up is always required which may not be desirable for every time. Actually on-chip implementation is more effective than software as it leads to automation and distinct performance. Moreover running time is also justified in hardware or on-chip execution. Therefore, real-time implementation of this software based program is required for a fast execution with less power. Providing a better flexibility, easy execution and flawless performance, FPGA (field programmable gate arrays) techniques are mostly favored for hardware implementation. Similar to the software design, the hardware framework of any watermarking scheme also consists of two different algorithms: (i) Watermark Insertion and (ii) Watermark Extraction.

There are several units in both data embedding and extracting blocks and utilization of those units are discussed below. The FPGA architecture for watermark insertion is shown in Figure 4.

Figure 4. Block Diagram for FPGA design of watermark insertion



Watermark Insertion Architecture

The embedding process starts with a cover image and a watermark being stored into a PIPO (Parallel-In-Parallel-Out) shift register and a 4×4 ROM respectively. Initially the cover image, resized into 8bits sub-blocks, is taken to the shift register. Then it passes through Flow Gate which consists of eight AND gate and its control the flow of data that if sub-blocks goes for watermarking or not. One input of each AND gate comes from output of PIPO and another input comes from 4bit counter which checks 2nd LSB bit of 16 sub-blocks are watermarked or not. The watermark embedding is performed by bit replacement process which depends on the decision of a combinational logic. If combinational logic value greater than or equal to the threshold value (which is “200” in decimal) then the 2nd bit of sub-block is replaced by data which is already stored in 4×4 ROM. ROM Outs preloaded 16bit data at a time and that will fed to Parallel-In-Serial-Out (PISO) register through which serially data replaces the 2nd bit of that 16 sub-blocks via 2:1 multiplexer whose select line comes from output of combinational circuit.

Data are out from encoder via Parallel-In-Parallel-Out (PIPO) shift register. All units of encoder are synchronized by one single clock.

Watermark Extraction Architecture

Extraction of the watermarked from a received image is essential to verify its novelty. Therefore designing a proper extraction algorithm for a corresponding embedding process is a vital issue. The watermark extraction framework also consists of numerous units like as watermark insertion block and some units have same function and utilization also. Here the received watermarked image, considered as the stego-image, is resized also into 1×8 sub-blocks and fed to Parallel-In-Parallel-Out (PIPO) and from there it is passes through Flow Gate (consist of AND gate) which control that al watermarked sub-blocks are passed through and watermark bits or logo are collected or not. The sub-blocks passes through then same combinational logic which is used in encoder and if decimal value of sub-block is equal or greater than threshold value(here this decimal value is “200”) then 2nd LSB is send to a 16bit Serial-In-Parallel-Out (SIPO) and from SIPO we get the watermarked bits or logo. The FPGA block diagram of watermark extraction process is given in Figure 5.

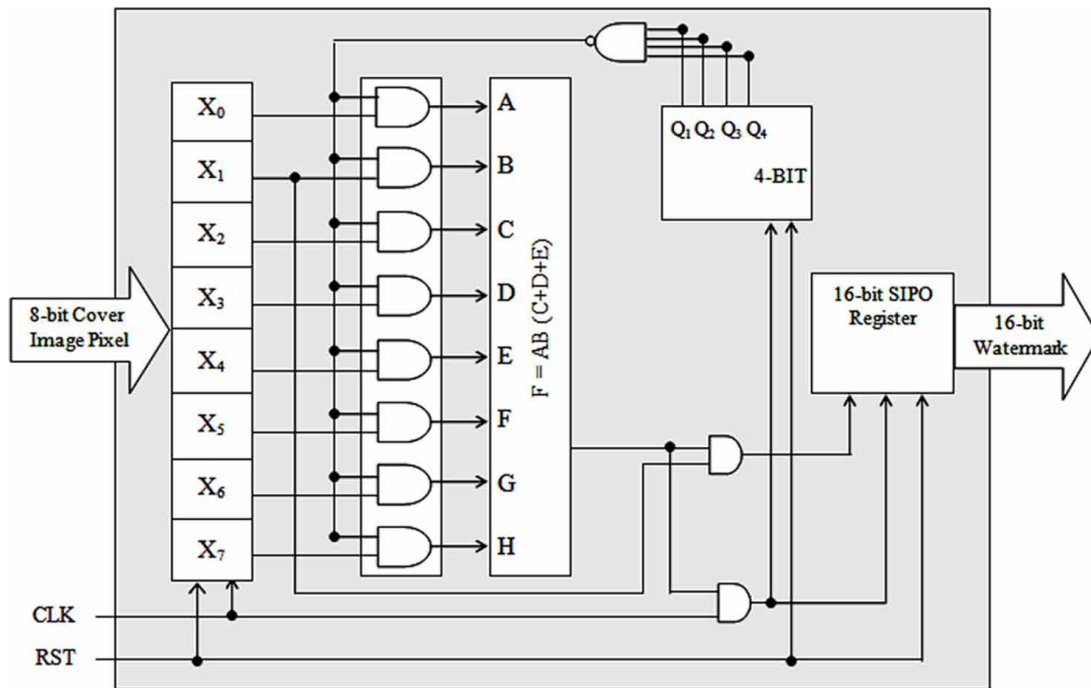
In the next section, the authors have projected how the reversible logic can be utilized in developing the real time circuit design for watermark embedding and extracting process. Here the combinational and sequential circuit units, involved in this process, are constructed through reversible logic gates. The operational behavior of those circuit blocks is also pointed out in this discussion.

INTRODUCTION TO QUBIT AND REVERSIBLE LOGIC CIRCUITS

Classical computing deals with the Boolean algebra where bits are physically represented by high and low voltages on wires or chip. The logic quantities process information in a sequence of ‘0’ and ‘1’ i.e. the digital data are quantized in two states i.e. ‘1’ (as high) and ‘0’ (as low). So, at a particular time instant it is considered to be in one state condition for the basic building blocks of the logic family like transistor, capacitor etc. But in practical the time taken for every transistor or capacitor to exchange states is quantifiable in billionths of a moment. Thus from the quantum-mechanics view point at any time instant the state of an information bit can be described in many different ways, Dasgupta S. et al.,

(2006). For an example, if the ground or OFF state is noted as $|0\rangle$ and the excited or ON state is noted as $|1\rangle$, then according to the superposition principle of quantum theory, for a single bit operation the state at any time instant can be defined as $c_0|0\rangle + c_1|1\rangle$ where, $|c_0|^2 + |c_1|^2 = 1$. Thus the coefficients c_0 and c_1 can be real or imaginary to satisfy the principle. Such a superposition, $c_0|0\rangle + c_1|1\rangle$, is the elementary unit of encoded data in quantum computers and it is known as qubit. A qubit in quantum computation is analogous to an electron in a magnetic field. Spin-up and spin-down are two preliminary states of an electron such that the former state is aligned to the field and the other is opposite to the field. An external energy pulse causes changes in states of the electron spin. For a certain amount of energy applied to a particle, superposition principle states that the particle can be in both of the states at the same time instant. A qubit, having superposition of $|0\rangle$ and $|1\rangle$, describes the same scenario and thus n number of qubits results in n^2 calculations in a single step. This is the exponentially increased proficiency over conventional computation achieved by the quantum computers. The computers based on quantum principle are exponentially more powerful to solve factoring in polynomial time. As a result, the internet transaction in quantum world undergoes security problem. Therefore the internet security protection relevant to the modern quantum computation becomes a challenging issue once again. Moreover throughout the last few decades, researchers successfully performed in quantum computation inspired network security and intelligence like Cryptography, Mayers D. (1998), image clustering, Pappas (1992), neural networks Rigatos, and Rzafeastas (2006), Meng and Gong (2010) evolutionary algorithms, Vlachopiantts (2008), Zhang G. (2011), genetic algorithm, Han and Kim (2000) and others. Thus the quantum computation has acquired preferences in advanced digital signal processing.

Figure 5. Block Diagram for FPGA design of watermark extraction



The reversible logic was introduced by Feynman (1982, 1986) to link up the quantum principles with the classical computation. A system will be said reversible if it consists of n number of outputs for n number of inputs so that the input state of the system could be achieved from the output states at any time instant. This seems to have no information loss in reversible methodologies. Information loss results in energy dissipation in irreversible hardware computation. Landauer's research states that the quantity of energy dissipated for every irreversible bit action is at least $KT \ln 2$ joules, where K is the Boltzmann's constant $= 1.3806505 \times 10^{-23} \text{ m}^2 \text{ kg}^{-2} \text{ K}^{-1}$ (Joule/Kelvin) and T is the temperature at which operation is carried out, Landauer R. (1961). The amount of heat generated for one bit information loss is negligible with respect to the room temperature. But the heat generation is significant for a high speed complex computational program where numerous information bits are lost. In this scenario the performance of the system gets affected by the excessive heat that results in a cutback of the life span of the components. In 1973, Bennett stated and proved that the energy dissipation can be reduced for the systems those permit to regenerate the inputs from received outputs, Bennett C.H. (1973). In addition reversible computation perks up energy efficiency that mostly boosts up the routine speed of the circuits. The portability of devices also enhanced through using reversible logic circuits as these logics reduce the size of the circuit elements to atomic size limits.

In establishment of any logic, reversibility means there should be no information concerned with the computational states that can be lost, so that the computation of any state from its previous or subsequently states through forward and backward computing process. This conditional function is acknowledged as logical reversibility. But the payback of logical reversibility is achieved only after making physically use of reversibility. For a device, physical reversibility fundamentally states that the analogous circuit operation does not dissipate any energy to heat. Therefore it is obvious that absolute physical reversibility is practically unfeasible. In a computing system, heat is generated with the changes of voltage levels from positive to negative or in other words, bits from zero to one. The largest part of the energy required to make that state modification is sent out in form of heat. Reversible circuit elements steadily shift charges from one node to the next in spite of altering voltages to new levels. In this fashion, a very diminutive amount of energy can be expected to lose on each alteration. Thus reversible computing sturdily influenced the practice of designing digital logics. In digital watermarking reversible logic can be utilized to recover the original watermark in terms state of inputs from the outputs i.e. the received watermarked image.

A circuit having n number of Boolean variables is reversible if it consists of exactly same number of inputs and outputs and there exists a unique pattern for inputs to map an inimitable output. Another essential criterion for a reversible logic circuit is that there should be no Fan-out. It is obvious that required input and outputs are not to be of same quantity. The constant inputs and garbage outputs are introduced to resolve this crisis. The constant inputs are to be retained constant (0/1) with the intention of synthesizing the given logical operation. Whereas the garbage outputs are the outputs, present in a reversible logic operation, which are unused but essential to attain reversibility. So, for a reversible logic circuit,

$$\text{Actual Input} + \text{Constant Input} = \text{Actual Output} + \text{Garbage Output}$$

The number of primitive reversible logic gates required to realize the circuit is known as the Quantum Cost.

A number of logic gates are available to achieve the reversible property. Few of them are discussed here.

Feynman Gate

The Feynman Gate is a 2*2 reversible logic gate, also known as ‘controlled-not’ or ‘quantum XOR’ gate. Its quantum cost is measured as 1. For input vector I(A,B) and output vector O(X,Y) the truth table is shown in table 1. The logic operation is expressed in Figure 6(a).

Table 1. Truth table for Feynman Gate

A	B	X	Y
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

From the truth table it is clear that the output Y acts as a NOT gate with respect to the input B when A is set as 1. That’s why this is called controlled NOT. Again for B = 1, both outputs copy the value of A, i.e. acts as a copying gate.

Double Feynman Gate

The 3*3 Double Feynman Gate has a quantum cost double to the Feynman Gate. If the input and output vectors are I(A,B,C) and O(X,Y,Z) then $X=A$, $Y=A \oplus B$ and $Z=A \oplus C$. The input output relationship is reflected from the truth table given in table 2 and operational diagram described in the Figure 6(b).

Toffoli Gate

The logic operation of Toffoli gate or 3*3 Feynman gate or controlled-controlled-not gate, having quantum value 5, can be described as $X=A$; $Y= B$ and $Z= AB \oplus C$. As shown in Figure 6(c), here two inputs A and B act as control inputs to obtain the output Z as a complement of input C. the truth table of this gate is obtained from table 3.

Peres Gate

The logic operation of a 3*3 Peres gate with the input variables A, B, C and the output variables X, Y, Z is defined as $X=A$; $Y= A \oplus B$ and $Z= AB \oplus C$. The quantum cost of a Peres gate is measured as 4. The truth table and the logic operation of a 3*3 Peres gate are shown in table 4 and Figure 6(d) respectively.

Fredkin Gate

In case of a 3*3 Peres gate consists of three input variables A, B, C and three output variables X, Y, Z, the reversible logic is built up as $X=A$; $Y= \bar{A} B \oplus AC$ and $Z= \bar{A} C \oplus AB$. Its quantum cost is calculated as shown in table 5.

Table 3. Truth table for Toffoli Gate

A	B	C	X	Y	Z
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Table 2. Truth table for Double Feynman Gate

A	B	C	X	Y	Z
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	1	1
1	0	1	1	1	0
1	1	0	1	0	1
1	1	1	1	0	0

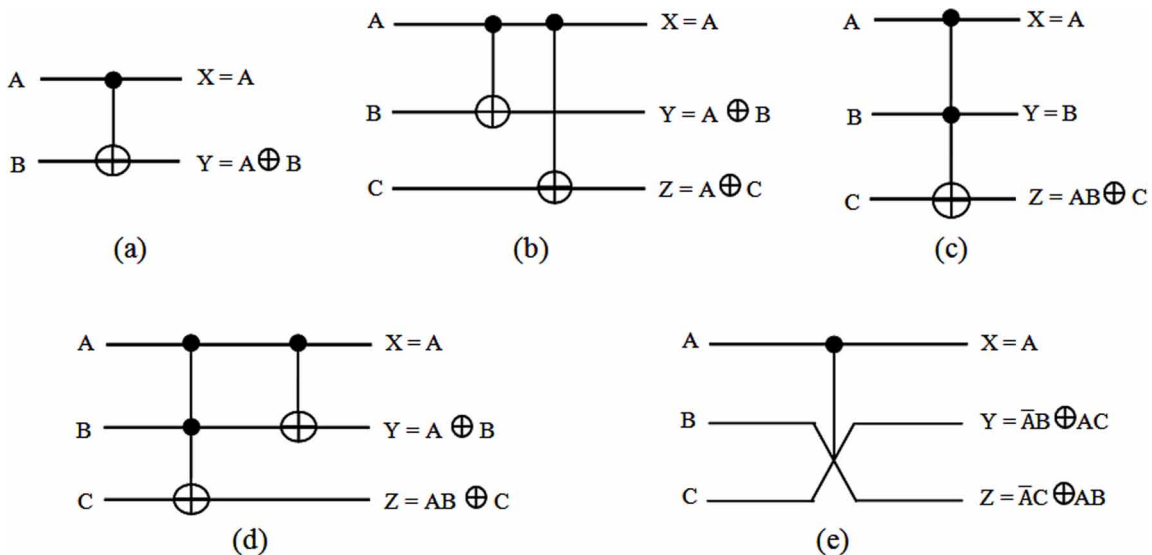
Table 4. Truth table for Peres Gate

A	B	C	X	Y	Z
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	1	0
1	0	1	1	1	1
1	1	0	1	0	1
1	1	1	1	0	0

Table 5. Truth table for Fredkin Gate

A	B	C	X	Y	Z
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	1	0
1	1	0	1	0	1
1	1	1	1	1	1

Figure 6. Block Diagram for (a) Feynman Gate (b) Double Feynman Gate (c) Toffoli Gate (d) Peres Gate (e) Fredkin Gate



LITERATURE SURVEY ON REVERSIBLE LOGIC INSPIRED DATA HIDING SCHEME

Besides surfacing on the various states of watermarking, this discussion also focused on the reversible logic synthesis methods which carry out a major role of this proposed work. Composition and decomposition are two well known multi level and very powerful tool used in synthesis procedures for reversible logic, Maslov D. et al. (2003). In composition methods, small and familiar reversible gates are composed to play the function of any complex reversible block, Dueck et al (2003), Miller et al. (2003). Then applying a conventional logic synthesis process, the network is synthesized. Decomposition methods operate like a top-down diminution of the function from the outputs to the inputs, Al-Rabadi A.N. (2004), Perkowski M. et al. (2001). Here a complex function is decomposed into several functions and these are individually implemented by distinct reversible circuits. The decomposition process is practiced based on several models like Ashenhurst-Curtis (AC) decomposition, Modified Reconstruct ability Analysis (MRA), Bi-decomposition (BD), etc. EXOR logic based methods are used mainly for heuristic synthesis Shende V.V. et al. (2002), Maslov D. et al. (2005). Combination of Toffoli gate, operating on EXOR logic, is utilized here to perform the reversible function. Genetic reversible algorithms introduce the evolutions concept proposed by Darwinian, Lamarckian and Baldwinian to minimize the logic functions Lukac M. et al. (2002), Lukac M. et al. (2003). The main drawback of these techniques is their poor scalability. Spectral techniques proposed by Miller (2002) are used to locate the finest gate to be composed in terms of NOT, CNOT or Toffoli gate. Then the gate is formed in a cascade-like manner. A set of the set of the actual outputs from each sub-block or their negations together describes the output function. To execute any Boolean function through reversible logic, binary decision diagram (BDD) methods can be applied Al-Rabadi A.N. (2004), Wille et al. (2008). In BDD based approaches all possible minimal networks are considered to find the most effective one in terms of quantum cost or circuit complexity. Thus it leads to a cheaper and faster realization. In the next section various watermarking techniques using these reversible logic has been discussed briefly.

As already discussed, digital watermarking embeds significant information (watermark) into multimedia for copyright protection. The insertion of watermark may cause distortion in the cover media. Furthermore, in some cases, the effects on the cover object may not be fully reversible after mining of the concealed insertion. Utilizing the perceptual imperfectness of human visual system the distortion can be optimized but the irreversibility cannot be tolerated for certain responsive applications like medical imaging or any legal issues. A loss less data hiding scheme obtained exigency in this purposes. Reversible watermarking, also called loss less data hiding allows us to implant a moderately large quantity of information into an image in such a manner that the inserted data can be rebuilt from the watermarked image. Thus the reversible logic serves the purpose to overcome the tradeoff between imperceptibility and payload capacity. Moreover, these reversible watermarking methods can provide robustness against most of the signal processing attacks. The watermark extraction process can also be made blind using reversible logic. So, these types of practices acquired fondness in copyright protection for multimedia objects like images and electronic documents. Numbers of reversible watermarking schemes are developed depending on several logics and methods like difference expansion, lossless data compression, bit planes modification, integer-to-integer wavelet transform, bijective transformation, histogram shifting and others. Some of existing reversible watermarking frameworks are discussed here.

Mintzer et al. (1997) first brought in the perception of a reversible watermark. They proposed a watermarking scheme where the original image could be formed from the watermarked image by taking off the watermark. This removal of the mark described the utilization of reversibility in watermarking. A hash function based method was proposed by Honsinger et al. (2001) where modulo-256 addition is used in implantation of hash value of the metadata. This algorithm enables reversibility and hampers the fact of watermark extraction under salt-and-pepper artifacts. Fridrich et al. (2001) introduced the practice of constriction of a set of chosen features from an image and insert the payload into the compressed region with a lossless computation scheme. Goljan et al (2001) developed a fragile data hiding scheme using called RS method. Here the watermark embedding is performed on the basis of the pixel group status which through a flipping operation using discrimination functions. This is also a lossless data approach. The exhaustive study of the RS method for JPEG images in DCT (Discrete Cosine Transfer) domain was made by Fridrich et al. (2002). Fridrich et al.'s methodology was improvised by the G-LSB (generalized-LSB) technique proposed by Celik et al. (2002). In their proposal a binary watermark is embedded into a gray level cover image through a simple LSB replacement method. The compression proficiency is enhanced by utilizing prediction based conditional entropy coder applied to the flat region of the input image. Celik et al. (2005) extended this version to obtain a generalized lossless data insertion. A semi-fragile lossless data hiding scheme is proposed by Vleeschouwer et al. (2003) which can sustain against high-quality JPEG compression. Here every information bit is associated to a pixel group formed by two equally distributed pseudo-random sets of pixels.

An IP (Inverted Pattern) based LSB substitution technique is developed by Yang (2008). The uniqueness of this approach is that the IP determines the hidden image regions to be inverted or not and this is utilized in the time of data extraction. Another prediction error based reversible data hiding approach is proposed by Thodi and Rodriguez (2004) where histogram shifting also utilized to calculate the correlation between adjacent pixels. This technique offers a low distortion to the cover image. A circular interpretation is applied to the bijective transformations of cover image histograms to enrich the rustiness. A further improvement is done by producing a robust statistical reversible method, Ni et al (2008), which is not applicable only for an extremely lossy compression attack. A block based reversible information hiding scheme is developed by Ono et al. (2009) where the data is implanted into certain precise regions like image edges. No location map is required here to specify the hidden bit positions in the embedded image. To increase the payload capacity congruency based watermarking scheme is introduced by Chaumont and Puech (2009). According to their approach, each pixel of the cover image may lies on three states. These are the embedding state where an integer coefficient is to be implanted, to correct state where the pixels are modified without any type of embedding and original state where the pixels are corresponds to the original or unchanged one. The utilization of these three states enhances the embedding capacity.

Lossless compression of bit planes is another type of reversible data hiding framework which can be generated through manipulations of the bit planes and provides a transparent data analysis during embedding and extracting time. Generally the purpose of these methods is to find out the suitable region in the cover image with least redundancy to hold the endorsement data like hash. And assuming the media is not noisy, naturally the preferable regions to hide the hash are provided by the lower bit-planes. Fridrich et al. (2001a) developed a bit-plane compressing based reversible information hiding scheme. In this approach to compress the bit-planes, JBIG lossless compression algorithm, Sayood (2006), is utilized which starts with analyzing the fifth LSB plane.

Another image watermarking scheme was proposed by Song et al. (2009) for substance validation. This approach involves the bit-plane technique in an irreversible watermarking where the image feature obtained from least significant bit-plane is implanted into a preset bit-plane by regulating the analogous sub-band values. A relative or parallel method to the bit-plane compression is Bit Plane Complexity Segmentation (BPCS) which is applicable to the irreversible data embedding processes. It was first set up by Kawaguchi and Eason (1998). The purpose of this improvisation was to modify the deficiencies of simple LSB manipulation methods. Although there is no likeliness between the complexities of any two images, in this approach two different image complexities were deliberated. The work focused on determining the number of concerned pixel areas can be utilized to define the complex regions. Hirohisa (2002) and Ramani et al (2007) also developed some watermarking schemes based on this BPCS concept. Hirohisa (2002) introduced two new complexity events named as the run-length irregularity and the border noisiness to distinguish noisy regions accurately. Ramani et al (2007) proposed a replaceable inverse Wavelet transform (IWT) based methodology where the replaceable IWT coefficient regions were defined by a complex quantification. Thus being developed through irreversible aspects, these research works put some important contributions in the era of digital image watermarking.

The reversible watermarking schemes, discussed till now, are suitable to be performed in spatial domain. The main problem of spatial domain is reduced robustness which can be overcome in transfer domain. In case of classical transfer domain practices like discrete wavelet transform it is not assured that utilization of reversible logic can achieve reversibility properly. This crisis can be conquered through a reversible integer-to-integer wavelet transform based lifting scheme. This is principally a difference expansion oriented computation where flexible pixel pairs are used to embed data or watermark. A location map, generated to trace the positions of the pixels, is utilized to recover the hidden mark properly at the receiving end. The concept of difference expansion based reversible watermarking was pioneered by Tian (2002). In this proposal gray level cover image was taken and the expanded difference numbers between two neighboring pixels were computed to implant the watermark bits into the cover. The hiding capacity of Tian's framework is increased by allowing for triplets instead of the pair of the pixels to embed a pair of watermark bits, Alattar (2003). This is a color image watermarking algorithm where the triplets can be considered either in spatial domain or as cross-spectral pixels. A further extension of this algorithm is performed to obtain an enhanced payload capacity as well as generalization of the data insertion methodology, Alattar (2004), where three bits are hidden in a quad of pixels having different values. It was verified that for required reversible integer transform, the perceptual image quality is affected with the increment of the number of inserting bits. Stach and Alattar (2004) utilize the generalized integer transform for vectors having any arbitrary length. The LSB prediction method proposed by Kamstra and Heijmans (2005) embeds the information enclosed in the most significant bit planes. This is a low payload capacitive scheme to improve image aesthetics. The insertion is performed based on the sorting process of the envisaged LSBs, that depends on an estimation of the prediction feature, also improves the coding adeptness. One more improvement over Tian's (2002) method was made by Kallel et al. (2007). This is a spatial domain approach where the image is divided into several blocks and each block is considered as an array of numerous rows and column elements. These elementary pixels of each row and column generate corresponding authentication codes. These codes are treated as the watermark and embedded into the least significant bit planes of the expanded differences of preferred regions in each block. Kim et al. (2008) improvised the difference equation technique for low capacitive watermarking schemes by simplifying the generation of location map without reference of it at the extracting end. Another modification on difference expansion based execution was done by Yaqub and Jaber

(2006) terms of hiding capacity and computational cost. A set of expandable vectors are produced from the divergence between the median pixels and the other pixel values. Information is embedded into the differences of all probable expandable vectors. Gao and Gu (2007) utilizes both LSB replacement and difference expansion based reversible methodology. The image features, generated from image pixel blocks, are divided into two parts. One of them is embedded through LSB based technique and the other one is hidden into the differences. Thodi and Rodriguez (2007) developed another prediction-error based reversible information hiding scheme that utilizes the intrinsic correlation between neighboring pixels in place of difference expansion method. Lee et al. (2007) established a wavelet transform based reversible watermarking scheme where the wavelet transform of non-overlapping blocks of the cover image is computed and the watermark is embedded into the pixels having high frequency components in transform domain through LSB replacement process.

Information hiding through histogram shifting is another reversible watermarking scheme that was introduced by Ni et al. (2003). Image histogram modification is generally a human visual system based operation, Xuan et al. (2002). In the proposal of Ni et al. first a peak point or zero point is estimated in the image histogram to exploit the hiding capacity. Next by right shifting of the points next to it, vacant points are created at the zero point and another point near it. These vacant points are used to insert the watermark bit. A large number of watermark bits are embedded into the cover image by simply repeating the histogram shifting procedure in multiple times. Although the hiding capacity is limited according the cover image. Information hidden into the image can be recovered by a reverse process. Although this is a spatial domain approach, image histogram can also be formed from an integer-to-integer wavelet transform can also be utilized here instead of the spatial domain image. This algorithm was modified by increasing data capacity through gray-scale pixel adaptation and utilization of the zero points, Ni et al. (2006). Xuan et al. (2004) proposed a spread spectrum based watermarking scheme developed in wavelet transform domain. Later they utilized histogram modification with a threshold to the data insertion to put off overflow and underflow as well as to make this technique loss less and reversible, Xuan et al. (2005). Image histogram with integer wavelets was utilized by Xuan et al. (2006). The Laplacian distribution was engaged in creating more points to enhance payload capacity.

Fallahpur and Sedaaghi (2007) developed another histogram shifting based watermarking scheme. Here histogram is computed through a block based approach and data embedding is performed depending on the position of the zero points and peaks of the image histogram. Difference histogram in sub-sampled images is modified to generate a reversible data hiding scheme in the proposal of Kim et al (2009). Yang et al. (2009) utilize optimal several pairs of peaks and zeroes in the image histogram.

HARDWARE IMPLEMENTATION OF WATERMARK EMBEDDING AND EXTRACTION USING REVERSIBLE LOGIC

Previously a number of reversible logic gates are initially briefed in this chapter. But the author developed their system designs basically using three logic gates – Feynman gate, Fredkin gate and Toffoli gate. The overtures of these three gates are already given. In this section, primarily the transistor implementation of the three logic gates are developed which is the designs of the other blocks using these logic gates.

As discussed earlier, one of the most well known (2*2) reversible gates is Feynman gate in which one of the input bits acts as a control signal. This gate is one-through gate which means that one input variable is also output. Feynman gate acts as a copying gate when the second input is zero by duplicating the

first input at the output. The proposed transistor implementation of Feynman gate is given in Figure 7(a). Figure 7(b) shows the transistor implementation of the Fredkin Gate which requires only 4 transistors.

In the proposed implementation, the output P is directly taken from input A as it is simply hardwired. The existing implementation of the Fredkin gate in literature is with 10 transistors and 16 transistors respectively. Thus proposed design achieves 60% reduction in number of transistors compared to 10 transistors and 75% reduction compared to 16 transistors. It is to be noted that proposed transistor implementation is completely reversible suitable both for forward as well as backward computation. The transistor logic execution for Toffoli gate is shown in Figure 7(c). From this figure it is exposed that for the projected design 12 number of transistors are required to carry out the reversible operation through Toffoli gate. In Figure 8, the characteristic plots of these three gates are displayed taking $V(A), V(B), V(C)$ as the input pulses and $V(1), V(2), V(3)$ as the output pulses with a pulse width of 10ns and a time period of 20ns. The power dissipation for each state alternation in these gates for different operation frequency has been calculated for forward computation as well as backward computation also. The experimental results are shown through tabular form in table 6.

Along with these three gates, T Flip-flop and D flip-flop are also required to develop the operational blocks involved in watermark insertion and extraction process. Therefore obligatorily authors have designed a T flip-flop and a D flip-flop using reversible logic gates.

Figure 7. Proposed Transistor Implementation for (a) Feynman Gate, (b) Fredkin Gate, (c) Toffoli Gate

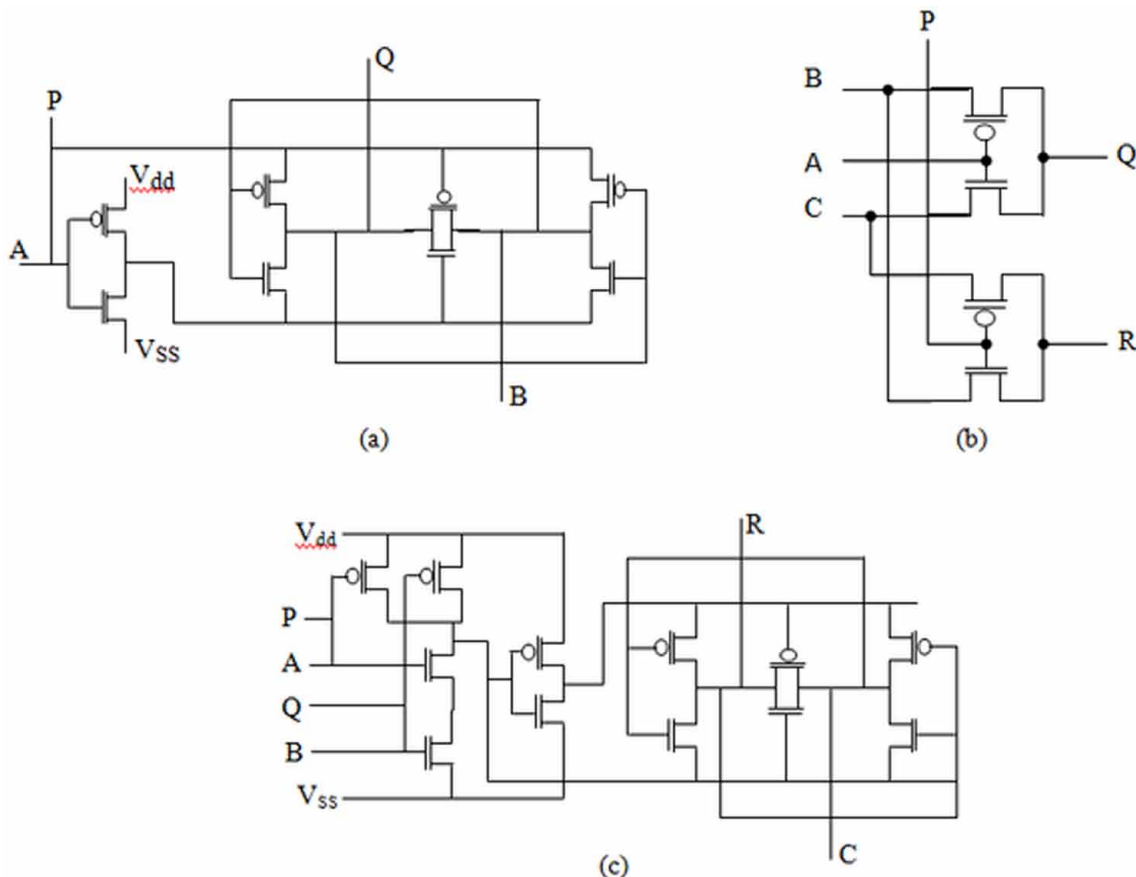
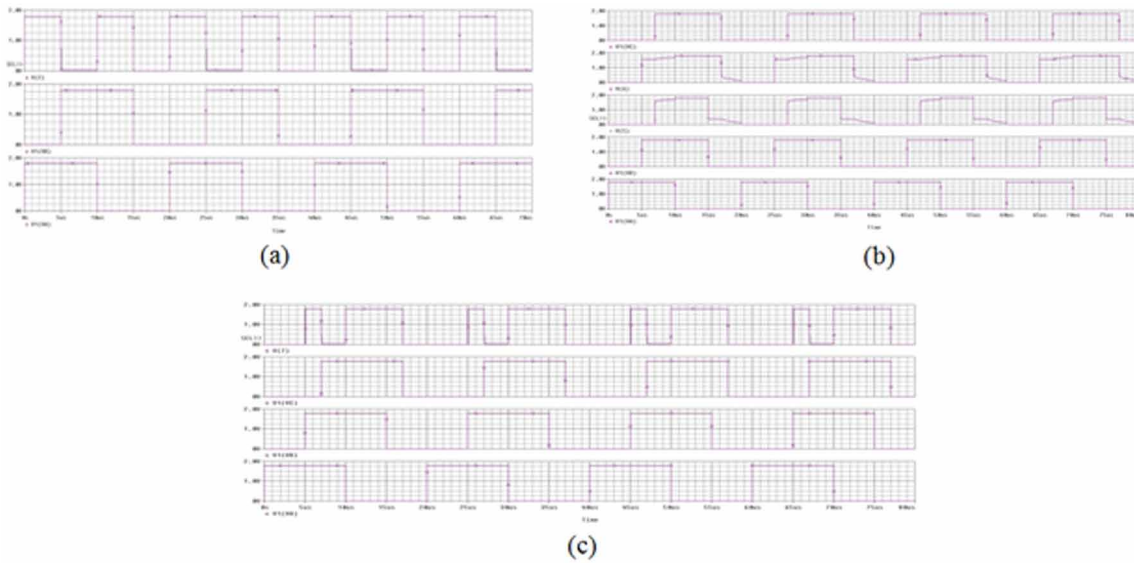


Figure 8. Proposed Transistor Implementation for (a) Feynman Gate, (b) Fredkin Gate, (c) Toffoli Gate



T Flip-Flop and D Flip-Flop Using Reversible Logic Gates

If the excitation of a T flip-flop is noted as T and the n^{th} state output is considered as the present state and noted as Q_n , then with addition to the clock pulse Clk, the characteristic equation of the flip-flop can be written as $Q_{n+1} = \overline{(T \cdot Q_n)} \cdot \text{Clk} + (T \cdot Q_n) \cdot \text{Clk}$. This equation can be directly mapped to Toffoli gate. The fan-out can be avoided and complementary output can be generated by using Toffoli gate with Fredkin Gate. The proposed design is shown in Figure 9(a). As shown in the figure, the first two inputs of the Toggle gate act as the clock input and the excitation T respectively and the other one is connected to the second output of the Fredkin gate. The first two outputs of it are made grounded and the other output, which is basically the output function of T flip-flop, is fed to the first input of the Fredkin gate. The other two inputs of the Fredkin gate are set to '1' and '0' respectively as default value. Therefore according to the logic, the first output of this gate provides its first input value and considered as output function of T flip-flop. The default values of the two inputs of this gate enable to copy the first output value to the second output value which is fed back to the last input of the Toffoli gate. A complement of the flip-flop output is obtained from the last one among the Fredkin gate outputs.

In case of D flip-flop, the characteristic equation with input excitation D is defined as, $Q_{n+1} = D \cdot \text{Clk} + \overline{Q_n} \cdot \text{Clk}$. This logic operation is executed through reversible logic using a Feynman gate sequentially connected to Fredkin gate as shown in Figure 9(b). Here the first two input of Fredkin gate act as the clock input and the input excitation D respectively and the other one is latched with the first output of the Feynman gate. The first two outputs of the Fredkin gate is grounded and the last output, producing the D function is fed to the first input of the Feynman gate. The other input of this gate is set to a default value of '0' and thus both of the outputs of the Feynman gate becomes its input value i.e. the D function. One of these output port is fed to the input of Fredkin gate and the other one is considered as the output of the flip-flop.

Table 6. Power calculation for forward and backward computation in (a) Feynman Gate

Working Frequency	Power Dissipation in Forward Computation (in watt)	Power Dissipation in Backward Computation (in watt)
1 KHz	1.06×10^{-9}	1.60×10^{-9}
10 KHz	1.05×10^{-8}	1.02×10^{-8}
100 KHz	1.02×10^{-7}	9.65×10^{-8}
1 MHz	1.01×10^{-6}	9.68×10^{-7}
10 MHz	1.01×10^{-5}	9.66×10^{-6}

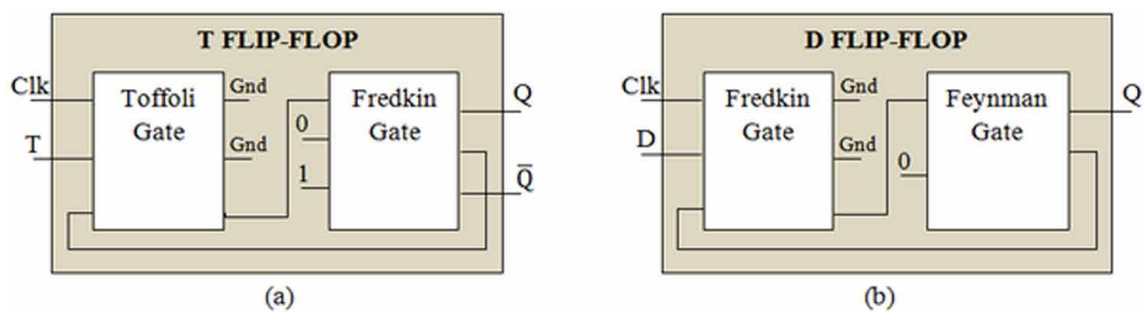
Table 7. (b) Fredkin Gate

Working Frequency	Power Dissipation in Forward Computation (in watt)	Power Dissipation in Backward Computation (in watt)
1 KHz	4.53×10^{-12}	4.50×10^{-12}
10 KHz	9.72×10^{-12}	8.90×10^{-12}
100 KHz	3.37×10^{-11}	2.27×10^{-11}
1 MHz	1.95×10^{-10}	1.06×10^{-9}
10 MHz	1.07×10^{-9}	4.98×10^{-9}

Table 8. (c) Toffoli Gate

Working Frequency	Power Dissipation in Forward Computation (in watt)	Power Dissipation in Backward Computation (in watt)
1 KHz	1.04×10^{-9}	1.60×10^{-9}
10 KHz	1.05×10^{-8}	1.02×10^{-8}
100 KHz	1.02×10^{-7}	9.65×10^{-8}
1 MHz	1.01×10^{-6}	9.68×10^{-7}
10 MHz	1.01×10^{-5}	9.66×10^{-6}

Figure 9. Block diagram for implementation of Flip-flops using reversible gates: (a) T Flip-flop, (b) D Flip-flop



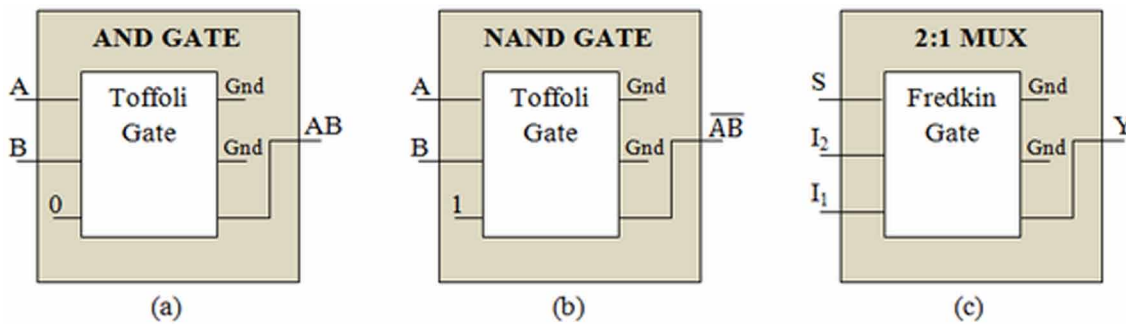
Now the discussion is lead to the implementation of the functional sub-blocks required in embedding and extracting block. According to the block diagrams shown in Figure 5 and 6, the functional circuits required to the process of watermarking and recovery of the watermark are 2:1 MUX, 16-bit ROM, 4-bit synchronous up/down counter, AND gate, NAND gate and register (PISO, PIPO, SIPO). These logic circuits should be realized using reversible operation.

AND Gate, NAND Gate and 2:1 MUX Using Reversible Logic

Each of the AND and NAND gate can easily implemented simply by using a single Toffoli gate only. In both of the cases the first two inputs of the Toffoli gate are considered as the inputs of AND or NAND gate. The third input value determines whether the Toffoli gate will act as an AND gate or a NAND gate. For the value is set to ‘0’ or ‘1’ then the gate behaves like an AND gate or NAND gate respectively. The first two outputs of the Toffoli gate is grounded and the last one operates like AND or NAND function as shown in the block diagrams given in Figure 10(a) and (b).

Fredkin gate itself operates like a 2:1 MUX when the first input is considered as the select line (S) and the other two as MUX inputs (I_1, I_2). The MUX output Y can be defined by the equation $Y = \bar{S}I_1 + SI_2$. In this design the functional behavior is also achieved from the last output port and the other outputs are made grounded. The operational diagram of 2:1 MUX using Fredkin gate is shown in Figure 10(c).

Figure 10. Block diagram for implementation using reversible logic: (a) AND Gate, (b) NAND Gate, (c) 2:1 MUX



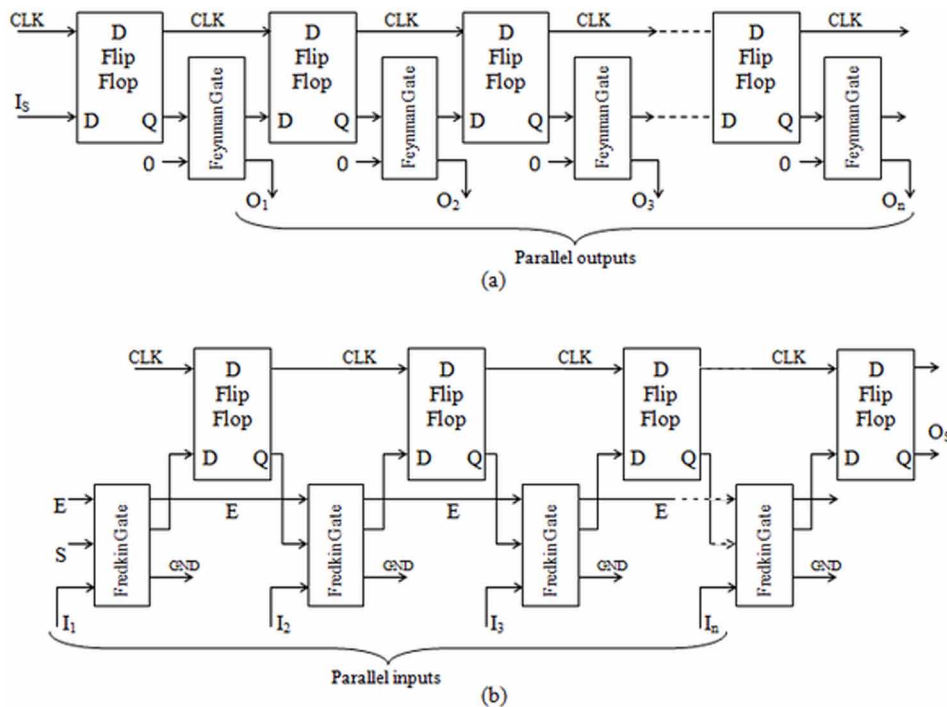
SIPO and PISO Shift Register Using Reversible Logic

A SIPO (Serial-In-Parallel-Out) shift register takes serial input and it makes all the stored bits being available as outputs. Thus a parallel output is produced. Reversible implementation of SIPO shift register using clocked D flip-flops is shown in Figure 11(a). The serial data are entered to the I_s input of the reversible left-most flip-flop while the outputs $O_1, O_2, O_3, \dots O_n$ are available in parallel each output bit Q of the flip-flops. It requires n reversible clocked D flip-flops and n-1 Feynman gates. Thus, it requires a total of 3n-1 gates and produces n+1 garbage outputs with quantum cost 7n-1.

PISO shift register intakes the parallel data and shifts it to the next flip-flop when the register is clocked. Fig shows the reversible implementation of PISO shift register using clocked D flip flops. The operations are controlled by the enable signal E. When E is high, the inputs $I_1, I_2, I_3 \dots I_n$ are loaded in

parallel into the register coincident with the next clock pulse. Again when E is low, the Q output of the flip-flop is shifted to the right by means of Fredkin gate. The desired register output is obtained serially from the n^{th} D flip-flop output port. It allows accepting data n bits at a time on n lines and then sending them one bit after another on one line. It requires n reversible clocked D flip-flops and n Fredkin gates. Thus, it requires a total of $3n$ gates and produces $2n+2$ garbage outputs with quantum cost $11n$. The operational block diagram is shown in figure 11.

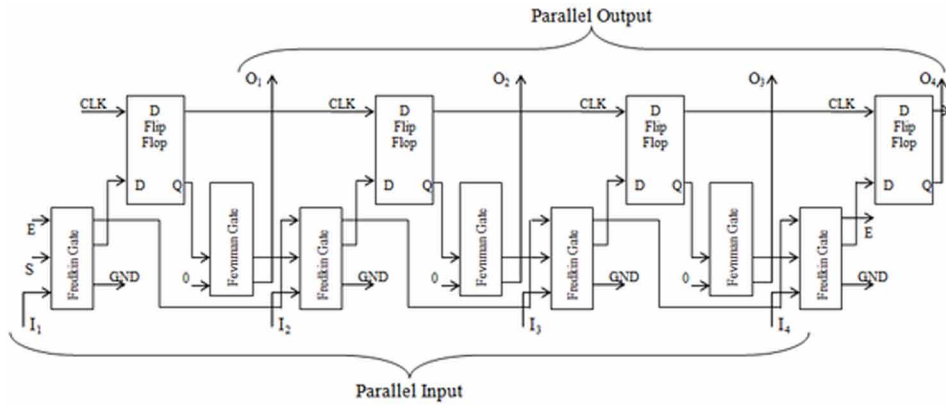
Figure 11. Block diagram for implementation of Shift Register using reversible logic: (a) SIPO (b) PISO



PIPO Shift Register Using Reversible Logic

The purpose of the PIPO (parallel-in-parallel-out) shift register is to take in parallel data shift. Here a 4-bit PIPO shift register has been implemented. A higher order i.e. 8-bit or 16-bit register can be formed by connecting two or four registers in series. As shown in Figure 12, the four bit of input data is applied to a parallel-in/ parallel-out shift register at D_1, D_2, D_3 and D_4 . A proper interconnected circuit, consists of D flip-flops, Feyman gates and Fredkin gates, operates to allow data being shifted one bit position for each clock pulse. The shifted data is available at the outputs Q_1, Q_2, Q_3 and Q_4 . The “data in” and “data out” are provided for cascading of multiple stages.

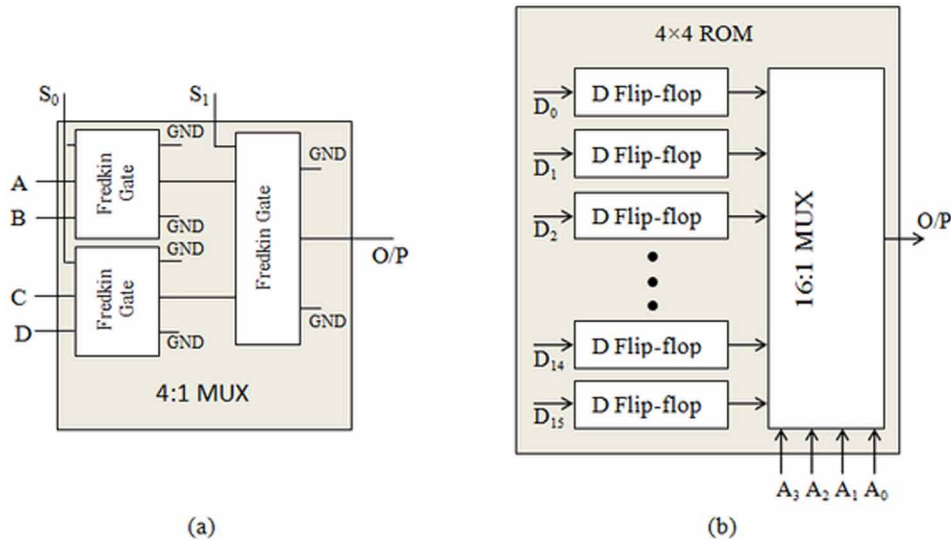
Figure 12. Block diagram for implementation of PIPO Shift Register using reversible logic



4×4 ROM Using Reversible Logic

It can be developed using reversible D flip-flop and 16:1 MUX where the 16:1 MUX is being made using five 4:1 reversible MUX. A reversible 4:1 MUX is a combination of three Fredkin gates, each of which acts like a 2:1 MUX. Figure 13 shows the operational structure of a 4×4 ROM with addition to the 4:1 MUX block diagram using Fredkin gates and reversible D flip-flops.

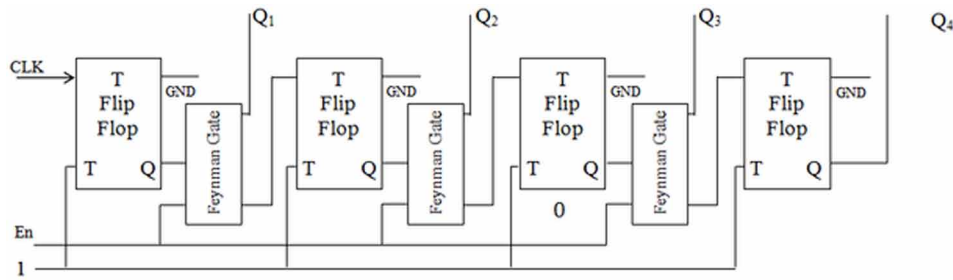
Figure 13. Block diagram for implementation of (a) 4:1 MUX and (b) 4×4 ROM using reversible logic



Up/Down Counter Using Reversible Logic

In an asynchronous counter, the output transition of one Flip-flop serves as a source for triggering other flip-flops. Two inputs are given to circuit i.e. enable and clock pulses in sequence and four outputs Q_1, Q_2, Q_3, Q_4 are obtained. Unlike to the conventional design, T flip-flops are used in this design along with Feynman gates. The control input value decides whether the counter will perform as an up or down counter. A '1' value of the control bit enables up operation whereas for '0' value causes down operation. Figure 14 defines the working blocks of an asynchronous up counter.

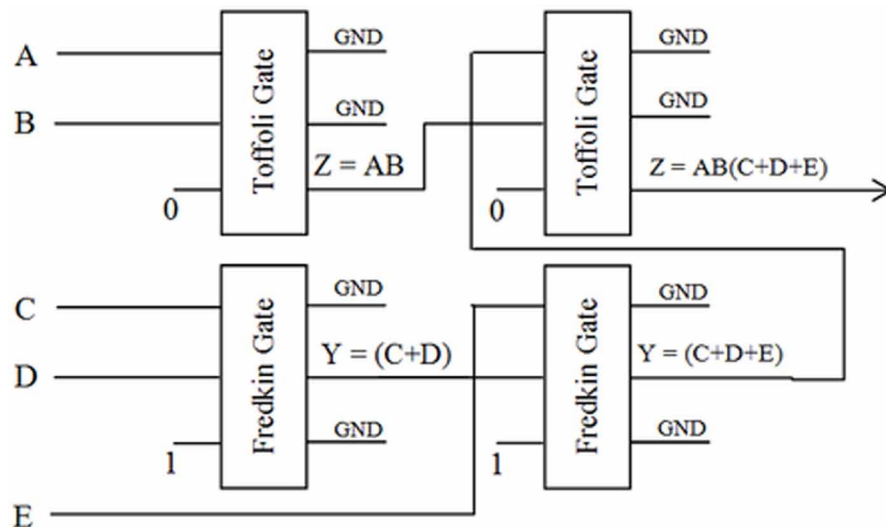
Figure 14. Block diagram for implementation of Up Counter



Combinational Logic to Obtain Proposed Threshold Using Reversible Logic

A combinational logic is introduced to give a threshold in the watermarking process. This logic can also be developed using Reversible circuit. The threshold logic is defined by the function $F=AB(C+D+E)$ of which reversible logic implementation is shown in Figure 15.

Figure 15. Block diagram for implementation of the desired Combinational Logic to obtain threshold



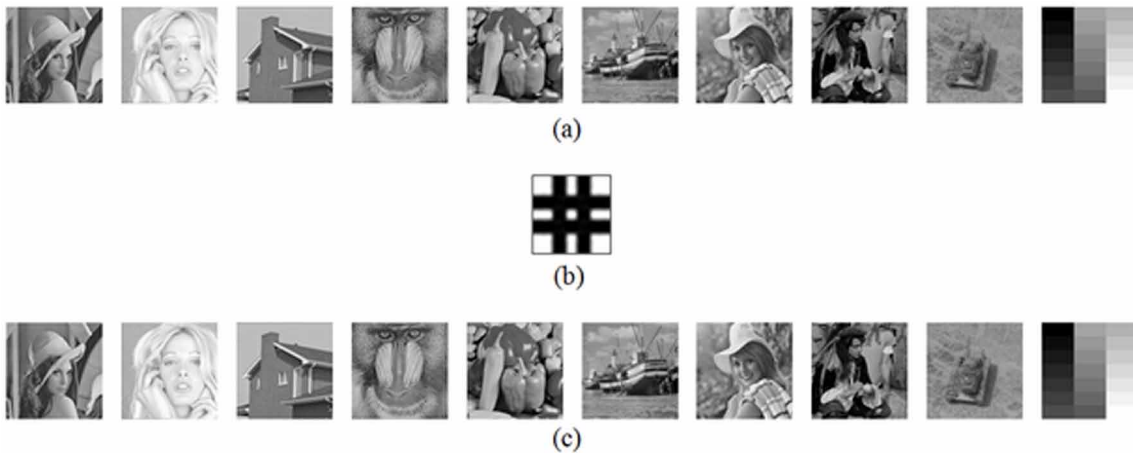
RESULTS AND DISCUSSION

Experimental outcomes for this proposed watermarking algorithm have been achieved in terms of software computation and hardware execution. The acceptability of the logic of the method depends on three qualitative quantity i.e. imperceptibility, robustness and hiding capacity.

Performance Estimation for Software Analysis

The author has chosen a database (USC-SIPI Image Database) of some images as cover images after adjusting each image to a 256×256 gray-scale image. Although all the images of the database are experienced the watermarking process for the same watermark, a few number of images have been shown in Figure 16(a). A binary image of size (16×16) shown in Figure 16(b) is built up to serve the purpose of watermark. The watermarked images obtained as the output of the embedding system for the corresponding original cover images are given in Figure 16(c). And as reflected from the figures, there are no perceptual differences between original and watermarked images perceived by the visual stimuli.

Figure 16. (a) Original cover images (b) Watermark Image (c) Watermarked Images



The visual perception measurement is achieved through some image quality metrics Sinha Roy, S. (2015) Kutter, M. et al. (2000) to differentiate between original image and watermarked image. These perceptual qualities together indicate imperceptibility of the proposed algorithm. From table 9, it is reflected that this algorithm provides increased PSNR typically has a value above 56.45 dB, whereas it is measured maximum (around 57 dB) for Img-2, 6 and 10. The maximum difference is 1 for all the images as the number of maximum LSBs replaced in a pixel is 1. Image fidelity should be 1 for two identical images. Here it is found around 0.9999, which is very close to unity. Middling value of SSIM and SC for all the images are more or less than 0.999, which is also 1 for two indistinguishable images. So, this approach can be considered as a good imperceptible algorithm which also reflects from the values of the other parameters.

Table 9. Imperceptibility measurement table

Parameter	Img-1	Img-2	Img-3	Img-4	Img-5	Img-6	Img-7	Img-8	Img-9	Img-10
MSE	0.128540	0.127869	0.117920	0.123657	0.128296	0.121826	0.122314	0.125977	0.125183	0.122070
LMSE	0.001919	0.002362	0.001861	0.000492	0.001892	0.001137	0.003744	0.000819	0.003406	0.001352
PSNR	56.51	57.06	56.85	55.65	56.00	57.00	56.84	56.34	54.96	57.26
SNR	51.37	55.50	52.55	51.69	51.30	51.91	52.28	49.46	51.63	52.57
MD	2	2	2	2	2	2	2	2	2	2
AD	0.064270	0.063934	0.058960	0.061821	0.064148	0.060913	0.061157	0.062988	0.062592	0.061035
NAD	0.000518	0.000303	0.000427	0.000477	0.000533	0.000470	0.000448	0.000708	0.000473	0.000480
NMSE	0.000004	0.000001	0.000003	0.000003	0.000004	0.000003	0.000003	0.000006	0.000003	0.000003
IF	0.999993	0.999997	0.999994	0.999993	0.999993	0.999994	0.999994	0.999989	0.999993	0.999994
SC	0.999732	0.999809	0.999609	0.999638	0.999740	0.999645	0.999692	0.999725	0.999680	0.999849
CQ	142.209	214.966	153.545	140.852	143.940	145.822	151.658	125.006	137.625	173.532
NQM	36.990	39.269	38.105	37.474	36.812	37.477	37.626	35.619	37.843	34.198
SSIM	0.999671	0.999143	0.999212	0.999782	0.999626	0.999553	0.999422	0.999332	0.999637	0.998700
HS	4212	4190	3864	4052	4204	3992	4008	4128	4102	4000
NCC	0.999869	0.999906	0.999807	0.999822	0.999874	0.999825	0.999849	0.999868	0.999843	0.999927
NAE	0.000518	0.000303	0.000427	0.000477	0.000533	0.000470	0.000448	0.000708	0.000473	0.000480

Table 10 exhibits the robustness of the proposed method against the above said spiteful attacks in comprehensive forms. Although all the images of the database is undergone through these robustness checking process, the effect of the attacks to the image is shown only for a randomly chosen image and the average results have been given. Table 10 and Figure 17 equally bear out that this proposed method is robust against most of the attacks. This scheme is least robust against non-uniform rotation and Median filtering attacks, as in these cases BER is around 6 to 8% and WDR is -15 to -19. Except from these, watermark can excellently persist against other attacks with 0% bit error rate as described here.

Table 10. Performance results of robustness

Sl. No	Attacks	BER (%)	NC	PCC	WDR	SM	NHD
1.	No attack	0	1	1	-∞	1	0
2.	180° Rotation	0	1	1	-∞	1	0
3.	90° Rotation	0	1	1	-∞	1	0
4.	45° Rotation	8.6	0.900	0.820	-15.14	0.999	0.086
5.	Negative	0	1	1	-∞	1	0
6.	Cropping	0	1	1	-∞	1	0
7.	Median Filtering	5.9	0.930	0.877	-18.97	0.998	0.058
8.	Salt & Pepper	0	1	1	-∞	1	0
9.	Erode	0	1	1	-∞	1	0
10.	Dilate	0	1	1	-∞	1	0

Hardware Implementation of a Visual Image Watermarking Scheme Using Qubit/Quantum Computation

A relative study between the proposed algorithm and some other existing methods is shown in table 11. It is obvious that the watermark and cover images, used in different proposals, are not identical in size or type. An average value through watermark to document scale is approximated.

Figure 17. Recovered watermark after several attacks: (a) No attack; (b) 180° Rotation (c) 90° Rotation (d) 45° Rotation (e) Negative (f) Cropping (g) Median Filtering (h) Salt & Pepper (i) Erode (j) Dilate

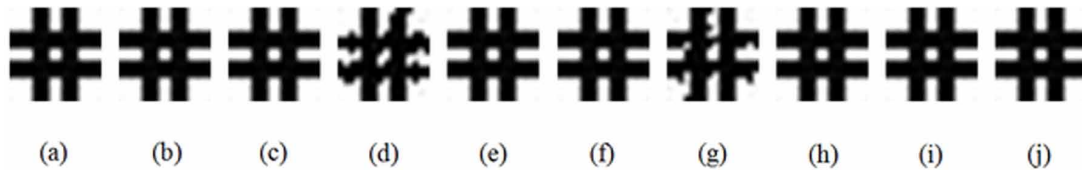


Table 11. Proficiency comparison results

Sl. No	Method	PSNR (dB)
1.	Proposed Method	56.50
2.	Salient Region Watermarking, Wong et al. (2013)	45.83
3.	IP LSB [Yang, 2008]	35.07
4.	Pair wise LSB matching, Xu et al. (2010)	35.05
5.	Optimal LSB pixel adjustment, Yang (2008)	34.84
6.	Matrix Encoding based Watermarking, Verma et al. (2013)	55.91
7.	LSB Replacement method, Goyal et al. (2014)	54.8
8.	DWT and SVD based Watermarking, Majumdar et al. (2011)	41.72
9.	Adaptive Pixel Pair Matching Scheme Hong, W. et al. (2012)	40.97
10.	Reversible Data Hiding Scheme, Gui et al. (2014)	34.26

Here it is observed that the projected watermarking scheme bids all other methods in terms of data transparency providing a high PSNR value. So, it can be concluded that this proposed watermarking algorithm is optimized in terms of both imperceptibility robustness.

Performance Analysis for Hardware Accomplishment

In this section the simulation and synthesis results are exemplified. The top level RTL schematics of the watermark insertion and extraction systems substantiate that the VHDL codes are executable. Xilinx ISE 13.2 is employed to synthesis the high level execution and the obtained schematics are shown in Figure 18. To optimize the behavioral simulation results of the system, a test cover image of size 4×4 and a binary watermark of size 2×2 have been chosen. The simulation consequences are exposed in Figure 19. With 100ns time period, 1750ns time is required to execute each of insertion and extraction process for images having the said sizes. As the code is running properly the reversible logic could be applied for each operational sub-blocks of the embedding and extracting blocks as well as the size of cover and watermark images can also be varied.

Hardware Implementation of a Visual Image Watermarking Scheme Using Qubit/Quantum Computation

Figure 18. RTL schematic diagram for (a) Watermark Insertion (b) Watermark Extraction

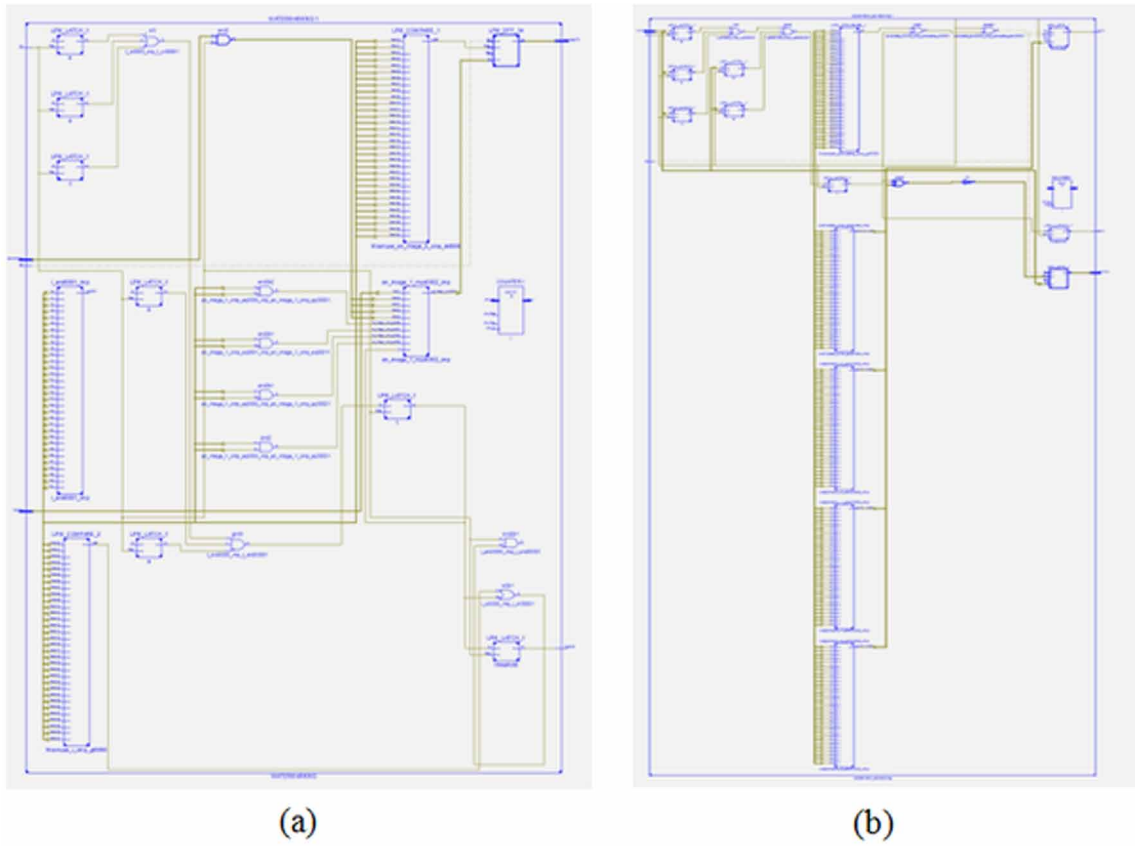
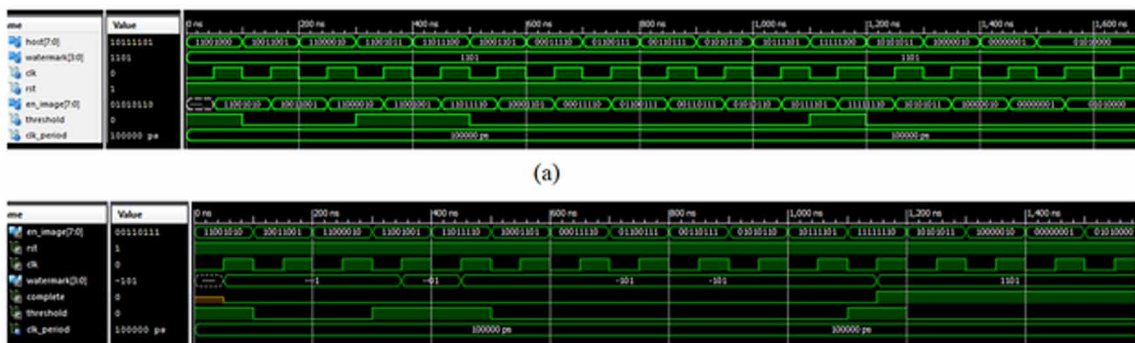


Figure 19. Behavioral simulation results for (a) Watermark Insertion (b) Watermark Extraction



CONCLUSION

The hardware implementation of an adaptive LSB replacement based digital image watermarking scheme is developed here. Preliminary discussions on digital watermarking convey the importance and utilizations of it in new age digital communication as well as the significance for using reversible logic. The authors initially developed the watermark embedding and extracting system in spatial domain. Here the watermark bits are adaptively embedded into the cover image pixels by satisfying a particular threshold. After the successful software execution of the system, its real time implementation is established through reversible logic. The circuit diagrams for individual sub-blocks involved in data embedding and extracting system to obtain the desired output. Accuracy of the FPGA implementation is reflected from the behavioral simulation results of the watermark insertion and extraction systems and thus it is obvious that both of the circuits can be executed through the proposed reversible logics. Thus the power dissipation can be reduced in a large scale providing a higher operating speed. The experimental results show that the technique offers excellent quality of imperceptibility by means of high PSNR value. Moreover the robustness, offered by this method, is also defensible. So, it can be concluded that the proposed framework successfully achieved the objective of developing a low power effective digital watermarking scheme.

REFERENCES

- Al-Nabhani, Jalab, Wahid, & Noor. (2015). Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network. *Journal of King Saud University – Computer and Information Sciences*, 27, 393-401.
- Al-Rabadi, A. N. (2004). New classes of Kronecker-based reversible decision trees and their group-theoretic representation. *Proceedings of the International Workshop on Spectral Methods and Multirate Signal Processing (SMMSP)*, 233–243.
- Alattar, A. M. (2003). Reversible Watermark Using Difference Expansion of Triplets. *Proc. of the International Conference on Image Processing, (ICIP 2003)*, 501-504. 10.1109/ICIP.2003.1247008
- Alattar, A. M. (2004). Reversible Watermark Using Difference Expansion of Quads. *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, 3, 377–380.
- Basu, A., Sinha Roy, S., & Chattopadhyay, A. (2016). Implementation of a Spatial Domain Salient Region Based Digital Image Watermarking Scheme. *Int. Conf. Research in Computational Intelligence and Communication Networks*, 269-272. 10.1109/ICRCICN.2016.7813669
- Basu, A., Sinha Roy, S., & Sarkar, S. (2015). FPGA Implementation of Saliency Based Watermarking Framework. *6th Int. Conf. on Computers and Devices for Communication*.
- Bennett, C. H. (1973). Logical reversibility of Computation. *IBM Journal of Research and Development*, 17(6), 525–532. doi:10.1147/rd.176.0525
- Celik, M. U., Sharma, G., Saber, E., & Tekalp, A. M. (2002). Hierarchical watermarking for secure image authentication with localization. *IEEE Transactions on Image Processing*, 11(6), 585–595. doi:10.1109/TIP.2002.1014990 PMID:18244657

Hardware Implementation of a Visual Image Watermarking Scheme Using Qubit/Quantum Computation

- Celik, M. U., Sharma, G., Tekalp, A. M., & Saber, E. (2005). Lossless generalized-LSB data embedding. *IEEE Transactions on Image Processing*, *14*(2), 253–266. doi:10.1109/TIP.2004.840686 PMID:15700530
- Chaumont, M., & Puech, W. (2009). A High Capacity Reversible Watermarking Scheme. *Visual Communications and Image Processing, Electronic Imaging*.
- Dasgupta, S., Papadimitriou, C. H., & Vazirani, U. V. (2006). *Algorithms*. McGraw-Hill Education.
- Dong, M. L., Dian, H. W., & Jie, L. (2012). A novel robust blind watermarking algorithm based on wavelet and Fractional Fourier Transform. *IEEE 14th International Conference on Communication Technology*.
- Dueck, G. W., & Maslov, D. (2003). Reversible function synthesis with minimum garbage outputs. *Proceedings of the 6th International Symposium on Representations and Methodology of Future Computing Technologies (RM 2003)*, 154–161.
- Emery, O. (1958). Des filigranes du papier. *Bulletin de l'Association technique de l'industrie papetiere*, *6*, 185–188.
- Fallahpur, M., & Sedaaghi, M. H. (2007). High capacity lossless data hiding based on histogram modification. *IEICE Electronics Express*, *4*(7), 205–210. doi:10.1587/elex.4.205
- Feynman, R. (1982). Simulating physics with computers. *International Journal of Theoretical Physics*, *21*(6/7), 467–488. doi:10.1007/BF02650179
- Feynman, R. (1986). Quantum mechanical computers. *Foundations of Physics*, *16*(6), 507–531. doi:10.1007/BF01886518
- Fridrich, J. J., Goljan, M., & Du, R. (2001). Detecting LSB steganography in color, and gray-scale images. *IEEE MultiMedia*, *8*(4), 22–28. doi:10.1109/93.959097
- Fridrich, J. J., Goljan, M., & Du, R. (2001a). Invertible authentication. *Security and Watermarking of Multimedia Contents III. Proceedings of the Society for Photo-Instrumentation Engineers*, (1): 197–208. doi:10.1117/12.435400
- Fridrich, J. J., Goljan, M., & Du, R. (2002). Lossless data embedding: New paradigm in digital watermarking. *EURASIP Journal on Applied Signal Processing*, *2002*(2), 185–196. doi:10.1155/S1110865702000537
- Gao, T., & Gu, Q. (2007). Reversible Image Authentication Based on Combination of Reversible and LSB Algorithm. *Proc. IEEE, Computational Intelligence and Security Workshops (CISW 07)*, 636–639. 10.1109/CISW.2007.4425576
- Goljan, M., Fridrich, J. J., & Du, R. (2001). Distortion-free data embedding for images. LNCS, 2137, 27–41.
- Goyal, R., & Kumar, N. (2014). LSB Based Digital Watermarking Technique. *International Journal of Application or Innovation in Engineering & Management*, *3*(9), 15–18.
- Gui, X., Li, X., & Yang, B. (2014, May). A high capacity reversible data hiding scheme based on generalized prediction-error expansion and adaptive embedding. *Signal Processing*, *98*, 370–380. doi:10.1016/j.sigpro.2013.12.005

Hamidreza, Omair, & Swamy. (2016). Multiplicative Watermark Decoder in Contourlet Domain Using the Normal Inverse Gaussian Distribution. *IEEE Transactions on Multimedia*, 18(2), 19 -207.

Han, K. H., & Kim, J. H. (2000). Genetic quantum algorithm and its application to combinatorial optimization problem. *Proc. of the 2000 Congress on evolutionary computation*, 2, 1354–1360. 10.1109/CEC.2000.870809

Hao-Tang, C., Wen-Jyi, H., & Chau-Jern, C. (2015). Digital Hologram Authentication Using a Hadamard-Based Reversible Fragile Watermarking Algorithm. *Journal of Display Technology*, 11(2), 193–203. doi:10.1109/JDT.2014.2367528

Hirohisa, H. (2002). A data embedding method using BPCS principle with new complexity measures. *Proc. of Pacific Rim Workshop on Digital Steganography*, 30-47.

Hong, L., Di, X., Rui, Z., Yushu, Z., & Sen, B. (2016). Robust and hierarchical watermarking of encrypted images based on Compressive Sensing. *Journal of Signal Processing: Image Communication*, 45, 41–51.

Hong, W., & Chen, T. S. (2012). A Novel Data Embedding Method Using Adaptive Pixel Pair Matching. *IEEE Transactions on Information Forensics and Security*, 7(1), 176–184. doi:10.1109/TIFS.2011.2155062

Honsinger, C. W., Jones, P., Rabbani, M., & Stoffel, J. C. (2001). *Lossless recovery of an original image containing embedded data*. US Patent Application, 6 278 791.

Hwai-Tsu, H., & Ling-Yuan, H. (2016). A mixed modulation scheme for blind image watermarking. *International Journal of Electronics and Communications*, 70(2), 172–178. doi:10.1016/j.aeue.2015.11.003

Jaseena & John. (2011). Text Watermarking using Combined Image and Text for Authentication and Protection. *International Journal of Computer Applications*, 20(4).

Juergen, S. (2005). *Digital Watermarking for Digital Media*. IGI.

Kallel, M., Lapayre, J. C., & Bouhlel, M. S. (2007). A multiple watermarking scheme for medical image in the spatial domain. *Graphics. Vision and Image Processing Journal*, 7(1), 37–42.

Kamstra, L., & Heijmans, H. J. (2005). Reversible data embedding into images using wavelet techniques and sorting. *IEEE Transactions on Image Processing*, 14(12), 2082–2090. doi:10.1109/TIP.2005.859373 PMID:16370461

Kawaguchi, E., & Eason, R. O. (1998). Principle and Applications of BPCS Steganography. *Proc. of SPIE, Multimedia Systems and Applications*, 3528, 464–473.

Khandare, S., & Shrawankar, U. (2015). Image bit depth plane digital watermarking for secured classified image data transmission. *Procedia Computer Science*, 78, 698–705. doi:10.1016/j.procs.2016.02.119

Khariththa, T., Pipat, S., & Thumrongrat, A. (2015). Digital Image Watermarking based on Regularized Filter. *14th IAPR International Conference on Machine Vision Applications*.

Kim, H. J., Sachnev, V., Shi, Y. Q., Nam, J., & Choo, H. G. (2008). A Novel Difference Expansion Transform for Reversible Data Embedding. *IEEE Transactions on Information Forensics and Security*, 3(3), 456–465. doi:10.1109/TIFS.2008.924600

- Kim, K. S., Lee, M. J., Lee, H. Y., & Lee, H. K. (2009). Reversible data hiding exploiting spatial correlation between sub-sampled images. *Pattern Recognition*, 42(11), 3083–3096. doi:10.1016/j.patcog.2009.04.004
- Kutter, M. (1999). *Digital Watermarking: Hiding Information in Images* (PhD thesis). Swiss Federal Institute of Technology, Lausanne, Switzerland.
- Kutter, M., & Petitcolas, F. A. P. (2000). A fair benchmark for image watermarking systems. *Journal of Electronic Imaging*, 9(4), 445–455. doi:10.1117/1.1287594
- Lalitha, N. V., & Rao, S. (2013). DWT - Arnold Transform based audio watermarking. *IEEE Asia Pacific Conference on Postgraduate Research in Microelectronics and Electronics*. doi:.2013.673120410.1109/PrimeAsia
- Landauer, R. (1961). Irreversibility and heat generation in the computing process. *IBM Journal of Research and Development*, 5(3), 183–191. doi:10.1147/rd.53.0183
- Lee, S., Yoo, C. D., & Kalker, T. (2007). Reversible Image Watermarking Based on Integer-to-Integer Wavelet Transform. *IEEE Transactions on Information Forensics and Security*, 2(3), 321–330. doi:10.1109/TIFS.2007.905146
- Lin, P.-L. (2001). Oblivious Digital Watermarking Scheme with Blob-Oriented and Modular-Arithmetic-Based Spatial-Domain Mechanism. *Journal of Visual Communication and Image Representation*, 12(2), 136–151. doi:10.1006/jvci.2000.0454
- Liu, N., Amin, P., Ambalavanan, A., & Subbalakshmi, K. P. (2006). An Overview of Digital Watermarking. In *Multimedia Security Technologies for Digital Rights Management*. Academic Press. doi:10.1016/B978-012369476-8/50009-9
- Lukac, M., Perkowski, M., Goi, H., Pivtoraiko, M., Yu, C. H., Chung, K., ... Kim, Y.-D. (2003). Evolutionary approach to quantum and reversible circuits synthesis. *Artificial Intelligence Review*, 20(3–4), 361–417. doi:10.1023/B:AIRE.0000006605.86111.79
- Lukac, M., Pivtoraiko, M., Mishchenko, A., & Perkowski, M. (2002). Automated synthesis of generalized reversible cascades using genetic algorithms. *5th International Workshop on Boolean Problems*, 33–45.
- Maity, S. P., Kundu, M. K., & Seba, M. (2009). Dual Purpose FWT Domain Spread Spectrum Image Watermarking in Real-Time. *Computers & Electrical Engineering*, 35(2), 415–433. doi:.compel-eceng.2008.06.003 doi:10.1016/j
- Majumdar, S., Das, T. S., & Sarkar, S. K. (2011). DWT and SVD based Image Watermarking Scheme using Noise Visibility and Contrast Sensitivity. *Int. Conf. on Recent Trends in Information Technology*, 938–942. 10.1109/ICRTIT.2011.5972409
- Maslov, D., & Dueck, G. W. (2003). Garbage in reversible designs of multiple output functions. *Proceedings of the 6th International Symposium on Representations and Methodology of Future Computing Technologies (RM 2003)*, 162–170.
- Maslov, D., Dueck, G. W., & Miller, D. M. (2005). Synthesis of Fredkin-Toffoli reversible networks. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 13(6), 765–769. doi:10.1109/TVLSI.2005.844284

- Mayers, D. (1998). *Unconditional Security in Quantum Cryptography*. quant-ph/9802025
- Megalingam, R. K., Nair, M. M., Srikumar, R., Balasubramanian, V. K., & Sarma, V. S. V. (2010). Performance Comparison of Novel, Robust Spatial Domain Digital Image Watermarking with the Conventional Frequency Domain Watermarking Techniques. *International Conference on Signal Acquisition and Processing*. 10.1109/ICSAP.2010.79
- Meng, Q., & Gong, C. (2010). Web information classifying and navigation based on neural network. *2nd Int. Conf. on signal processing systems*, 2, V2-431-V2-433.
- Miller, D. M. (2002). Spectral and two-place decomposition techniques in reversible logic. *Proceedings of the IEEE Midwest Symposium on Circuits and Systems (MWSCAS 02)*, II 493–II 496. 10.1109/MWSCAS.2002.1186906
- Miller, D. M., Maslov, D., & Dueck, G. W. (2003). A transformation based algorithm for reversible logic synthesis. *Proceedings of the Design Automation Conference*, 318–323. 10.1145/775832.775915
- Mintzer, F., Braudaway, G. W., & Yeung, M. M. (1997). Effective and ineffective digital watermarks. *Proceedings - International Conference on Image Processing*, 3, 9–12.
- Mislav, G., Kresimir, D., & Mohammed, G. (2009). *Recent Advances in Multimedia Signal Processing and Communications*. Springer Science & Business Media.
- Mohanty, S. P. (1999). *Digital Watermarking: A Tutorial Review*. Retrieved from <http://www.csee.usf.edu> accessed
- Mohanty, S. P., Parthasarathy, G., Elias, K., & Nishikanta, P. (2006). A Novel Invisible Color Image Watermarking Scheme using Image Adaptive Watermark Creation and Robust Insertion-Extraction. *Proceeding of the 8th IEEE International Symposium on Multimedia (ISM '06)*. 10.1109/ISM.2006.7
- Mukherjee, D. P., Maitra, S., & Acton, S. T. (2004). Spatial domain digital watermarking of multimedia objects for buyer authentication. *IEEE Transactions on Multimedia*, 6(1), 1–15. doi:10.1109/TMM.2003.819759
- Ni, Z., Shi, W. Q., Ansari, N., Su, W., Sun, Q., & Lin, X. (2008). Robust Lossless Image Data Hiding Designed for Semi-Fragile Image Authentication. *IEEE Transactions on Circuits and Systems for Video Technology*, 18(4), 497–509. doi:10.1109/TCSVT.2008.918761
- Ni, Z., Shi, Y. Q., Ansari, N., & Su, W. (2003). Reversible data hiding. *Proc. of the 2003 Int. Symposium on Circuits and Systems (ISCAS 2003)*, 2, 912-915.
- Ni, Z., Shi, Y. Q., Ansari, N., & Su, W. (2006). Reversible data hiding. *IEEE Transactions on Circuits and Systems for Video Technology*, 16(3), 354–362. doi:10.1109/TCSVT.2006.869964
- Ono, M., Han, S., Fujiyoshi, M., & Kiya, H. (2009). A location map-free reversible data hiding method for specific area embedding. *IEICE Electronics Express*, 6(8), 483–489. doi:10.1587/elex.6.483
- Pappas, T. E. (1992). An adaptive clustering algorithm for image segmentation. *INEE Trans. on Signal Processing*, 40(4), 901–914. doi:10.1109/78.127962

Hardware Implementation of a Visual Image Watermarking Scheme Using Qubit/Quantum Computation

Patra, J. C., Phua, J. E., & Rajan, D. (2010). DCT domain watermarking scheme using Chinese Remainder Theorem for image authentication. *IEEE International Conference on Multimedia and Expo*. 10.1109/ICME.2010.5583326

Perkowski, M., Jozwiak, L., & Kerntopf, P. (2001). A general decomposition for reversible logic. *Proceedings of the 5th International Workshop on Applications of Reed-Muller Expansion in Circuit Design (Reed-Muller'01)*, 119–138.

Ramani, K., Prasad, E. V., & Varadarajan, S. (2007). Steganography using BPCS to the Integer Wavelet Transformed image. *International Journal of Computer Science and Network Security*, 7(7), 293–302.

Rigatos, G. G., & Rzafestas, S. G. (2006). Quantum learning for neural associative memories. *Fuzzy Sets and Systems*, 157(13), 1797–1813. doi:10.1016/j.fss.2006.02.012

Sayood, K. (2006). Introduction to data compression. *Morgan Kaufmann Series in Multimedia Information and Systems*, Elsevier, 3E, 183–217.

Shah, P. (2015). A DWT-SVD Based Digital Watermarking Technique for Copyright Protection. *International Conference on Electrical, Electronics, Signals, Communication and Optimization*. 10.1109/EESCO.2015.7253806

Shende, V. V., Prasad, A. K., Markov, I. L., & Hayes, J. P. (2002). Reversible logic circuit synthesis. *Proceedings of the International Conference on Computer Aided Design*, 125–132.

Sinha Roy, S., Saha, S., & Basu, A. (2015). Generic Testing Architecture for Digital Watermarking. *Proc. FRCCD-2015*, 50-58.

Song, W., Hou, J., & Li, Z. (2008). SVD and pseudorandom circular chain based watermarking for image authentication. *Journal of Beijing Jiaotong University*, 32(2), 71–75.

Stach, J., & Alattar, A. M. (2004). A High Capacity Invertible Data Hiding Algorithm using a Generalized Reversible Integer Transform. *IS&T/SPIE's 16th International Symposium on Electronic Imaging*, 5306, 386-396.

Sur, A., Sagar, S. S., Pal, R., Mitra, P., & Mukhopadhyay, J. (2009). A New Image Watermarking Scheme using Saliency Based Visual Attention Model. *Proceedings of IEEE Annual India Conference*. 10.1109/INDCON.2009.5409402

Tanaka, K., Nakamura, Y., & Matsui, K. (1990). Embedding secret information into a dithered multilevel image. *Proc. IEEE Military Communications Conference*. 10.1109/MILCOM.1990.117416

The USC-SIPI Image Database. (n.d.). Retrieved from <http://sipi.usc.edu/database/database.php?volume=misc>

Thodi, D. M., & Rodriguez, J. J. (2004). Reversible watermarking by prediction-error expansion. *Proceedings - IEEE Southwest Symposium on Image Analysis and Interpretation*, 6, 21–25.

Thodi, D. M., & Rodriguez, J. J. (2007). Expansion Embedding Techniques for Reversible Watermarking. *IEEE Transactions on Image Processing*, 16(3), 721–730. doi:10.1109/TIP.2006.891046 PMID:17357732

- Tian, J. (2002). Reversible watermarking by difference expansion. *Proc. of Workshop on Multimedia and Security: Authentication, Secrecy, and Steganalysis*, 19-22.
- Tirkel, A. Z., Rankin, G. A., Van Schyndel, R. M., Ho, W. J., Mee, N. R. A., & Osborne, C. F. (1993). *Electronic Water Mark. Digital Image Computing: Techniques and Applications 1993*. Macquarie University.
- Tsai, C., Chiang, H., Fan, K., & Chung, C. (2005, November). Reversible data hiding and lossless reconstruction of binary images using pair-wise logical computation mechanism. *Pattern Recognition*, 38(11), 1993–2006. doi:10.1016/j.patcog.2005.03.001
- Verma, M., & Yadav, P. (2013). Capacity and Security analysis of watermark image truly imperceptible. *Int. Journal of Advanced Research in Computer and Communication Engineering*, 2(7), 2913–2917.
- Vlachopiantts, G., & Lee, K. Y. (2008). Quantum-inspired evolutionary algorithm for real and reactive power systems. *IEEE Transactions on Power Systems*, 23(4), 1627-1636.
- Vleeschouwer, C. D., Delaigle, J. F., & Macq, B. (2003). Circular interpretation of bijective transformations in lossless watermarking for media asset management. *IEEE Transactions on Multimedia*, 5(1), 97–105. doi:10.1109/TMM.2003.809729
- Weiner, J., & Mirkes, K. (1972). *Watermarking*. Appleton, WI: The Institute of Paper Chemistry.
- Wille, R., Le, H. M., Dueck, G. W., & Grobe, D. (2008). Quantified synthesis of reversible logic. *Design, Automation and Test in Europe (DATE 08)*, 1015–1020.
- Wioletta, W., & Ogiela, M. R. (2016). Digital images authentication scheme based on bimodal biometric watermarking in an independent domain. *Journal of Visual Communication and Image Representation*, 38, 1–10. doi:10.1016/j.jvcir.2016.02.006
- Wong, M. L. D., Lau, S. I. J., Chong, N. S., & Sim, K. Y. (2013). A Salient Region Watermarking Scheme for Digital Mammogram Authentication. *International Journal of Innovation, Management and Technology*, 4(2), 228–232.
- Wujie, Z., Lu, Y., Zhongpeng, W., Mingwei, W., Ting, L., & Lihui, S. (2016). Binocular visual characteristicsbased fragile watermarking schemefor tamper detection in stereoscopic images. *International Journal of Electronics and Communications*, 70(1), 77–84. doi:10.1016/j.aee.2015.10.006
- Xiang-yang, W., Yu-nan, L., Shuo, L., Hong-ying, Y., Pan-pan, N., & Yan, Z. (2015). A new robust digital watermarking using local polar harmonic transform. *Journal of Computers and Electrical Engineering*, 46, 403–418. doi:10.1016/j.compeleceng.2015.04.001
- Xu, H., Wang, J., & Kim, H. J. (2010). Near-Optimal Solution to Pair Wise LSB Matching Via an Immune Programming Strategy. *Information Sciences*, 180(8), 1201–1217. doi:10.1016/j.ins.2009.12.027
- Xuan, G., Shi, Y. Q., Ni, Z. C., Chen, J., Yang, C., Zhen, Y., & Zheng, J. (2004). High capacity lossless data hiding based on integer wavelet transform. *Proceedings of IEEE 2004 International Symposium on Circuits and Systems*, 2, 29-32.

Hardware Implementation of a Visual Image Watermarking Scheme Using Qubit/Quantum Computation

Xuan, G., Shi, Y. Q., Yang, C., Zheng, Y., Zou, D., & Chai, P. (2005). Lossless data hiding using integer wavelet transform and threshold embedding technique. *IEEE Int. Conf. on Multimedia and Expo (ICME05)*. 10.1109/ICME.2005.1521722

Xuan, G., Yao, Q., Yang, C., Gao, J., Chai, P., Shi, Y. Q., & Ni, Z. (2006). Lossless Data Hiding Using Histogram Shifting Method Based on Integer Wavelets. *5th Int. Workshop on Digital Watermarking (IWDW 2006)*, LNCS 4283, p. 323-332. 10.1007/11922841_26

Xuan, G., Zhu, J., Chen, J., Shi, Y. Q., Ni, Z., & Su, W. (2002). Distortionless Data Hiding Based on Integer Wavelet Transform. *Electronics Letters*, 38(Dec), 1646–1648. doi:10.1049/el:20021131

Yang, C. H. (2008). Inverted pattern approach to improve image quality of information hiding by LSB substitution. *Pattern Recognition*, 41(8), 2674–2683. doi:10.1016/j.patcog.2008.01.019

Yang, Y., Sun, X., Yang, H., Li, C., & Xiao, R. (2009). A Contrast-Sensitive Reversible Visible Image Watermarking Technique. *IEEE Transactions on Circuits and Systems for Video Technology*, 19(5), 656–667. doi:10.1109/TCSVT.2009.2017401

Yaqub, M. K., & Jaber, A. (2006). Reversible watermarking using modified difference expansion. *Int. Journal of Computing and Information Sciences*, 4(3), 134–142.

Zhang, G. (2011). Quantum-inspired evolutionary algorithms: A survey and empirical study. *Journal of Heuristics*, 17(3), 303–351. doi:10.1007/10732-010-9136-0

This research was previously published in Quantum-Inspired Intelligent Systems for Multimedia Data Analysis; pages 95-140, copyright year 2018 by Engineering Science Reference (an imprint of IGI Global).

Chapter 7

True Color Image Segmentation Using Quantum-Induced Modified-Genetic-Algorithm- Based FCM Algorithm

Sunanda Das

University Institute of Technology, India

Sourav De

Cooch Behar Government Engineering College, India

Siddhartha Bhattacharyya

 <https://orcid.org/0000-0003-0360-7919>

RCC Institute of Information Technology, India

ABSTRACT

In this chapter, a quantum-induced modified-genetic-algorithm-based FCM clustering approach is proposed for true color image segmentation. This approach brings down the early convergence problem of FCM to local minima point, increases efficacy of conventional genetic algorithm, and decreases the computational cost and execution time. Effectiveness of genetic algorithm is tumid by modifying some features in population initialization and crossover section. To speed up the execution time as well as make it cost effective and also to get more optimized class levels some quantum computing phenomena like qubit, superposition, entanglement, quantum rotation gate are induced to modified genetic algorithm. Class levels which are yield now fed to FCM as initial input class levels; thus, the ultimate segmented results are formed. Efficiency of proposed method are compared with classical modified-genetic-algorithm-based FCM and conventional FCM based on some standard statistical measures.

DOI: 10.4018/978-1-7998-8593-1.ch007

INTRODUCTION

True color image segmentation always be a highly research oriented field as it is treated in the fields of vision, medical image processing, biometric measurements etc for the purpose of detection, face recognition, tracking of an object. Image segmentation is the process to partition an image into some non disjoint regions by groupifying the pixels having same characteristics such as intensity, homogeneity, texture etc. A true color image contains much more information than a gray scale image as a color image convey much more features than gray scale image. The underlying data of a true color image deal with the information in primary color components viz Red(R), Green(G) and Blue(B) and also their admixtures. So a proper segmentation algorithm always be needed for more perfect and accurate result, otherwise it may be happened that after segmentation a new color component may be generated which does not belong to the original true color image.

Different classical and soft computing based techniques are used for segmentation purpose. Classical techniques are categorized into three categories: feature space based segmentation, image domain based segmentation and graph based segmentation. Thresholding, region growing and merging, edge detection, clustering are popularly used some classical segmentation techniques. On the other hand, soft computing techniques have been manifested for the solution of control problems. Fuzzy Logic, artificial neural network, genetic algorithm are three components of soft computing techniques. Fuzzy logic mainly deals with the problem of imprecision and uncertainty, artificial neural network used for learning and adaptation and GA is opted for optimization problem. By using classical segmentation techniques, uncertainties may be arrived as segmentation results if incomplete, imprecise and/or ambiguous information used as input data, overlapping boundaries between classes are present and extracting features and relations among them are indefinite. Soft computing techniques deal with these kinds of problems and produce more convenient result.

Fuzzy C-Means (FCM) [Bezdek, 1981] clustering, a soft clustering technique, is widely used for image segmentation. It follows the rule of fuzzy set theory [Zadeh, 1965]. Though it is more efficient than many other clustering techniques but it also has some deficiencies like it may be stuck into local minima point unless to reach global maxima point; second at the very first time cluster centres are initialized by the programmer; and third it is only applied to hyper spherical structured clusters. Incorporating different evolutionary algorithms like GA [Goldberg, 1989], PSU [Mekhmoukh, 2015] into FCM above stated problems can be solved. Evolutionary algorithms produce global optimal solutions which will be gone to FCM as input data. Though this kind of hybrid algorithm produces optimal solutions but they take high computational time.

High computational time indicates usage of large amount of electronic circuits. From Moore's law, it is known that electronic circuits loss their efficiency and computing ability in day to day fashion. So after some more years later it may be happened that to compute the same algorithm much more circuits will be needed which will be become obviously cost effective. To decrease the computational cost as well as computational time and also to get more accurate and competent results, quantum computing [Mcmohan, 2008] concept is evolved and induced to classical methods. It sustains some properties of quantum mechanics like qubit, superposition, entanglement, orthogonality, quantum rotational gate etc.

In this chapter a Quantum induced Modified Genetic Algorithm (QIMfGA) based FCM algorithm is proposed for true color image segmentation. Here a modified genetic algorithm is applied to FCM to overcome the problem of stucking to local minima. Modified Genetic Algorithm (MfGA) [Das, 2016] indicates some modifications done in population initialization and crossover part of GA, which enhance

efficacy of traditional GA. The above stated quantum properties are now incorporated to modified GA as a result computational time is decreased and the output class levels generated by quantum induced modified GA are more optimal than conventional version. The resultant class levels are now employed to FCM as initial input class levels which yield more accurate and competent segmented result. This QIMfGA based FCM algorithm is applied on two true color test images Lena and Peppers and all the results are compared with both classical MfGA based FCM and conventional FCM methods using three evaluation metrics ρ [De, 2012], F' [Borosotti, 1998] and Q [Borosotti, 1998]. The comparison leads to the conclusion that our proposed method efficiently segment true color images than both classical MfGA based FCM and conventional FCM methods.

This chapter is formed in the following manner. A literature review is given here where different eminent works are presented. After that a brief description of FCM, Genetic algorithm and quantum computing concept are stated. Then it proceeds to proposed methodology, comparison based experimental results and lastly to the conclusion.

LITERATURE REVIEW

Segmentation is an important image processing technique which helps to analyze an image automatically. Different classical and non classical segmentation approaches are proposed to segment true color images in [Gonzales, 2002]. Bhattacharyaa [Bhattacharyaa, 2011] presented a survey paper where different segmentation techniques are discussed for color images. Thresholding is one of the most popular image segmentation techniques, used by many researchers. A multilevel thresholding approach has been applied to a color image to extract the information of the main object from its background and others object [Kulkarni, 2012]. A modified watershed algorithm has been conducted to true color images [Rahman, Islam, 2013]. In this article, to overcome the problem of over segmentation, an adaptive masking and thresholding approach are applied to each plane of color images, before merging them to final one. A multilevel thresholding method combined with data fusion technique applied to color images for segmentation purpose which increased information quality and produced more reliable segmented output [Harrabi and Braiek, 2012]. A morphological gradient based active contour model is used for color image segmentation [Anh, 2011]. Here, the proposed model extract the edge map direct from color images without losing the color characteristics and this provides good region and edge information as an active contour without re-initialization. Tan and Isa [Tan, 2011] proposed a histogram thresholding based FCM algorithm where thresholding methods used to determine the class levels for color images and those are employed to FCM. Mao et al. [Mao, 2009] used region growing and ant colony algorithms to segment color image. In this article, based on the similar intensity value, edge information and spatial information, seeds are first automatically selected. Then applying ant colony technique, the regions are merged maintaining the homogeneity property. In article [Verma, 2011], a single seeded region growing technique is adopted for true color image segmentation. To decrease the computational cost and execution time, a new region growing formula is formulated and Otsu's thresholding method is used here as the stopping criteria. A meta-heuristics algorithm is introduced for color image segmentation in [Preetha, 2014]. Segmentation has done based on seed region growing. Primarily the seeds are chosen by Cuckoo search method. Tao *et al.* [Tao, 2007] proposed a method where mean shift segmentation and normalized cut are used in a combined manner. Mean shift algorithm is applied to color image to store the discontinuity characteristics and after that n-cut algorithm are applied to those region to get

global optimized clusters. An automatic color image segmentation using adaptive grow cut algorithm is proposed by Basavaprasad *et al.* [Basavaprasad, 2015]. Chen and Ludwig [Chen, 2017] proposed a Fuzzy C- regression model for color image segmentation. It considered spatial information and applied to the hyperplaned cluster. Chaabane *et al.* [Chaabane, 2015] used a feature based modified FCM clustering technique to segment color images. In first stage, statistical features and fuzzy clustering technique are integrated to obtain the segmented image; after that these segmented results are merged over different channel based on some combination rule. Dong *et al.* [Dong, 2005] evolved a segmentation technique where both supervised and unsupervised techniques are used. SOM and simulated annealing are used to achieve color reduction and color clustering respectively for segmentation. After that supervised learning is applied to get the ultimate segmented result. In another article [Arumugadevi, 2016] features of color images are employed to FCM to get the class levels which are fed to the feed forward network to get segmented results. The parallel optimized multilevel sigmoidal (ParaOptiMUSIG) activation function in connection with the multilevel self-organizing neural network (MLSONN) is introduced for the true color image segmentation [De, 2010, 2012]. In this method, the genetic algorithm is applied to generate the ParaOptiMUSIG activation function. This algorithm is also applied for multi objective function without confining within the single objective function. De *et al.* [De, 2013] proposed NSGA II based ParaOptiMUSIG activation function incorporating the multi-criterion to segment the color images. GA in combination with the weighted undirected graph is employed to segment the color images [Amelio, 2013]. Krishna *et al.* [Krishna, 2015] proposed a new approach for color image segmentation where texture and color features are applied to Sequential Minimal Optimization-Support Vector Machine (SMO-SVM). A soft rough FCM is used here to train the SMO-SVM classifier for segmentation purpose. A new approach is introduced where modified GA and FCM are combined to get more optimal solution [Das, 2016]. Class levels generated by Modified GA are employed to FCM to overcome the convergence problem of FCM. Modifying the population initialization part and crossover section of GA with the use of a new weighted mean and new crossover probability formula, more optimal results are found.

Though the hybrid systems give more reliable results but computational cost and execution time are also extended. To overcome this problem quantum characteristics are incorporated to different conventional or classical methods in different research articles. To solve TSP problem in minimum computational time quantum computing concept is merged with GA [Talbi, 2004]. Here a lookup table is maintained for rotational angel. A quantum based PSO algorithm is used for color image segmentation [Nebti, 2013]. A multiobjective quantum inspired evolutionary algorithm [Li, 2014] is applied to SAR images to get more optimal segmented results in less time. A quantum inspired tabu search algorithm is applied to color image for multilevel thresholding in [Dey, 2014]. Dey *et al.* [Dey, 2013] incorporate quantum computing phenomena to particle swarm algorithm and differential evolutionary algorithm. These quantum versions are used for multilevel thresholding of color images.

FUZZY C-MEANS CLUSTERING

To make clustering concept more convenient, Fuzzy C-Means clustering (FCM) technique was introduced by Dunn [Dunn, 1973] in 1973 and improved by Bezdek [Bezdek, 1981] in 1981. It is actually a classification based unsupervised clustering algorithm works on the principle of fuzzy set theory [Zadeh, 1965]. The main aim of this algorithm is to minimize the objective function with respect to the cluster centre $Centre_i$ and the membership function U . The membership matrix U denotes the belongingness

of each data point in each cluster as here one data point resides more than one cluster. The data points, belong to the same cluster, have higher membership value with respect to that cluster and others have lower membership value. Clusters are formed based on the Euclidean distance between each data point and cluster centre. By iteratively updating its cluster centre and membership function this algorithm reaches to its goal. Suppose $X=\{x_1, x_2, x_3, \dots, x_N\}$ is a set of N number of unlabeled data patterns having f number of features which are allowed to partition in C number of clusters. Now this can be done by updating membership function U_i and cluster centre $Centre_i$ using the following formula:

$$U_{ik} = \frac{1}{\frac{\|x_k - Centre_i\|^{\frac{2}{m-1}}}{\sum_{j=1}^j \|x_k - Centre_j\|^{\frac{2}{m-1}}}}, 1 \leq k \leq N, 1 \leq i \leq C \quad (1)$$

where U_{ik} denotes the degree of membership of x_k in i^{th} cluster and m represents the degree of fuzziness which is greater than 1.

The cluster centroids are calculated by the following formula:

$$Centre_i = \frac{\sum_{k=1}^N (U_{ik})^m x_k}{\sum_{k=1}^N (U_{ik})^m}, 1 \leq i \leq C \quad (2)$$

GENETIC ALGORITHM

Genetic Algorithm, a heuristics search method, provides global optimal solution in large, complex and multimodal problem space. This method forged the idea of natural evolution procedure. In GA a fixed population size is maintained throughout the method. This method starts by random generation of individuals which are called chromosomes. Quality of each individual is manipulated using fitness value. Using three genetically inspired operation selection, crossover and mutation, better solutions are produced.

A chromosome is made of a set of genes which are noting but the values of cluster centroids and a set of chromosomes are created a population pool. Each chromosome actually represents solution of the problem space, having some properties. These solutions are altered and mutated using the crossover and mutation probability to produce the global optimized solution. Crossover is occurred between two or more selected candidate solutions. This selection can be done using different selection procedures like Roulette wheel selection, Rank selection, Tournament selection, Boltzman selection etc. There are also different types of crossover techniques e.g. single point crossover, two point crossover, uniform crossover. Next to the crossover operation, mutation is applied to child solution to make it more fitted.

True Color Image Segmentation Using Quantum-Induced Modified-Genetic-Algorithm

Figure 1. Graphical representation of Gene, Chromosome and Population

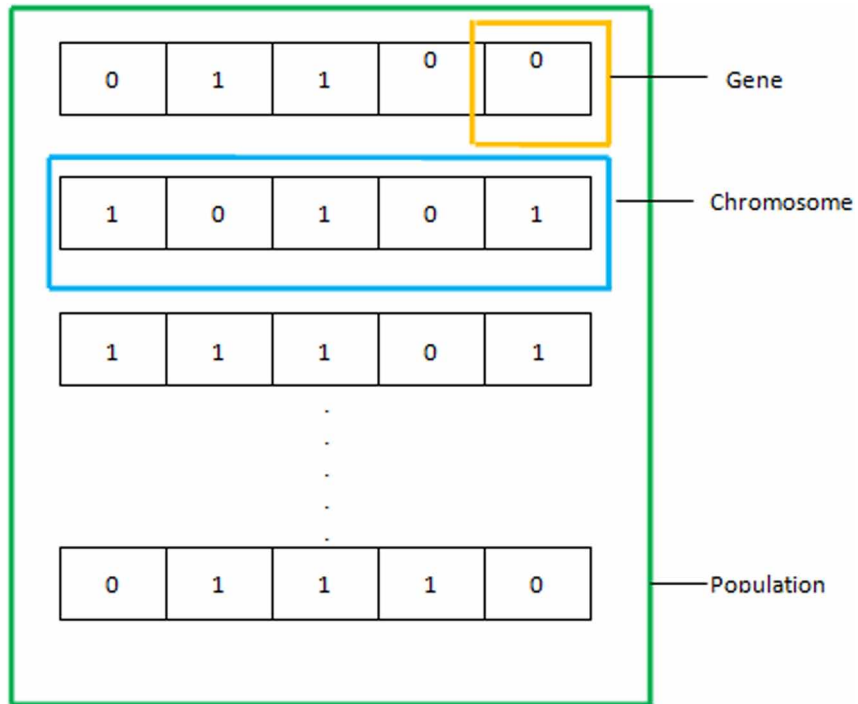


Figure 2. Single Point Crossover

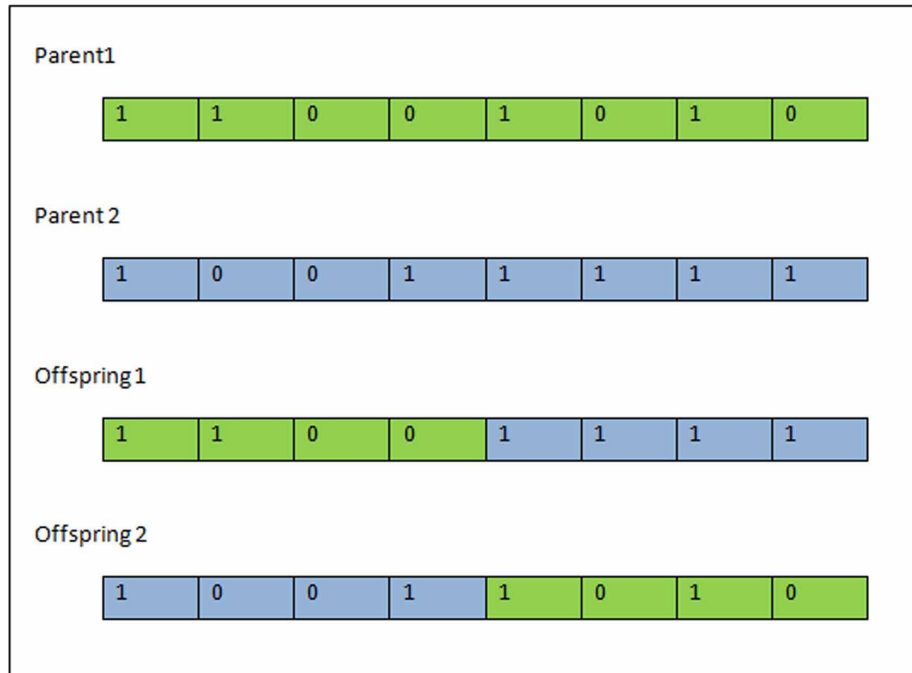


Figure 3. Two Point Crossover

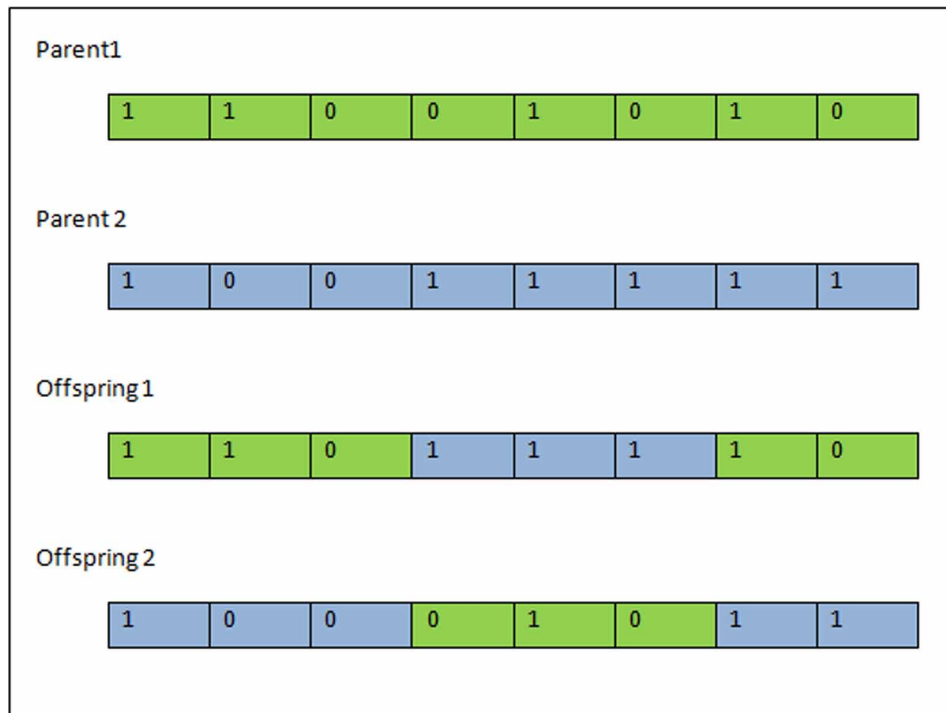


Figure 4. Multi Point Crossover

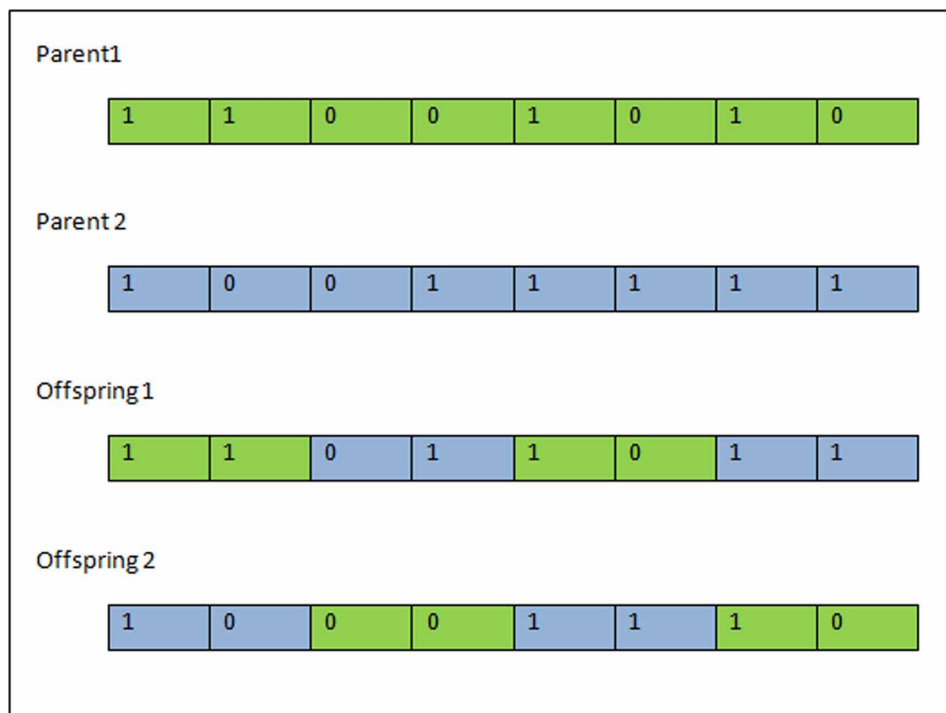


Figure 5. Mutation

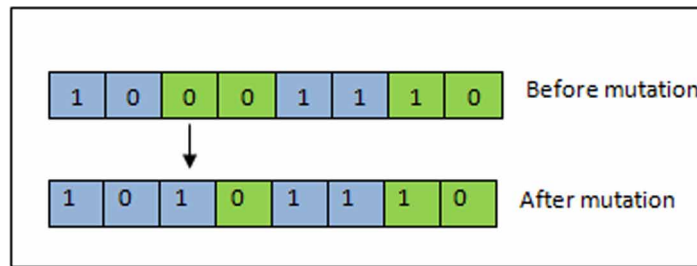
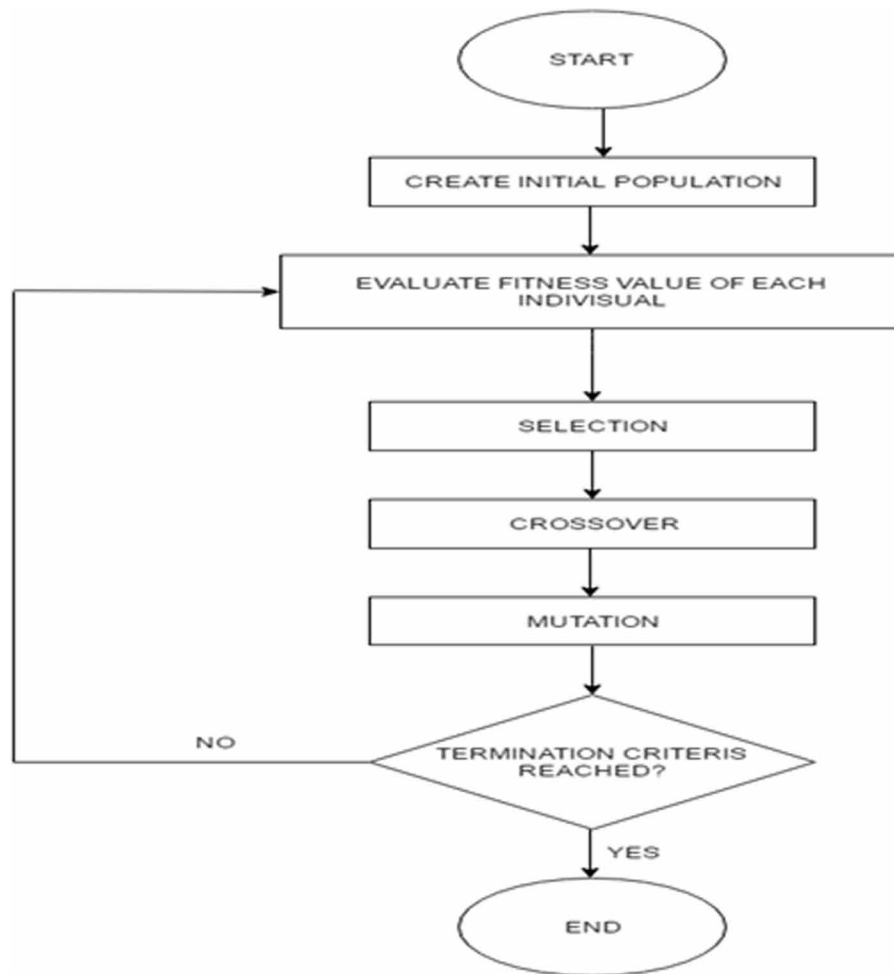


Figure 6. Flow Diagram of Genetic Algorithm



QUANTUM COMPUTING CONCEPT

Now-a-days, quantum computing plays a vital role in different research area. Different conventional methods accomplished their jobs in efficient manner; hybrid systems enhance efficiencies of those

conventional methods. But, though the hybrid system provides more accurate and effective results than conventional methods, it takes huge computational time. High computation indicates usage of more computational circuits. Again from Moore's law it can be said that the number of transistors per square inch on integrated circuits would double in every 18 months. So whatever amount of electronic circuits are used today for one program, in future the same program will need more electronic circuits, which leads to the problem of high computational cost. From this point of view Quantum Computing has been evolved by American computer engineer Howard Aiken in 1947. It works on the principle of quantum mechanics and follows some properties like qubit, orthogonality, entanglement, rotational gate etc. When these properties are embedded into the classical methods, within the minimum time period a high quality of output is generated.

In quantum computing the smallest information bit is known as *qubit*. Where classical computers deal with bit, represents by 0 or 1, in quantum computing a single qubit can be represented by 0 or 1 or any linear superposition of both states. If a sphere has been taken as consideration then in classical computing bits are resided either of two poles of sphere but in quantum computing qubit can be any point of the sphere. When qubit system is applied to classical computers, to represents states of an *n-qubit* system it requires the storage of 2^n complex coefficient, where classical computers represent states by only *n*- bit. So it can be said that using less energy quantum computing can store more information than classical computing. A qubit can be represented as

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \tag{3}$$

where, $|0\rangle$ denotes "ground state" and $|1\rangle$ is known as "excited state" and α, β are complex numbers follow the quantum orthogonality property, presented as

$$\alpha^2 + \beta^2 = 1 \tag{4}$$

Another property of quantum computing is *quantum entanglement*. In this property quantum states are highly correlated to each other so that it is hardly differentiable. It is a tensor product of states given as

$$|\vartheta_1\rangle \otimes |\vartheta_2\rangle.$$

Quantum measurement is the procedure where entangled states are converted to its corresponding single state. From equation 3, it can be stated that to transform the function $|\psi\rangle$ in a single state $|0\rangle$ and $|1\rangle$ have the probability of α^2 and β^2 respectively.

Quantum gates [Nielsen, 2002] are reversible in nature. They are represented by unitary matrices. Different types of quantum gates are used like Hadamard gate [Maitra,2005], Pauli-X gate (= NOT gate), Pauli-Y gate, Pauli-Z gate, Square root of NOT gate (ÖNOT), Phase shift gates, Swap gate, Square root of Swap gate, Controlled gates, Toffoli gate [Muthukrishnan, 1999], Fredkin gate [Lee, 2010]. In this article quantum rotational gate is used which is defined as

$$\begin{pmatrix} \alpha'_i \\ \beta'_i \end{pmatrix} = \begin{pmatrix} \cos \theta_i & -\sin \theta_i \\ \sin \theta_i & \cos \theta_i \end{pmatrix} \begin{pmatrix} \alpha_i \\ \beta_i \end{pmatrix} \tag{5}$$

where (α_i, β_i) and (α'_i, β'_i) are the i^{th} qubit before and after updating; and θ_i denotes the rotation angle between α_i and β_i .

DIFFERENT QUALITY EVALUATION METRICS

Quality evaluation metrics are different statistical mathematical formulas which apply to the output result to verify the efficiency of the applied method. It measures the quality of output segmented image after applying different segmentation on an image. In this article three quality evaluation metrics, one correlation coefficient (ρ) and two empirical measures ($F'(I)$ and $Q(I)$) are defined which show the goodness of segmented result.

Correlation Coefficient (ρ)

It is a standard measure metric which measures the degree of similarity between original and segmented image [De, 2012]. This is defined as

$$\rho = \frac{\frac{1}{n^2} \sum_{i=1}^n \sum_{j=1}^n (X_{ij} - \bar{X})(Y_{ij} - \bar{Y})}{\sqrt{\frac{1}{n^2} \sum_{i=1}^n \sum_{j=1}^n (X_{ij} - \bar{X})^2} \sqrt{\frac{1}{n^2} \sum_{i=1}^n \sum_{j=1}^n (Y_{ij} - \bar{Y})^2}} \quad (6)$$

where \bar{X} stands for mean of the original image and \bar{Y} stands for mean of the segmented image. As the ρ value of the segmented image increases, the quality of the segmentation enhances. X_{ij} , $1 \leq i, j \leq n$ and Y_{ij} , $1 \leq i, j \leq n$ are the original and the segmented images respectively, each of dimensions $n \times n$.

$F'(I)$

It is another evaluation function which is introduced by Borosotti *et al.* [Borosotti, 1998].

$$F'(I) = \frac{1}{1000S_M} \sqrt{\sum_{u=1}^{max\ area} [N(u)]^{1+\frac{1}{u}} \sum_{Re=1}^N \frac{e_{Re}^2}{\sqrt{S_{Re}}}} \quad (7)$$

where, N is the number of segmented regions, S_M represents the area of an original image, $maxarea$ represents the area of the largest region in the segmented image, $N(u)$ refers to the number of regions in the segmented image having an area of exactly u . e_{Re}^2 defines the squared color error of region Re and is presented as

$$e_{Re}^2 = \sum_{v \in (R,G,B)} \sum_{px \in RE_{Re}} (C_v(px) - C_v(\widehat{RE}_{Re}))^2 \quad (8)$$

Here, RE_{Re} signifies the number of pixels placed in region Re . $C_v(\widehat{RE}_{Re})$ is the average value of feature v (Red, Green or Blue) of a pixel px in region Re and is given by

$$C_v(\widehat{RE}_{Re}) = \frac{\sum_{px \in RE_{Re}} C_v(px)}{S_{Re}} \quad (9)$$

where, $C_v(px)$ denotes the value of component v for pixel px .

Q(I)

It is another evaluation function proposed by Borosotti *et al.* [Borosotti, 1998]. It is actually modified version of $F'(I)$.

$$Q(I) = \frac{1}{1000S_M} \sqrt{N} \sum_{Re=1}^N \left[\frac{e_{Re}^2}{1 + \log S_{Re}} + \left(\frac{N(S_{Re})}{S_{Re}} \right)^2 \right] \quad (10)$$

where, $N(S_{Re})$ stands for the number of regions having an area S_{Re} .

PROPOSED METHODOLOGY

In this article, a quantum induced modified genetic algorithm based FCM algorithm is proposed for true color image segmentation. FCM suffers with some difficulties which are described before. Quantum induced Modified Genetic algorithm is added to FCM to solve the convergence problem of FCM. In case of FCM, initial cluster centroids play a very important role. If they are not defined properly then the algorithm may stuck to the local minima point which hampers the ultimate segmented result.

Despite of superiority of GA, a modified genetic algorithm (MfGA) [Das, 2016] is introduced to enhance the efficacy of GA. In MfGA, population initialization and crossover part are modified to some extent which increases optimality of GA. In case of GA, when chromosomes are created by randomly selecting their cluster centroids, then perhaps the difference between two cluster centroids are too small that these are not considered as different cluster. To bring down this situation a weighted mean formula is formulated in MfGA. In crossover section, fixed crossover probability is modified in that way that the probability varies at every iteration. Crossover probability indicates the ratio that how many couples are chosen for mating purpose. As in GA a fixed crossover probability is used so when good chromosomes are mated with bad chromosomes there is a possibility that good chromosomes are not stored in population pool for next generation. So in MfGA, crossover probability is formulated in that manner that at each iteration crossover probability is decreased as iterations are increased. Selection and mutation sections are same in both GA and MfGA. After running the method optimal class levels are generated which are fed to FCM for ultimate result. Though MfGA provides more optimal results than GA but it takes huge computational time. To remit this computational time as well as cost quantum computing concept is added to MfGA.

True Color Image Segmentation Using Quantum-Induced Modified-Genetic-Algorithm

Here the proposed methodology is applied to true color images. A true color image consists of three color components viz *Red*(R), *Green* (G) and *Blue* (B). So it is the first job to segregate R , G , B as different color components. Now this QIMfGA based FCM algorithm is applied to each plane to get the output. A brief description of this proposed algorithm is given here. After decomposing the image into three color planes, the population pool P is generated for each plane i.e. population pool for red, population pool for green and population pool for blue. Now the procedure is applied to each population pool simultaneously. This population pool is generated using the weighted mean formula of MfGA. Each chromosome contains a set of centroids which are actually the pixel intensity values. Now as per the rule of quantum computing these intensity values are randomly converted to the any real number between 0 and 1 thus create the population P' . Applying quantum orthogonality property to population P' we get another population called P'' . Afterwards quantum rotational gate is embedded to P'' for quick convergence and the ultimate population P^+ is evolved. Now selection, crossover and mutation are applied to P^+ . After compilation of first iteration the child solutions are spawned which are added to the parent solution and create population P' for next generation maintaining the fixed population size. Again from P' , P'' and P^+ are formed and the same procedure is iterated for certain time. After completion of QIMfGA near-optimal solutions are produced which are employed to FCM as initial input cluster centres thus the desired segmented output is get. As this method is applied to R , G , B planes differently so the segmented output is also produced for three planes differently. So as a last step the three segmented results are merged and the final true color segmented output image is formed. The total procedure in step by step manner is demonstrated below:

Quantum Inspired MfGA (QIMfGA) Based FCM Algorithm

Input

1. Number of segment
2. Size of population
3. Number of iterations
4. Maximum crossover probability and minimum crossover probability
5. Mutation probability
6. Error

Procedure

Step 1: At the very first step a true color image is to be decomposed into R , G , B three color components. Now the following steps are applied to each color plane separately.

Step 2: After segregating the image, population pool is created for each plane. Here to segment an image into N partitions, $N+1$ number of initial class levels which are actually pixel intensity values, are randomly selected. Afterwards using the weighted mean formula ultimate N number of class levels are generated. Following this concept a set of chromosomes is produced called population pool P for each plane. The weighted mean defined as

$$N_i = \frac{\sum_{j=L_i}^{L_{i+1}} f_j * I_j}{\sum_{j=L_i}^{L_{i+1}} f_j} \quad (11)$$

where L_i and L_{i+1} are the temporary class levels, f_j is the frequency of the j^{th} pixel and I_j denotes pixel intensity value of j^{th} pixel.

Step 3: Each pixel intensity value of each chromosome is now encoded with the real number between 0 and 1, and formed new population P' .

Step 4: In population P' , quantum orthogonality property is applied to create population P'' .

Step 5: For quick convergence, lastly quantum rotational gate is induced to each chromosome of population P'' ; and final population P^+ is generated for further processing.

Step 6: The method propagates by manipulating the fitness values based on some fitness functions, and based on those fitness values better fitted chromosomes are selected using Roulette-wheel selection method for crossover and mutation operations.

Step 7: Crossover is happened based on crossover probability. Here crossover probability depends on the maximum and minimum crossover probability and is decreased as the iterations are increased. It can be defined as

$$C_p = C_{max} - \frac{C_{max} - C_{min}}{Iteration_{max} - Iteration_{current}} \quad (12)$$

where C_{max} and C_{min} are the maximum and minimum crossover probability; and $Iteration_{max}$ and $Iteration_{current}$ indicate maximum and present iteration number.

Step 8: After crossover, the child solutions are passed to the mutation part where they are mutated according to mutation probability.

Step 9: Now the mutated child solutions are mixed with parent solution and create the population P' .

Step 10: For a certain time of iteration, this algorithm follows the step 4 to step 9 and after that the optimized result is produced.

Step 11: This optimized class levels are now employed to FCM as the initial class levels thus get the desired segmented output.

Step 12: The desired segmented output for each color component are now merged and formed the final true color segmented image.

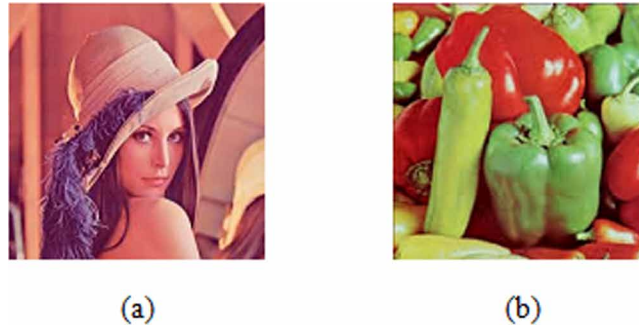
EXPERIMENTAL RESULT AND ANALYSIS

Segmentation results of true color images using Quantum induced modified genetic algorithm (QIM-fGA) based FCM algorithm are demonstrated in this section. Two true color test images viz Lena and Peppers with size of 256 X 256 are used here for segmentation purpose. Though the segmentation re-

True Color Image Segmentation Using Quantum-Induced Modified-Genetic-Algorithm

sults are taken for different number of clusters but here results are presented only for $K = \{6, 8\}$ clusters. Experimental results of both classical MfGA based FCM and conventional FCM are also presented in this section. Those results are compared with respect to their efficiency based on three quality measure metrics ρ , F' and Q .

Figure 7. Original color image (a) Lena (b) Peppers



In initial phase it is needed to define value of some constant terms which play important role in the proposed method. GA considers a fixed population size, a crossover probability and also a mutation probability throughout the method. A population of 50 is considered here as fixed population size. Unlike GA, in MfGA a maximum and minimum crossover probability is used, as in MfGA the crossover probability varies with respect to iteration. In this methodology maximum and minimum crossover probability is applied as 0.9 and 0.5 respectively, based on which the present crossover probability for that instance of iteration is manipulated. After crossover the child solutions are taken part in mutation operation to make them more fitted. Mutation are committed based on mutation probability which is considered here as 0.01. After the mutation better solutions are evolved and mixed up with previous parent solution but maintain their population size. After certain iterations the ultimate class levels are generated which are employed to FCM as initial class levels thus the ultimate segmented results are formed.

Segmented result of color image of Lena based on three measurement functions ρ , F' and Q are demonstrated in Table 1, Table 2 and Table 3 respectively. Those tables are structured in that manner that the first column defines the number of segment, second column indicates methods which are applied to test color image, third and fourth column present serial number and class levels of corresponding applied method, respectively and lastly the fitness value is presented. These methods are applied to the test images many times but only three good results are presented in this section. The best result obtained by any process for each number of segments are highlighted by boldfaced.

The mean and standard deviation are evaluated for each algorithm based on each fitness functions and are reported in Table 4. The mean computational time for FCM is also presented in the same table. It is known that if initial class levels of FCM are defined properly then FCM easily reaches to its goal. In this table the mean time indicates that, in minimum time span FCM meets to its goal using the proposed methodology than both classical MfGA based FCM and conventional FCM methods.

True Color Image Segmentation Using Quantum-Induced Modified-Genetic-Algorithm

Table 1. Class boundaries and evaluated segmentation quality measures, ρ by different algorithms for different classes of Lena image.

# Segments	Algorithm	#	Class Levels	Fit val
6	Conventional FCM	1	R={ 89, 110,152, 181, 208, 219}	0.9623
			G={ 24, 65,98, 126, 153, 196}	
			B={ 57, 78, 99, 111,152, 181}	
		2	R={ 90, 116,152, 181, 208, 233}	0.9326
			G={ 21, 64,95, 120, 153, 196}	
			B={ 60, 78, 110, 121,152, 181}	
		3	R={ 90, 116,152, 181, 208, 233}	0.9320
			G={ 24, 63,95, 126, 150, 196}	
			B={ 57, 78, 99, 121,152, 181}	
MfGA based FCM	MfGA based FCM	1	R={ 93, 130,170, 198, 218, 238}	0.9806
			G={ 24, 63,95, 126, 153, 196}	
			B={ 57, 78, 99, 121,152, 181}	
		2	R={ 92, 125,152, 190, 213, 233}	0.9768
			G={ 21, 63,95, 126, 153, 196}	
			B={ 57, 78, 99, 121,152, 181}	
		3	R={ 90, 116,152, 181, 208, 233}	0.9832
			G={ 24, 63,95, 126, 153, 196}	
			B={ 57, 78, 99, 121,152, 181}	
Proposed	Proposed	1	R={93, 126, 170, 188, 219, 233}	0.9898
			G={24, 63, 95, 126, 154, 196}	
			B={56, 78, 99, 123, 152, 181}	
		2	R={91, 130, 170, 192, 211, 238}	0.9874
			G={25, 63, 98, 126, 158, 196}	
			B={57, 81, 99, 121, 152, 181}	
		3	R={93, 130, 170, 198, 219, 238}	0.9859
			G={24, 63, 95, 126, 154, 196}	
			B={57, 78, 101, 121, 149, 181}	
8	Conventional FCM	1	R={86,106,138,168,188,205,222,239}	0.9126
			G={20,43,67,92,114,135,164,198}	
			B={55,73,90,106,121,139,161,185}	
		2	R={ 86,106,138,165,182,201,220,241}	0.9257
			G={18,43,65,92,110,135,164,196}	
			B={54,72,89,104,120,138,160,185}	
		3	R={83,101,128,155,178,202,221,239}	0.9543
			G={20,43,69,92,114,135,164,198}	
			B={55,73,90,105,121,139,161,185}	

continues on following page

True Color Image Segmentation Using Quantum-Induced Modified-Genetic-Algorithm

Table 1. Continued

# Segments	Algorithm	#	Class Levels	Fit val
	MfGA based FCM	1	R={83,101,128,155,178,202,221,239}	0.9815
			G={20,43,68,92,114,135,164,198}	
			B={45,63,79,95,112,128,156,183}	
		2	R={81,101,129,155,175,202,221,239}	0.9824
			G={20,43,67,92,114,135,164,198}	
			B={55,73,90,105,121,139,161,185}	
		3	R={83,101,128,155,178,202,221,239}	0.9792
			G={20,43,67,92,114,135,164,198}	
			B={45,63,79,95,112,128,156,183}	
	Proposed	1	R={81,100,128,159,178,202,221,239}	0.9876
			G={20,44,67,91,119,135,164,198}	
			B={45,63,79,95,112,128,156,189}	
		2	R={83,101,134,155,178,202,221,239}	0.9864
			G={20,46,67,92,114,135,164,198}	
			B={45,63,83,98,112,128,156,185}	
		3	R={84,101,128,155,178,202,221,239}	0.9861
			G={21,43,70,92,114,135,164,198}	
			B={45,63,80,95,112,128,156,183}	

Table 2. Class boundaries and evaluated segmentation quality measures, F' by different algorithms for different classes of Lena image.

# segments	Algorithm	#	Class Levels	Fit val
6	Conventional FCM	1	R={ 89, 110,150, 179, 218, 236}	326547.42
			G={ 24, 64,95, 125, 150,198}	
			B={ 57, 79, 101, 121,152, 181}	
		2	R={ 91, 116,152, 181, 210, 233}	254791.34
			G={ 25, 63,95, 125, 153, 196}	
			B={ 52, 70, 99, 120,152, 186}	
		3	R={ 90, 118,156, 181, 210, 233}	289325.74
			G={ 24, 63,95, 126, 153, 196}	
			B={ 59, 80, 99, 121,152, 181}	

continues on following page

True Color Image Segmentation Using Quantum-Induced Modified-Genetic-Algorithm

Table 2. Continued

# segments	Algorithm	#	Class Levels	Fit val
	MfGA based FCM	1	R={ 90, 116,152, 181, 208, 233}	58484.59
			G={ 24, 63,95, 125, 153, 196}	
			B={ 57, 80, 101,121,152, 181}	
		2	R={ 91, 116,154, 181, 208, 231}	75358.72
			G={ 21, 63,95, 128, 153, 196}	
			B={ 58,78, 99, 120,152, 181}	
		3	R={ 90, 116,153, 181, 209, 230}	66751.31
			G={ 24, 63,95, 126, 153, 196}	
			B={ 57, 79, 99, 120,151, 181}	
	Proposed	1	R={40, 78, 111, 145, 183, 236}	43698.47
			G={38, 68, 98,128, 158, 192}	
			B={21, 56, 89, 122, 165, 210}	
		2	R={93, 130, 171, 198, 219, 238}	45744.65
			G={24, 63, 95, 126, 154, 196}	
			B={57, 78, 101, 121, 152, 181}	
		3	R={92, 130, 172, 198, 219, 238}	39778.79
			G={24, 63, 90, 126, 156, 198}	
			B={57, 78, 99, 121, 152, 181}	
8	Conventional FCM	1	R={86,106,139,168,190,205,222,239}	987636.25
			G={20,43,67,92,114,135,164,198}	
			B={45,63,79,95,112,128,156,183}	
		2	R={81,102,139,162,188,206,220,238}	1270489.10
			G={21,46,65,93,111,135,165,190}	
			B={57,72,86,106,120,138,161,185}	
		3	R={83,100,128,152,178,202,221,240}	1025394.78
			G={20,43,69,92,114,135,162,198}	
			B={54,71,91,105,122,139,161,185}	
	MfGA based FCM	1	R={86,106,126,138,168,188,220,239}	332122.96
			G={20,43,68,93,114,136,199,165}	
			B={45,68,79,95,111,128,156,183}	
		2	R={86,106,138,168,188,205,222,239}	394524.47
			G={20, 45, 68,93,115,136, 199,165}	
			B={55,73,90,106,121,139,161,185}	
		3	R={87,106,138,168,189,205,222,239}	316578.63
			G={21,43,68,93,115,136,166,201}	
			B={55,73,90,106,121,139,161,185}	

continues on following page

True Color Image Segmentation Using Quantum-Induced Modified-Genetic-Algorithm

Table 2. Continued

# segments	Algorithm	#	Class Levels	Fit val
Proposed		1	R={88,110,138,168,187,205,222,242}	146789.25
			G={21,43,68,96,115,136,167,199}	
			B={54,73,90,106,121,141,163,185}	
		2	R={86,106,138,168,188,205,220,239}	254789.69
			G={20,45,68,93,114,136,166,199}	
			B={55,73,90,106,121,139,161,187}	
		3	R={86,106,138,168,188,208,222,238}	298772.72
			G={20,43,68,93,119,136,161,199}	
			B={52,73,98,106,121,139,161,185}	

Table 3. Class boundaries and evaluated segmentation quality measures, **Q** by different algorithms for different classes of Lena image.

# segments	Algorithm	#	Class Levels	Fit val
6	Conventional FCM	1	R={ 89, 110,150, 181, 218, 233}	25315.77
			G={ 24, 63,95, 125, 150,198}	
			B={ 57, 79, 100, 121,152, 181}	
		2	R={ 91, 116,152, 181, 208, 233}	21973.64
			G={ 25, 63,95, 126, 153, 196}	
			B={ 52, 70, 99, 120,152, 181}	
		3	R={ 90, 115,156, 181, 210, 233}	26977.81
			G={ 24, 63,95, 126, 153, 196}	
			B={ 57, 78, 99, 121,152, 181}	
MfGA based FCM		1	R={ 90, 116,152, 181, 208, 233}	9299.335
			G={ 24, 63,95, 126, 153, 196}	
			B={ 57, 80, 99, 121,152, 181}	
		2	R={ 90, 116,154, 181, 208, 231}	8973.337
			G={ 24, 63,95, 128, 153, 196}	
			B={ 57, 78, 99, 120,152, 181}	
		3	R={ 90, 116,153, 181, 209, 230}	9555.05
			G={ 24, 63,95, 126, 153, 196}	
			B={ 57, 78, 99, 121,152, 181}	

continues on following page

True Color Image Segmentation Using Quantum-Induced Modified-Genetic-Algorithm

Table 3. Continued

# segments	Algorithm	#	Class Levels	Fit val
	Proposed	1	R={40, 78, 111, 145, 183, 236}	6459.53
			G={38, 68, 98,128, 158, 192}	
			B={21, 56, 88, 122, 165, 210}	
		2	R={93, 130, 170, 198, 219, 238}	7473.59
			G={24, 63, 95, 126, 154, 196}	
			B={57, 78, 99, 121, 152, 181}	
		3	R={92, 130, 172, 198, 219, 238}	6648.63
			G={24, 63, 90, 126, 156, 198}	
			B={57, 78, 99, 121, 152, 181}	
8	Conventional FCM	1	R={86,106,138,168,188,205,222,239}	70869.63
			G={20,43,67,92,114,135,164,198}	
			B={45,63,79,95,112,128,156,183}	
		2	R={81,102,139,162,188,206,220,238}	84254.32
			G={21,42,65,93,114,135,165,199}	
			B={54,72,86,106,120,138,161,185}	
		3	R={83,100,128,152,178,202,221,240}	69701.27
			G={20,43,69,92,114,135,162,198}	
			B={54,73,90,105,121,139,161,185}	
	MfGA based FCM	1	R={86,106,126,138,168,188,222,239}	45944.56
			G={20,43,68,93,114,136,199,165}	
			B={45,63,79,95,112,128,156,183}	
		2	R={86,106,138,168,188,205,222,239}	50472.78
			G={20, 43, 68,93,115,136, 199,165}	
			B={55,73,90,106,121,139,161,185}	
		3	R={86,106,138,168,188,205,222,239}	51976.51
			G={20,43,68,93,115,136,166,199}	
			B={55,73,90,106,121,139,161,185}	
	Proposed	1	R={87,110,138,168,187,205,222,242}	35679.23
			G={21,43,68,96,115,136,167,199}	
			B={54,73,90,105,121,141,161,185}	
		2	R={86,106,138,168,188,205,220,239}	39543.87
			G={20,45,68,93,114,136,166,199}	
			B={55,73,90,106,121,139,161,185}	
		3	R={86,106,138,168,188,208,222,238}	38453.16
			G={20,43,68,93,118,136,161,199}	
			B={52,73,95,106,121,139,161,185}	

Table 4. Different algorithm based mean and standard deviation using different types of fitness functions and mean of time taken by different algorithms for Lena image.

Fit. fn.	# segments	Algorithm	Mean \pm Std. Div.	Mean time
ρ	6	Conventional FCM	0.9510 \pm 0.0173	00:02:22
		MfGA based FCM	0.9850 \pm 0.0011	00:01:58
		Proposed	0.9874\pm0.0015	00:01:46
	8	Conventional FCM	0.9237 \pm 0.0144	00:02:57
		MfGA based FCM	0.9831 \pm 0.0023	00:02:43
		Proposed	0.9865\pm0.0009	00:02:01
F'	6	Conventional FCM	273668.44 \pm 104648.48	00:02:39
		MfGA based FCM	66674.73 \pm 9941.64	00:02:23
		Proposed	43297.81\pm8716.32	00:01:51
	8	Conventional FCM	3275837.43 \pm 4373796.89	00:03:10
		MfGA based FCM	404902.11 \pm 119179.93	00:02:48
		Proposed	222546.40\pm67476.67	00:02:12
Q	6	Conventional FCM	16551.48 \pm 6437.06	00:02:40
		MfGA based FCM	8830.74 \pm 654.32	00:02:05
		Proposed	6972.52\pm314.87	00:01:51
	8	Conventional FCM	85576.15 \pm 13697.8	00:02:53
		MfGA based FCM	51898.67 \pm 8452.06	00:02:41
		Proposed	39273.63\pm5439.23	00:02:06

If a comparison is done between proposed methodology and both classical MfGA based FCM and conventional FCM methods, then it will be seen that fitness value as well as mean time of proposed method are better than the other two methods. This indicates that the class levels generated by QIMfGA always be better than other two methods so that when it is employed to FCM, the ultimate result is more convenient in respect of fitness value and computational time.

The same procedures are applied on Peppers image. The class boundaries along with their fitness value based on fitness function of ρ , F' and Q for each algorithm applied on that image are reported in Table 5, Table 6 and Table 7 respectively. Good results for each method are enlightened.

In Table 8, mean and standard deviation of fitness value for each algorithm are demonstrated. Mean time has taken by those algorithms are also reported here. If the accounted results are taken as consideration then it will be cleared that the proposed methodology outperforms than classical MfGA based FCM and conventional FCM.

The segmented output results for each method according to fitness functions and class levels is reported here. Figure 8 presents the color segmented image of Lena for 6 segments based on fitness function ρ . Here the first row shows the segmented result by conventional FCM, second row represents segmented image by MfGA based FCM and third row indicates segmented image by QIMfGA based FCM. In the same manner segmented images of Lena for 8 segment based on fitness function Q are depicted in Figure 9.

True Color Image Segmentation Using Quantum-Induced Modified-Genetic-Algorithm

Table 5. Class boundaries and evaluated segmentation quality measures, ρ by different algorithms for different classes of Peppers image.

# segments	Algorithm	#	Class Levels	Fit val
6	Conventional FCM	1	R={45, 87, 118, 147, 176, 201}	0.9190
			G={10, 48, 96, 143, 178, 206}	
			B={7,42, 62, 92, 132, 184}	
		2	R={45, 87, 118, 147, 176, 201}	0.8964
			G={10, 48,96, 143, 178, 206}	
			B={5, 39, 70, 92, 132, 184}	
		3	R={45, 87, 118, 147, 176, 201}	0.9197
			G={9, 52, 96, 143, 178, 206}	
			B={8, 39, 70, 92, 132, 184}	
MfGA based FCM	MfGA based FCM	1	R={90, 116, 152, 181, 208, 233}	0.9814
			G={24, 63, 95, 126, 153, 196 }	
			B={57, 78, 99, 121, 152, 181}	
		2	R={42, 87, 120, 147, 175, 200}	0.9837
			G={15, 48, 99, 142, 178, 206}	
			B={8,39, 70, 92, 131, 185}	
		3	R={45, 87, 118, 147, 176, 201}	0.9850
			G={10, 48, 96, 143, 178, 206}	
			B={8,39, 70, 92, 132, 184}	
Proposed	Proposed	1	R={45, 88, 118, 150, 176, 200}	0.9865
			G={10, 48, 96, 145, 178, 204}	
			B={8,42, 70, 93, 132, 184}	
		2	R={45, 87, 116, 147, 176, 201}	0.9889
			G={10, 49, 96, 141, 178, 206}	
			B={8, 39, 73, 92, 132, 189}	
		3	R={45, 87, 118, 147, 176, 201}	0.9878
			G={10, 48, 96, 143, 178, 208}	
			B={6, 42, 70, 92, 132, 185}	
8	Conventional FCM	1	R={41, 80, 110, 129, 150, 172, 192, 208}	0.9289
			G={5, 32, 54, 90, 126, 159, 184, 208}	
			B={6, 30, 44, 67, 86, 109, 147, 191}	
		2	R={42, 79, 111, 129, 152, 172, 198, 203}	0.9436
			G={5,33,54,91,125,159,184,208}	
			B={5,30,43,63,80,108,147,191}	
		3	R={42,81,109,129,155,172,198,209}	0.9164
			G={5,33,54,91,125,160,184,208}	
			B={5,30,44,69,80,108,147,191}	

continues on following page

True Color Image Segmentation Using Quantum-Induced Modified-Genetic-Algorithm

Table 5. Continued

# segments	Algorithm	#	Class Levels	Fit val
	MfGA based FCM	1	R={40,77,108,127,148,170,190,207}	0.9841
			G={5,32,53,90,125,159,184,208}	
			B={6,35,51,74,91,115,193,152}	
		2	R={41,79,110,129,150,171,192,208}	0.9833
			G={5,32,53,90,125,159,184,208}	
			B={5,29,43,67,86,109,147,191}	
		3	R={41,80,110,129,151,172,192,208}	0.9812
			G={5,32,53,90,125,159,184,208}	
			B={5,30,44,68,86,109,148,191}	
	Proposed	1	R={42,78,110,127,148,171,190,207}	0.9873
			G={5,32,53,93,125,163,185,208}	
			B={6,37,51,74,89,115,193,152}	
		2	R={40,77,108,127,148,170,190,207}	0.9879
			G={5,32,53,90,125,159,184,208}	
			B={6,35,51,74,91,118,193,152}	
		3	R={42,77,108,129,148,170,190,209}	0.9884
			G={5,32,51,90,125,159,184,208}	
			B={8,35,51,74,90,115,193,155}	

Table 6. Class boundaries and evaluated segmentation quality measures, F' by different algorithms for different classes of Peppers image.

# segments	Algorithm	#	Class Levels	Fit val
6	Conventional FCM	1	R={ 45, 89, 110, 150, 166, 198 }	493779.18
			G={8, 49, 98, 143, 178, 206}	
			B={ 6, 41, 64, 91, 132, 184}	
		2	R={ 48, 85, 118, 147, 176, 199 }	214505.86
			G={10,59, 91, 140, 178, 202}	
			B={ 8, 41, 70, 92, 132, 184}	
		3	R={ 48, 75, 111, 147, 176, 198 }	476584.74
			G={10, 51, 98, 143, 178, 200}	
			B={ 8, 41,78, 92, 132, 184}	

continues on following page

Table 6. Continued

# segments	Algorithm	#	Class Levels	Fit val
8	MfGA based FCM	1	R={45, 87, 118, 147, 176, 201}	36987.49
			G={10, 48, 96, 143, 178,206}	
			B={8, 39, 70, 92, 132, 184}	
		2	R={49, 83, 120, 147, 178, 200}	45896.87
			G={10, 48, 96, 143, 206, 178}	
			B={8, 39, 70, 92, 132, 184}	
		3	R={48, 87, 118, 147, 176, 201}	54256.52
			G={10, 51,96, 143,187, 208 }	
			B={6, 41, 69, 92, 132, 184}	
8	Proposed	1	R={51, 89, 120, 147, 176, 201}	21547.91
			G={10, 48, 96, 143, 179,208}	
			B={8, 39, 71, 92, 132, 185}	
		2	R={45, 87, 118, 145, 176, 202}	26797.79
			G={11, 48, 96, 143, 178,206}	
			B={7, 39, 70, 92, 132, 184}	
		3	R={45, 89, 118, 147, 178, 201}	31687.54
			G={10, 51, 96, 143, 181,206}	
			B={7, 39, 10, 92, 132, 184}	
8	Conventional FCM	1	R={40,80,112,129,155,172,192,208}	1270489.09
			G={6,35,55,98,132,163,187,209}	
			B={6,38,52,76,91,115,152, 193}	
		2	R={41,79,110,130,150,172,192,208}	2976124.94
			G={6,35,56,98,132,187,163,209}	
			B={5,37,52,71,91,112,152, 199}	
		3	R={41,79,110,129,150,169,192,208}	2457839.24
			G={4,34,54,97,130,187,163,209}	
			B={6,35,52,74,91,115,152, 193}	
8	MfGA based FCM	1	R={41,79,110,129,150,171,208, 192}	413654.65
			G={5,34,55,95,130,162,186,209}	
			B={6,35,51,74,90,152,115,193}	
		2	R={41,79,110,129,150,172,192,208}	453259.44
			G={5,34,125,90,53,184,159,208}	
			B={5,31,45,69, 110,123,148,191}	
		3	R={41,79,110,150,129,152,172,208}	513697.46
			G={5,33,54,92,127,160,185,208}	
			B={5,31,44,68,86,110,191,148}	

continues on following page

True Color Image Segmentation Using Quantum-Induced Modified-Genetic-Algorithm

Table 6. Continued

# segments	Algorithm	#	Class Levels	Fit val
Proposed		1	R={41,81,110,129,150,171,208, 192}	298534.74
			G={5,34,52,95,131,167,186,209}	
			B={6,35,49,74,90,152,116,193}	
		2	R={41,79,111,129,150,171,198,208}	312599.66
			G={5,34,55,98,130,162,186,209}	
			B={6,35,51,74,90,152,115,193}	
		3	R={45,80,110,131,150,171,208, 192}	371675.49
			G={5,34,55,95,130,162,186,209}	
			B={6,35,44,67,87,115,149,193}	

Table 7. Class boundaries and evaluated segmentation quality measures, **Q** by different algorithms for different classes of Peppers image.

# segments	Algorithm	#	Class Levels	Fit val
6	Conventional FCM	1	R={ 45, 89, 110, 150, 166, 198 }	31566.56
			G={8, 48, 96, 143, 178, 206}	
			B={ 6, 39, 64, 90, 132, 184}	
		2	R={ 48, 85, 118, 147, 176, 201 }	32759.42
			G={ 10, 58, 90, 140, 178, 202}	
			B={ 8, 41, 70, 92, 132, 184}	
3	R={ 48, 75, 111, 147, 176, 198 }	26457.05		
	G={10, 48, 98, 143, 178, 200}			
	B={ 8, 39, 76, 92, 132, 184}			
MfGA based FCM		1	R={45, 87, 118, 147, 176, 201}	9546.87
			G={10, 48, 96, 143, 178,206}	
			B={8, 39, 70, 92, 132, 184}	
		2	R={49, 83, 120, 147, 178, 200}	9854.54
			G={10, 48, 96, 143, 206, 178}	
			B={8, 39, 70, 92, 132, 184}	
		3	R={45, 87, 118, 147, 176, 201}	10443.71
			G={10, 48,96, 143,187, 208 }	
			B={6, 40, 70, 92, 132, 184}	

continues on following page

Table 7. Continued

# segments	Algorithm	#	Class Levels	Fit val
	Proposed	1	R={51, 89, 120, 147, 176, 201}	7964.61
			G={10, 48, 96, 143, 179,208}	
			B={8, 39, 71, 92, 132, 185}	
		2	R={45, 87, 118, 145, 176, 202}	7818.24
			G={11, 48, 96, 143, 178,206}	
			B={8, 39, 70, 92, 132, 184}	
		3	R={45, 87, 118, 147, 178, 201}	8158.46
			G={10, 51, 96, 143, 181,206}	
			B={7, 39, 10, 92, 132, 184}	
8	Conventional FCM	1	R={40,80,112,129,155,172,192,208}	38569.22
			G={6,38,55,98,132,163,187,209}	
			B={6,35,52,76,91,115,152, 193}	
		2	R={41,79,110,130,150,172,192,208}	39320.89
			G={6,38,56,97,132,187,163,209}	
			B={5,35,52,71,91,112,152, 195}	
		3	R={41,79,110,129,150,169,192,208}	38628.41
			G={4,34,54,97,130,187,163,209}	
			B={6,35,52,74,91,115,152, 193}	
	MfGA based FCM	1	R={41,79,110,129,150,171,208, 192}	33285.41
			G={5,34,55,95,130,162,186,209}	
			B={6,32,51,74,90,152,115,193}	
		2	R={41,79,110,129,150,172,192,208}	31316.45
			G={5,32,125,90,53,184,159,208}	
			B={5,31,45,69, 110,123,148,191}	
		3	R={41,79,110,150,129,152,172,208}	33654.86
			G={5,33,54,92,127,160,185,208}	
			B={5,31,44,68,86,110,191,148}	
	Proposed	1	R={41,81,110,129,150,171,208, 192}	29766.79
			G={5,34,52,95,131,167,186,209}	
			B={6,35,49,74,90,152,116,193}	
		2	R={41,79,111,129,150,171,208, 192}	28497.41
			G={5,34,55,98,130,162,186,209}	
			B={6,35,51,74,90,152,115,193}	
		3	R={45,80,110,131,150,171,208, 192}	31657.55
			G={5,34,55,95,130,162,186,209}	
			B={6,35,44,67,87,115,149,193}	

True Color Image Segmentation Using Quantum-Induced Modified-Genetic-Algorithm

Table 8. Different algorithm based mean and standard deviation using different types of fitness functions and mean of time taken by different algorithms for Peppers image.

Fit. fn.	# segments	Algorithm	Mean \pm Std. Div.	Mean time
ρ	6	Conventional FCM	0.9098 \pm 0.0111	00:01:46
		MfGA based FCM	0.9835 \pm 0.0054	00:01:24
		Proposed	0.9869\pm0.0023	00:01:09
	8	Conventional FCM	0.9289 \pm 0.0329	00:02:51
		MfGA based FCM	0.9826 \pm 0.0017	00:02:25
		Proposed	0.9879\pm0.0043	00:02:02
F'	6	Conventional FCM	316707.31 \pm 190897.43	00:02:06
		MfGA based FCM	44909.88 \pm 6770.82	00:01:56
		Proposed	26750.14\pm3717.35	00:01:24
	8	Conventional FCM	2313022.28 \pm 730888.96	00:03:12
		MfGA based FCM	492546.95 \pm 76658.40	00:02:51
		Proposed	326238.85\pm31805.60	00:02:06
Q	6	Conventional FCM	39094.12 \pm 29621.6	00:02:06
		MfGA based FCM	10256.26 \pm 3028.12	00:01:56
		Proposed	8074.45\pm2201.54	00:01:12
	8	Conventional FCM	39260.52 \pm 10019.85	00:03:08
		MfGA based FCM	33894.33 \pm 2601.31	00:02:49
		Proposed	27701.33\pm2809.64	00:02:04

In Figure 10 and Figure 11, 6-class levels and 8-class levels segmented result for Peppers image are depicted based on F' and Q as fitness functions respectively. From those images it is clear that proposed algorithm is better than the classical MfGA based FCM and conventional FCM.

A statistical one way ANOVA analysis is also deduced here for each test images. This test ensures that rejection of null hypothesis. One way ANOVA test is actually analyze statistical difference between more than two independent group mean. If the value of F is greater than value of F_{crit} then it reject the null hypothesis. If the Table 9 and Table 10 are considered, then it will be clearly shown that $F > F_{crit}$ which indicates that they reject null hypothesis that means the group means are different and independent. In this analysis 5% significance level is used.

CONCLUSION

A quantum induced modified genetic algorithm (QIMfGA) based FCM clustering approach is discussed here for segmentation of true color images. This method has been compared with its classical counterpart and also with conventional FCM. In this article class levels for different number of segments based on different fitness functions are reported. The convergence time of FCM for each method are also shown here. Considering all accounted results, one can concluded that after incorporating quantum concepts into classical methods the results are changed in drastic manner. Quantum version is not only efficient

by its fitness value but it also effectively reduces execution time which makes it cost effective. From all stated and presented facts and figures it is concluded that the proposed methodology qualitatively and quantitatively is more superior to its classical approach and conventional FCM for true color image segmentation.

Figure 8. 6-class segmented 256×256 Lena image with the class levels obtained by (a-c) FCM (d-f) MfGA based FCM (g-i) QIMfGA based FCM algorithm of three results of Table 1 with ρ as the quality measure.



True Color Image Segmentation Using Quantum-Induced Modified-Genetic-Algorithm

Figure 9. 8-class segmented 256×256 Lena image with the class levels obtained by (a-c) FCM (d-f) MfGA based FCM (g-i) QIMfGA based FCM algorithm of three results of Table 3 with Q as the quality measure.



Table 9. Single ANOVA analysis based on for ρ for Lena image

Anova: Single Factor						
SUMMARY						
Groups	Count	Sum	Average	Variance		
Conventional FCM	10	9.2367	0.92367	0.00020968		
MfGA based FCM	10	9.8311	0.98311	5.0677E-06		
QIMfGA based FCM	10	9.8655	0.98655	8.9611E-07		
ANOVA						
Source of Variation	SS	df	MS	F	P-value	F crit
Between Groups	0.024996139	2	0.012498069	173.867367	3.786E-16	3.354130829
Within Groups	0.001940835	27	7.18828E-05			
Total	0.026936974	29				

True Color Image Segmentation Using Quantum-Induced Modified-Genetic-Algorithm

Figure 10. 6-class segmented 256×256 Peppers image with the class levels obtained by (a-c) FCM (d-f) MfGA based FCM (g-i) QIMfGA based FCM algorithm of three results of Table 6 with F' as the quality measure.

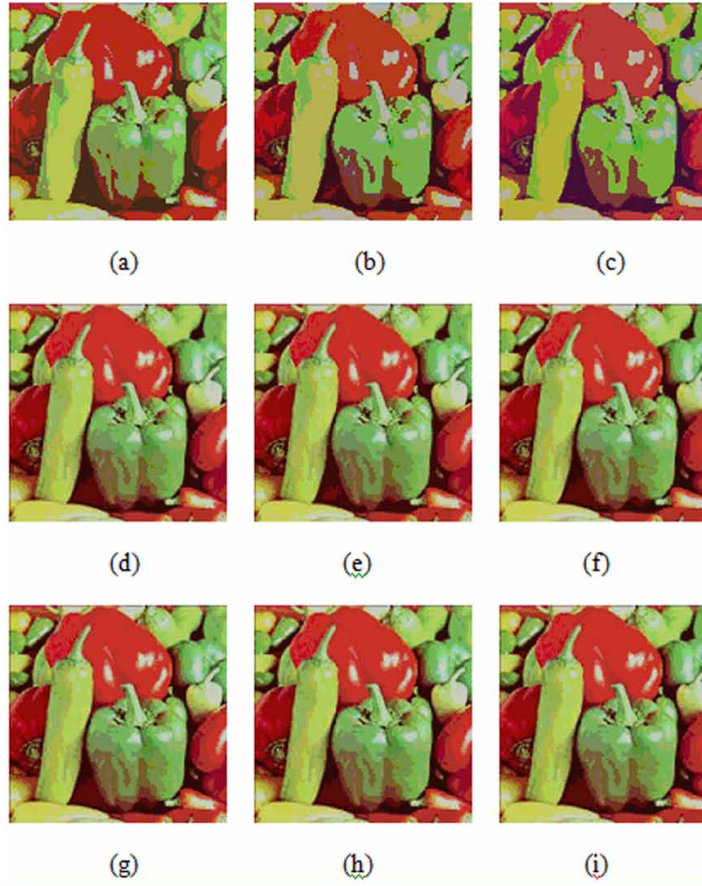
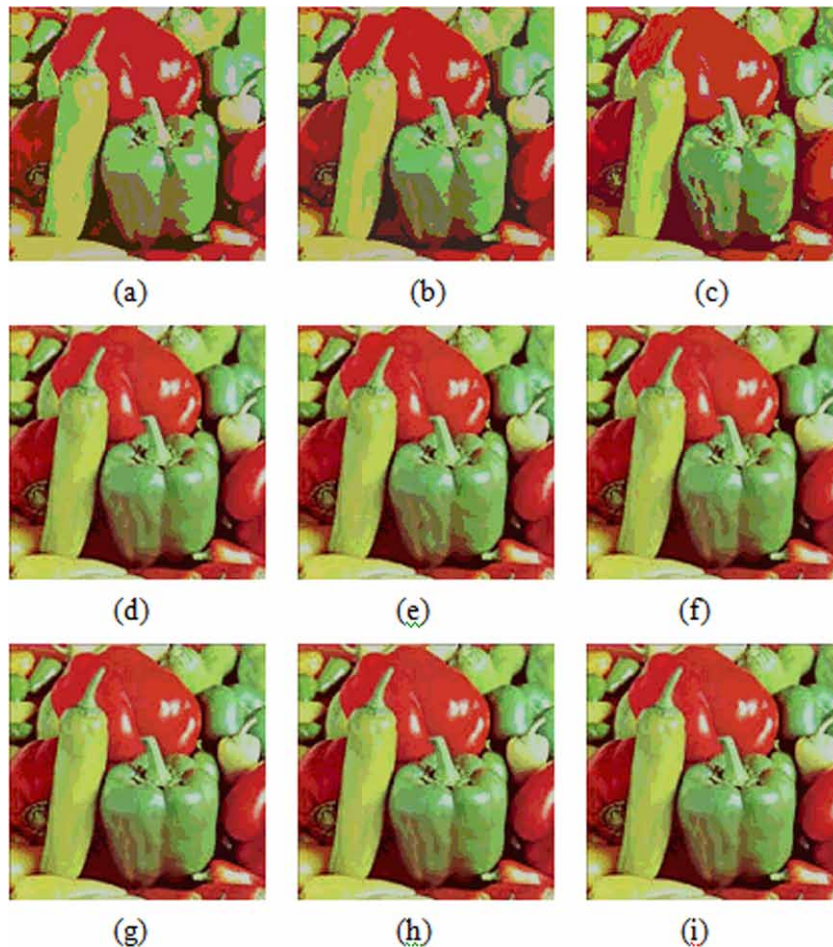


Table 10. Single ANOVA analysis based on for Q for Peppers image

Anova: Single Factor						
SUMMARY						
Groups	Count	Sum	Average	Variance		
Conventional FCM	10	392605.29	39260.529	100397451.1		
MfGA based FCM	10	338943.35	33894.335	6766814.343		
QIMfGA based FCM	10	277013.35	27701.335	7894109.613		
ANOVA						
Source of Variation	SS	df	MS	F	P-value	F crit
Between Groups	669214202	2	334607101	8.724452278	0.001195	3.354131
Within Groups	1.036E+09	27	38352792			
Total	1.705E+09	29				

Figure 11. 8-class segmented 256×256 Peppers image with the class levels obtained by (a-c) FCM (d-f) MfGA based FCM (g-i) QIMfGA based FCM algorithm of three results of Table 7 with Q as the quality measure.



REFERENCES

- Amelio, A., & Pizzuti, C. (2013). A Genetic Algorithm for Color Image Segmentation. In A. I. Esparcia-Alc'azar (Eds.), *EvoApplications, LNCS 7835* (pp. 314–323). Verlag Berlin Heidelberg. doi:10.1007/978-3-642-37192-9_32
- Anh, N. T. L., Kim, S. H., Yang, H. J., & Lee, G. S. (2013). Color Image Segmentation using Morphological Gradient based Active Contour Model. *International Journal of Innovative Computing, Information, & Control*, 9(11), 4471–7784.
- Arumugadevi, S., & Seenivasagam, V. (2016). Color Image Segmentation Using Feedforward Neural Networks with FCM. *International Journal of Automation and Computing*, 13(5), 491–500. doi:10.1007/11633-016-0975-5

- Bezdek, J. C. (1981). *Pattern Recognition with Fuzzy Objective Function Algorithms*. New York: Plenum. doi:10.1007/978-1-4757-0450-1
- Bhattacharyya, S. (2011). A Brief Survey of Color Image Preprocessing and Segmentation Techniques. *Journal of Pattern Recognition Research*, 1(1), 120–129. doi:10.13176/11.191
- Borsotti, M., Campadelli, P., & Schettini, R. (1998). Quantitative evaluation of color image segmentation results. *Pattern Recognition Letters*, 19(8), 741–747. doi:10.1016/S0167-8655(98)00052-X
- Chaabane, S. B., Bouchouicha, M., & Fnaiech, F. (2015). *A Hybrid Technique for Color Image Segmentation: Application to the Fire Forest Images*. *International Journal of Scientific Engineering and Research*.
- Chen, M., & Ludwig, S. A. (2017). *Color Image Segmentation Using Fuzzy C-Regression Model*. *Advances in Fuzzy Systems*.
- Das, S., & De, S. (2016). Multilevel Color Image segmentation using Modified Genetic Algorithm (MfGA) inspired Fuzzy C-Means Clustering. *Second International Conference on Research and Computational Intelligence and Communication Networks (ICRCICN)*, 1, 78-83. 10.1109/ICRCICN.2016.7813635
- De, S., Bhattacharyya, S., & Chakraborty, S. (2010). True color image segmentation by an optimized multilevel activation function. *IEEE International Conference on Computational Intelligence and Computing Research*, 545-548. 10.1109/ICCIC.2010.5705833
- De, S., Bhattacharyya, S., & Chakraborty, S. (2012). Color image segmentation using parallel OptiMUSIG activation function. *Appl. Soft Comp. J.*, 12(10), 3228–3236. doi:10.1016/j.asoc.2012.05.011
- De, S., Bhattacharyya, S., & Chakraborty, S. (2013). Color Image Segmentation by NSGA-II based ParaOptiMUSIG Activation Function. *IEEE International Conference on Machine Intelligence Research and Advancement*, 105 - 109. 10.1109/ICMIRA.2013.27
- Dey, S., Bhattacharyya, S., & Maulik, U. (2013). Quantum inspired meta-heuristic algorithms for multi-level thresholding for true colour images. *2013 Annual IEEE Conference on India Conference (INDICON)*, 1-6. 10.1109/INDICON.2013.6726024
- Dey, S., Bhattacharyya, S., & Maulik, U. (2014). New quantum inspired tabu search for multi-level colour image thresholding. *2014 IEEE International Conference on Computing for Sustainable Global Development (INDIACom)*, 311-316. 10.1109/IndiaCom.2014.6828150
- Dong, G., & Xie, M. (2005). Color Clustering and Learning for Image Segmentation Based on Neural Networks. *IEEE Transactions on Neural Networks*, 16(4), 925–936. doi:10.1109/TNN.2005.849822 PMID:16121733
- Dunn, J. C. (1973). A Fuzzy Relative of the ISODATA Process and Its Use in Detecting Compact Well-Separated Clusters. *Journal of Cybernetics*, 3(3), 32–57. doi:10.1080/01969727308546046
- Goldberg, D. E. (1989). *Genetic Algorithm in Search Optimization and Machine Learning*. New York: Addison-Wesley.
- Gonzalez, R. C., & Woods, R. E. (2002). *Digital image processing*. Upper Saddle River, NJ: Prentice Hall.

True Color Image Segmentation Using Quantum-Induced Modified-Genetic-Algorithm

- Harrabi, R., & Braiek, E. B. (2014). Color image segmentation using a modified Fuzzy C-Means technique and different color spaces: Application in the breast cancer cells images. *2014 1st International Conference on Advanced Technologies for Signal and Image Processing (ATSIP)*, 231-236.
- Krishna, R. V. V., & Kumar, S. S. (2015). Color Image Segmentation using Soft Rough Fuzzy-C-Means Clustering and SMO Support Vector Machine. *An International Journal on Signal & Image Processing*, 6(5), 49. doi:10.5121/ipij.2015.6504
- Kulkarni, N. (2012). Color Thresholding Method for Image Segmentation of Natural Images, *I.J. Image. Graphics and Signal Processing*, 1(1), 28–34. doi:10.5815/ijigsp.2012.01.04
- Lee, J., Huang, X., & Zhu, Q. (2010). Decomposing Fredkin Gate into Simple Reversible Elements with Memory. *International Journal of Digital Content Technology and its Applications*, 4(5).
- Li, Y., Feng, S., Zhang, X., & Jiao, L. (2014). SAR image segmentation based on quantum-inspired multiobjective evolutionary clustering algorithm. *Information Processing Letters*, 114(6), 287–293. doi:10.1016/j.ipl.2013.12.010
- Maitra, A., & Parashar, P. (2005). *Hadamard type operations for qubits*. arXiv:quant-ph/0505068v1
- Mao, X., Zhang, Y., Hu, Y., & Binjie, S. (2009). Color Image Segmentation Method Based on Region Growing and Ant Colony Clustering. *Intelligent Systems, GCIS*, 09. doi:10.1109/GCIS.2009.344
- Mcmohan, D. (2008). *Quantum computing explained*. Hoboken, NJ: John Wiley & Sons.
- Mekhmoukh, A., & Mokrani, K. (2015). Improved Fuzzy C-Means based Particle Swarm Optimization (PSO) initialization and outlier rejection with level set methods for MR brain image segmentation. *Computer Methods and Programs in Biomedicine*, 122(2), 266–281. doi:10.1016/j.cmpb.2015.08.001 PMID:26299609
- Menon, P. S., & Ritwik, M. (2014). A Comprehensive but not Complicated Survey on Quantum Computing. *2014 International Conference on Future Information Engineering*, 10, 144 – 152. 10.1016/j.ieri.2014.09.069
- Muthukrishnan, A. (1999). *Classical and Quantum Logic Gates: An Introduction to Quantum Computing*. Quantum Information Seminar, Rochester Center for Quantum Information.
- Nebti, S. (2013). Bio-Inspired Algorithms for Color Image Segmentation. *International Journal of Computers and Applications*, 73(18).
- Nielsen, M. A., & Chuang, I. L. (2002). *Quantum Computation and Quantum Information*. Cambridge University Press.
- Preetha, M. M. S. J., Suresh, L. P., & Bosco, M. J. (2015). Cuckoo Search Based Color Image Segmentation Using Seeded Region Growing. In C. Kamalakannan, L. Suresh, S. Dash, & B. Panigrahi (Eds.), *Power Electronics and Renewable Energy Systems* (Vol. 326). New Delhi: Academic Press. doi:10.1007/978-81-322-2119-7_154
- Rahman, H., & Islam, R. (2013). Segmentation of color image using adaptive thresholding and masking with watershed algorithm. *2013 International Conference on Informatics, Electronics & Vision (ICIEV)*. 10.1109/ICIEV.2013.6572557

Talbi, H., Draa, A., & Batouche, M. (2004). A New Quantum-Inspired Genetic Algorithm for Solving the Travelling Salesman Problem. *2004 IEEE International Conference on Industrial Technology*, 3, 1192-1197.

Tao, W., Jin, H., & Zhang, Y. (2007). Color Image Segmentation Based on Mean Shift and Normalized Cuts. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 37(5), 1382 – 1389. doi:10.1109/TSMCB.2007.902249

Verma, O. P., Hanmandlu, M., Susan, S., Kulkarni, M., & Jain, P. K. (2011). A Simple Single Seeded Region Growing Algorithm for Color Image Segmentation using Adaptive Thresholding. *2011 International Conference on Communication Systems and Network Technologies (CSNT)*. 10.1109/CSNT.2011.107

Zadeh, L. A. (1965). Fuzzy sets. *Information and Control*, 8(3), 338–353. doi:10.1016/S0019-9958(65)90241-X

KEY TERMS AND DEFINITIONS

Cluster: Data having homogeneous characteristics form a group called a cluster.

Clustering: It is a segmentation technique that groups the objects in such a manner that objects of the same group are more similar than objects residing in other groups.

FCM: It is a soft clustering technique used for segmentation purpose. It works on the principle of fuzzy set theory.

Genetic Algorithm: It is a probabilistic technique used to achieve optimal solutions for large problem space. It imitates working procedures of natural evolution.

Quantum Computing: It makes the direct use of quantum mechanics principle on data to get more reliable output.

Segmentation: In this process a set of non-homogeneous data are partitioned in non-overlapping homogeneous data sets.

Statistical Measure: It provides some mathematical formulas that are used to assess the quality of the output image.

This research was previously published in Quantum-Inspired Intelligent Systems for Multimedia Data Analysis; pages 55-94, copyright year 2018 by Engineering Science Reference (an imprint of IGI Global).

Chapter 8

Grayscale Image Segmentation With Quantum-Inspired Multilayer Self-Organizing Neural Network Architecture Endorsed by Context Sensitive Thresholding

Pankaj Pal

RCC Institute of Information Technology, India

Siddhartha Bhattacharyya

 <https://orcid.org/0000-0003-0360-7919>

RCC Institute of Information Technology, India

Nishtha Agrawal

RCC Institute of Information Technology, India

ABSTRACT

A method for grayscale image segmentation is presented using a quantum-inspired self-organizing neural network architecture by proper selection of the threshold values of the multilevel sigmoidal activation function (MUSIG). The context-sensitive threshold values in the different positions of the image are measured based on the homogeneity of the image content and used to extract the object by means of effective thresholding of the multilevel sigmoidal activation function guided by the quantum superposition principle. The neural network architecture uses fuzzy theoretic concepts to assist in the segmentation process. The authors propose a grayscale image segmentation method endorsed by context-sensitive thresholding technique. This quantum-inspired multilayer neural network is adapted with self-organization. The architecture ensures the segmentation process for the real-life images as well as synthetic images by selecting intensity parameter as the threshold value.

DOI: 10.4018/978-1-7998-8593-1.ch008

INTRODUCTION

Image processing using image segmentation is a difficult task to recover the objects from multilevel images. So many research approaches have been taken out to reconstruct the object from the multilevel background, but it still remains a fallacy to recover the true objects ideally. The multilayer self organizing neural network (MLSONN) architecture is unable to extract the gray scale objects from the blurred and noisy atmosphere which is designed by Ghosh et al., 1993 (Ghosh et al., 1993) and is used to extract the binary objects efficiently. Here, interconnection weights of different layers viz. between input to hidden layer and hidden to output layer are updated by means of fuzzy measures. This architecture is limited only for the bi-level sigmoid activation function to segment the binary images. The authors (Pal et al., 1993) have described the color image segmentation technique using fuzzy and non-fuzzy methods considering segmentation of range images and neural network based approaches. The authors (Pantofaru et al., 2005) have presented the result of the mean shift segmentation and the efficient graph-based segmentation techniques for objective evaluation algorithm describing the three components viz. the Correctness, the Stability with respect to parameter choice and the Stability with respect to image choice. If these characteristics are fully satisfied by the segmentation technique, then it can be more useful by larger systems. The authors have considered the pixel location and color feature for each and every image for this segmentation algorithm using the Berkeley segmentation database. The authors (Bhattacharyya et al., 2007) have described on the true color image segmentation by self supervised PSONN architecture using multilevel sigmoidal activation function. Regarding this proposed architecture, it is the extension version of standard single self organizing neural network architecture (SONN) and comprises input or source layer, three middle layers for segmentation of three primary color components and the output layer or sink layer. To segment the color image for first object recovery in large image database, the probability of pixel distribution is implemented (Kang et al., 2008). After incorporating three channel images of R, G and B from the given image, and then applying pixel distribution is taken out using similarity measures using the well known defined distribution function Weibull, Exponential, Beta, Gamma, Normal, and Uniform. Using the measurement of sum least of square error, to fit the image to the distribution. Under consideration of minimum amount of error, image is quantized to gray levels for three channels of distribution using threshold value and then these three channel values are fused together to get the desired information. Few years' latter authors (Bhattacharyya et al., 2010) proposed multilevel image segmentation using a MUSIG activation function which is more efficient to extract the multilevel images by means of functionally modifying the network. The MUSIG activation function is characterized by ignoring heterogeneity of the image information content for understanding equal and fixed class responses. The authors De S. et al. (De S. et al., 2010) described under consideration of the heterogeneity of the image information content in the segmented images by applying optimized MUSIG (OptiMUSIG) activation function. OptiMUSIG activation function is used in another way to segment the true color image segmentation (De S. et al, 2012) on optimized class responses on self organizing neural network architecture. The authors De S. et al. considered generic based optimized segmentation method. Gray scale image is segmented (De S. et al., 2012) on optimized class responses without considering the heterogeneity of image information content by optimization of MUSIG (OptiMUSIG) activation function. It may or may not generate good quality of segmented outputs. There are so many research works have been done to recover the object from the different images. Segmentation is one of the approaches where object is reconstructed from the image. The gray scale image is segmented to recover the object by means of context sensitive thresholding implementation technique. In this chapter, the authors propose a

gray scale image segmentation method with a quantum inspired based neural network architecture having multilayer self organization nature with endorsed by context sensitive thresholding approaches, which is more efficient to extract the multilevel gray scale objects. The objective of this chapter is to extend the functional modification of QMLSONN architecture so as to segment the gray scale multilevel images by adapting the context sensitive thresholding using multilevel sigmoidal activation function (MUSIG) activation function as shown in Figure 1. Quantum computer has the ability to segment the gray scale images very efficiently as the extraction time is very less as compared to the classical computation technique. Quantum bit is able to do this job tactically using the quantum superposition principle. In this chapter, authors use the segmentation technique using a context sensitive thresholding concept to improve the image intensity information. In the process of image segmentation, image is subdivided i.e. segmented into different classes corresponding to correlate in different regions according to the required features of interest. Here the pixels of compactness of groups are taken together as a whole for the stipulated attributes of similar properties. Authors (Yogamangalam et al., 2013) have described the different image segmentation techniques, mentioning Markov Random Field (MRF) is the strongest and the simplest method for cancelling the noise to recover the object from the noisy atmospheric image. According to the authors' overview, the segmented parts are enclosed to cancel the noise more easily from the noisy image. Binary object is extracted from the noisy environment is efficiently done using quantum version of MLSONN architecture, proposed by Bhattacharyya et al. (Bhattacharyya et al., 2014).

Image segmentation using quantum computation plays an important role in the field of image processing to reconstruct and recollect the objects from the original background. In classical approaches, an image is segmented using the classical bits either zero ('0') or one ('1') in the thresholding technique. In this chapter authors propose the quantum version of MLSONN architecture that is known as QMLSONN architecture. It is used to segment the gray scale/ multilevel images efficiently using the multilevel sigmoidal activation function (MUSIG) activation function accompanied by context sensitive thresholding technique. In the QMLSONN architecture the inter connection weights are in the form of rotation gates and follow a second order neighborhood topology. The processing nodes of the different layers are simply qubits and are represented as

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$$

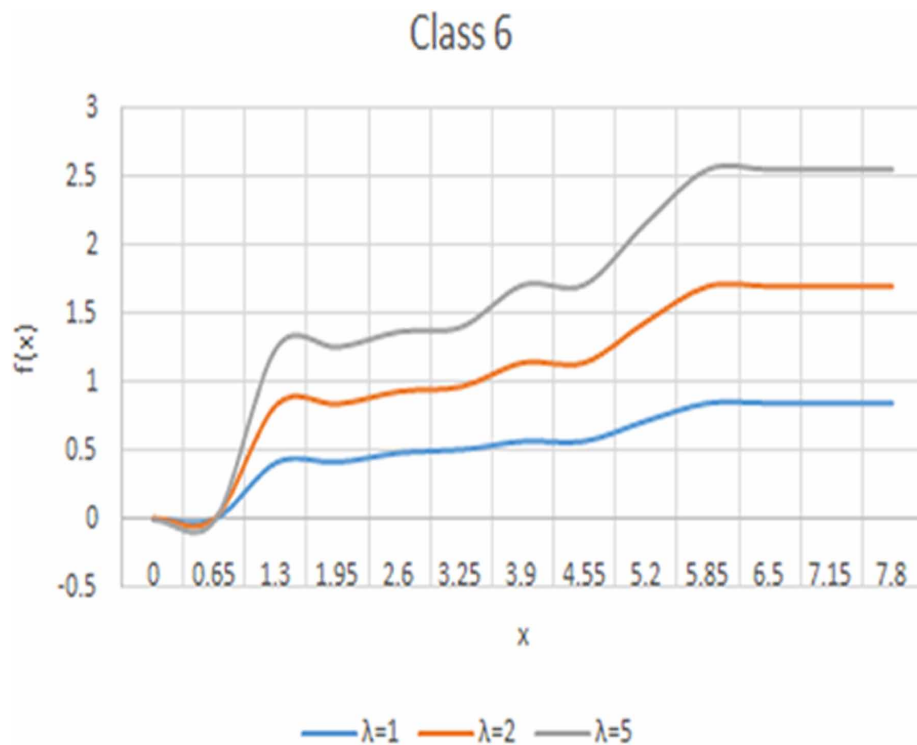
where, α and β are the probability amplitudes corresponding to $|0\rangle$ and $|1\rangle$ respectively, provided that $\alpha^2 + \beta^2 = 1$. The qubits in the input layer, hidden layer and output layers look like as given:

$$\begin{pmatrix} \langle\beta_{11}| & \langle\beta_{12}| & \dots & \dots & \langle\beta_{1n}| \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ \langle\beta_{m1}| & \langle\beta_{m2}| & \dots & \dots & \langle\beta_{mn}| \end{pmatrix} \dots \begin{pmatrix} \langle\lambda_{11}| & \langle\lambda_{12}| & \dots & \dots & \langle\lambda_{1n}| \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ \langle\lambda_{m1}| & \langle\lambda_{m2}| & \dots & \dots & \langle\lambda_{mn}| \end{pmatrix} \dots \begin{pmatrix} \langle\delta_{11}| & \langle\delta_{12}| & \dots & \dots & \langle\delta_{1n}| \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ \langle\delta_{m1}| & \langle\delta_{m2}| & \dots & \dots & \langle\delta_{mn}| \end{pmatrix}$$

Qubits of input layer *Qubits of hidden layer* *Qubits of output layer*

The organization of this chapter is as follows. Firstly introduction section illustrates the use of MUSIG activation function on MLSONN and QMLSONN architectures along with the concepts of qubits in the input, hidden and output layers. After that the concept of fuzzy logic behind the image pixels intensity using the fuzzy hostility, fuzzy cardinality, etc are described and measured. Covering these discussions the architectures of MLSONN and QMLSONN are explained one by one for gray scale image segmentation. In the next phase of this chapter, the various segmentation techniques are explained. Here gray scale image segmentation using quantum computation by means of superposition principle is discussed. After that, the various thresholding techniques in existence are discussed. In this phase it is illustrated as to how the segmentation efficiency is measured and the skewness measurement in thresholding is done using various threshold strategies. Last but not least, there is a result, discussion and comparison between the MLSONN and QMLSONN architectures. The final section of this chapter ends with a conclusion and few references are given for further study.

Figure 1. Three types of MUSIG functions



QUBITS AND RELATED THINGS

The basic unit of quantum computation is known as quantum bits or simply qubits. In classical computation system, the bit is represented either '0' or '1' but in quantum computation qubit is the superposition of '0' and '1'. At any moment qubit represents '0' and '1' simultaneously. The qubit can be represented as

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1}$$

Here, α and β represent the probability amplitudes of $|\phi\rangle$ for finding $|0\rangle$ and $|1\rangle$ respectively provided $\alpha^2 + \beta^2 = 1$

The notation $|\ \rangle$ is represented as ket notation. In quantum gates, qubit acts as unitary operator in Hilbert space (Aytekin et al., 2013).

The qubit is represented in matrix notation as $\begin{bmatrix} \cos \varphi \\ \sin \varphi \end{bmatrix}$

To process the information on qubit, the rotation gate is used and is used as

$$R(\theta) = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}$$

In quantum mechanics, the qubits have distinct properties such as superposition, entanglement, coherence, de-coherence, etc., which is more useful to design quantum gates to process the information (Bhattacharyya et al., 2013).

CONCEPT OF IMAGE

Image is considered as two dimensional $m \times n$ array of elements in the form of matrix pattern arranged as a numbers of square pixels (picture elements) having manipulated in the rows and columns fashion. It has different intensity distribution of the permutation of various pixels I_{ij} . $I = I_{ij}$, where, I_{ij} ($i \leq m$ and $j \leq n$) are the intensities of $m \times n$ image. A gray scale image in 8-bit notation having the intensity values in the range from 0 (black) to maximum 255 (white). Gray scale images can be considered as black and white with more number of gray shades. For segmentation, into class L (where L is considered as number of classes), then the function ‘f’ can be written as for segmentation process using Equation 2.

$$f: I \rightarrow [0 \dots L] \tag{2}$$

For 256 gray levels of L class classification, the group can be considered of gray levels as $\{p_l: 0 \leq l \leq L\}$ provided

$$0 = p_0 \leq p_1 \leq p_2 \dots \leq p_{L-1} \leq p_L \tag{3}$$

all the pixels having the gray levels s_L belong to $[p_{L-1}, p_L]$ of L class contribution. For a particular class in the L class classification the following conditions must be satisfied $s_L \cap s_R = 0$, for $L^1 R$, $1 \leq l, R \leq L$ and $\cup_{l=1}^L s_L = [0 \dots 255]$

FUZZY SET BASICS

Image is considered as a matrix of different fuzzy intensity levels of pixels. So, a fuzzy set can be characterized as a membership function of $\mu_A(x_i)$ of different pixels of fuzzy set (Ross et al., 1995) $A = \{x_1, x_2, x_3, \dots, x_n\}$, where $0 \leq \mu_A(x_i) \leq 1$. The degree of containment of the fuzzy set is defined by the membership (Bhattacharyya et al., 2010) function. More is the degree of containment the membership value of the fuzzy set is close to 1 and less is the degree of containment, lower is the membership value. To understand the fuzziness for two kinds of fuzzy sets A and B having the membership functions $f_A(x)$ and $f_B(x)$, the truth values must lie within the range [0 1]. Two fuzzy sets A and B should be equal provided $f_A(x) = f_B(x), \forall x \in X$. The complement of the fuzzy set A can be written as $A' = 1 - A$. If C be a union of two fuzzy sets A and B having membership functions $f_A(x)$ and $f_B(x)$, then $C = A \cup B$, provided the membership functions are related by the equation $f_C(x) = \text{Max}[f_A(x), f_B(x)], \forall x \in X$, where $f_C(x)$ is the membership function of the fuzzy set C. If C generates a fuzzy set having the membership function $f_C(x)$ after insertion of two kinds of fuzzy sets A and B, having the membership functions $f_A(x)$ and $f_B(x)$, then C is given by $C = A \cap B, \forall x \in X$ and the membership function $f_C(x)$ is given by $f_C(x) = \text{Min}[f_A(x), f_B(x)], \forall x \in X$; the truth values lie within the range [0 1].

Fuzzy Cardinality

Considering finite number of elements, the fuzzy cardinality is defined as the sum of the membership values present within the fuzzy set (Bhattacharyya et al., 2010) and is defined as in the Equation 4 as

$$\xi_A = \sum_{i=1}^n \mu_A(x_i) \quad (4)$$

The fuzzy cardinality will be more if higher is the degree in containment of the elements within the fuzzy set and when the degree of contentment of the element in the fuzzy set is less, and then fuzzy cardinality will be less.

Fuzzy Hostility Index

Any image can be considered as the fuzzy set intensity function. Image is formed by the subsets of neighbors of candidate pixel having different fuzzy set intensity values. The homogeneity of the neighborhood pixels is determined by the closer membership values. Closer are the membership values, higher is the homogeneity and the candidate key is less hostile to its neighbors. The heterogeneity on the other hand determines the rear membership values having the dissimilar intensity values. The neighbors having the homogeneity or heterogeneity are determined by the parameter called hostility index (ζ). The degree of the hostility index for the case of homogeneity or heterogeneity pixels of neighbors for the n^{th} order neighborhood can be determined by equation (Bhattacharyya et al., 2010)

$$\zeta = \frac{3}{2^{n+1}} \sum_{i=1}^{2^{n+1}} \frac{|\mu_p - \mu_{q_i}|}{|\mu_p + 1| + |\mu_{q_i} + 1|} \quad (5)$$

Where, μ_p = membership values of the candidate pixels and μ_{qi} membership values of the i^{th} neighbors of the corresponding pixels. Hostility index (ζ) lies in the range of 0 and 1 [$0 \leq \zeta \leq 1$]. It indicates that the lesser the hostility index (ζ), higher is the homogeneity and higher the hostility index (ζ) higher the heterogeneity.

MLSONN ARCHITECTURE

The classical version of the Multilayer Self Organizing Neural Network Architecture (MLSONN) is shown in Figure 2. It (Ghosh et al., 1993) has the ability to extract objects from noisy blurred images. This self supervised self organizing multilayer neural network architecture is more useful for removal of noise from the real life noisy images for extraction of the objects. It comprises three layers viz. input layer, hidden layer and the output layer. There are two types of connection weights, one is input to hidden layer and another is hidden to output layer. The sigmoidal activation function as shown in equation 6 is applied to initiate the process of noise removing from the noise state of images. Each pixel is connected of the input layer by the connection weight to the pixels of the hidden layer. Similarly, connection weight connects the output layer with the hidden layer. At the output stage the error is calculated and for unrecognized output the process is backpropagated from the output layer to the input layer. This process is continued until a stable output is achieved. The bipolar sigmoidal activation function is illustrated by

$$f(x) = \frac{1}{1 + e^{-\lambda(x-\theta)}} \quad (6)$$

Here, λ parameter decides how the function is stiffer and the parameter θ determines the bias or the threshold value of this function. This bi-level sigmoidal activation function lies in the range 0 to 1 and generates two types of responses, one is bright (1) and another is black (0).

QMLSONN ARCHITECTURE

The Quantum Multilayer Self Organizing Neural Network Architecture (QMLSONN) (Bhattacharyya et al., 2014) is a quantum version of the self organizing self supervised error correction type neural network architecture. Here each and every pixel is considered as a quantum bit having the ability to process the qubit using the second order neighborhood topology. The quantum bit has the ability to process the error correction ability using the threshold values. In the QMLSONN architecture as shown in figure 3, where there are three layers – input layer, hidden layer and lastly the output layer. Each qubit of the input layer is connected to the hidden layer by the connection of rotational quantum gate using the second order neighborhood topology. Similarly, the hidden layer and the output layer are connected by the quantum rotational gates using the second order neighborhood topology. QMLSONN operates on real life images to reconstruct the objects from the blurred and noisy environment. Each of pixel intensity is converted to the fuzzified range [0 1] and then converted to the corresponding quantum bits.

Qubits have the ability to change its phase transform in the quantum states to $\begin{bmatrix} 0 & \frac{\pi}{2} \end{bmatrix}$. In this process

qubits information are summed up and transfer to hidden layer and subsequently to the output layer. At the output stage error is detected and compared with the reference levels and then processed information is fed back to the input layer for further processing by the quantum backpropagation principle. When the error is considered as minimum and the stabilization is achieved then we get the desire output. The single qubit rotational gate (as shown in Equation 7) (Bhattacharyya et al., 2014) is applied to the quantum bits, rotational gate is transformed to the required format to generate the output (as shown below in Equation 8) (Bhattacharyya et al., 2014).

$$R(\theta) = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix} \tag{7}$$

$$R'(\theta) = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix} \begin{bmatrix} \cos \varphi_0 \\ \sin \varphi_0 \end{bmatrix} = \begin{bmatrix} \cos(\theta + \varphi_0) \\ \sin(\theta + \varphi_0) \end{bmatrix} \tag{8}$$

Figure 2. MLSONN Architecture

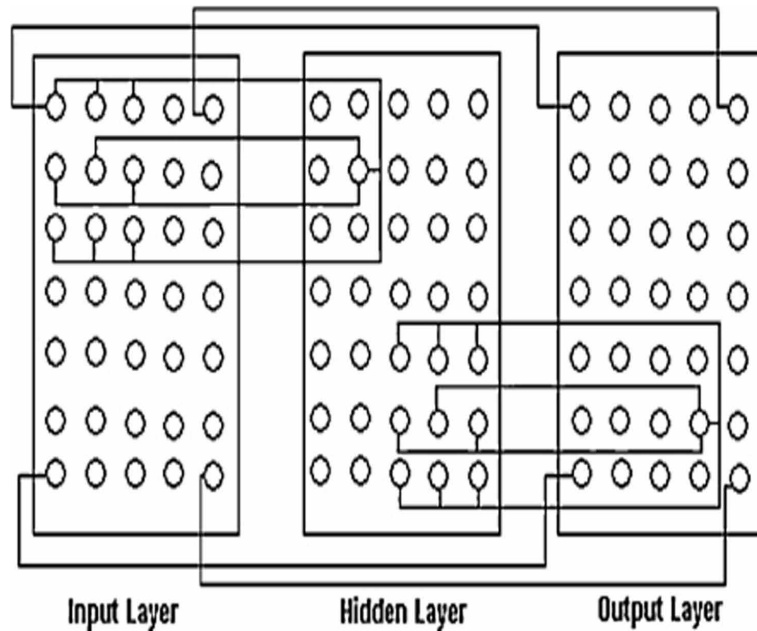
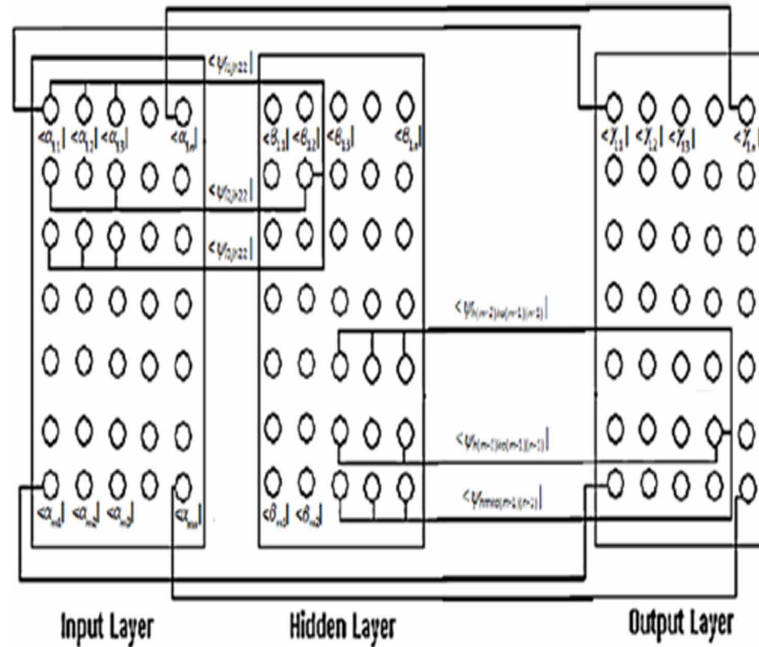


IMAGE SEGMENTATION CLASSIFICATION FUNDAMENTAL AND THE RELATED DIFFERENT METHODS

Image segmentation plays an important role to retrieve the feature measurement for an object belonging to a particular category. Various types of segmentation techniques are adapted for image segmentation

Figure 3. Schematic of QMLSONN



viz. Edge-Based Segmentation, Pixel-Based Segmentation, Region-based Segmentation, Model-Based Segmentation, Clustering Based Segmentation, Watershed Based Segmentation, PDE based Segmentation, ANN Based Segmentation, etc. Authors describe these topics one by one in this chapter.

Edge-Based Segmentation

In this method the information is collected from the edges of the image. Categorically all the edge detection operators are two types. One belongs to 1st order derivatives and other belongs to the 2nd derivatives. Prewitt operator, Sobel operator, Canny operator, Test operator are of 1st order derivatives types where as Laplacian operator, Zero-crossings are of the 2nd derivatives types (Saini et al., 2014). Within this edge it can be determined either by the zero crossing for 2nd order derivatives or by the extremity of the 1st order derivatives. If segmentation of image is not accepted for the segmented outcome, then it can be grouped into chains and are added to recover the whole border of the image using different techniques. As it determines the edge by considering edge detecting operator, so edge cannot be determined when there is no border or where there is no real border exists. In the context of edge detection, three discontinuities are considered as point, line and edge. To solve these discontinuities of an image, spatial masks can be used.

Pixel-Based Segmentation

It is the simplest approach for segmentation technique where the pixel intensity is considered by proper selection algorithm. Here the global value is determined using the different sets of objects by higher standard definition methods (Das et al., 2015). In the process of image segmentation the gray value of

a pixel is used to determine the pixel based segmentation technique. It determines the bias of the gray value on the size of the objects for dissimilar characteristics and makes a conclusion where the darker objects will become of low gray value and the brighter objects will become of high gray value. Authors have used the pixel-based segmentation technique for pixel based for automatic color image segmentation for automatic pipe inspection by the support vector machine (SVM) (Mashford et al., 2007). The RGB, HSB, Gabor, local window and HS feature sets are used by the authors but the HSB feature set gives better performance.

Region-Based Segmentation

Here image is segmented into different sub regions based on continuity method considering similar gray values of one kind of region and different gray values of other kind of regions. To determine the object information, the region based segmentation process may be considered where the candidate pixels and with its neighbors (Saini et al., 2014) have the same gray values. It is very much useful where the noise immunity is high. It is simpler than that of edge based segmentation. In the edge based partition the intensity is changed rapidly from the nearer to the edges and in the region based method partition is based on a predetermined method. Region growing is based on the accumulation of the pixels to make a larger region. To determine the region-based segmentation the algorithm can be described is as follows: (a) selecting the candidate pixel from the original image as considered as seed pixel. (b) Using the selection of the similarities measures according to the intensity value, color, noise, etc. (c) arrange the group of pixels according to predetermined characteristics having similar type of characteristics. (d) stop the region growing procedure when no more pixels can be accommodated with this criterion (Saini et al., 2014).

Model-Based Segmentation

Using this approach, labels are collected by means of pixels having priory known objectives of the image data. Ambiguity or uncertainty may be introduced to generate the labels to (Suetens 1991) pixels. The low level image features may be considered such as homogeneity, discontinuity, etc for pixels generations from the labels in a deterministic approach. Another author has presented the model based segmentation approach where the method is explained in two parts. The first part is the localization process and the second part optimizes the procedure.

Clustering Based Segmentation

It is an unsupervised approach to segment the image to get better information and betterment of the object information (Bora et al., 2014). When partition is being done using clustering based segmentation we consider two properties viz. High Cohesion and Low Coupling. In this clustering technique, the data items having the high similarities may be considered belonging to the High Cohesion property and for Low Coupling prosperity each and every cluster should have different data items. In the clustering principles the cluster is divided in two categories- one is Hard Clustering and another is Soft Clustering. In the hard clustering technique the data items are tightly bound from the other clustering but in case of Soft Clustering the membership values of the data items include their presence in the different clusters. Due to low computational complexity K-Means algorithm is best way for hard clustering technique (Bora et al., 2014).

Watershed Based Segmentation

Before going to watershed based segmentation technique, the segmentation of image is done using the different intensity levels of each pixels and the clusters are generated having the minimum distance. In (Salman, 2006) have combined between K-means, watershed segmentation method, and Difference In Strength (DIS) have been combining for segmentation. At first it is used to determine the watershed segmentation by means of average intensity value of segmented images. In the second part an edge strength method is designed to measure the accurate edge map without the help of watershed algorithm considering the raw data images. Using the different gray values, the image is segmented in different regions (Salman., 2006).

PDE Based Segmentation

An image is segmented by means of Partial Differential Equation (PDE) based mathematical (Sharma et al., 2015) segmentation technique where the boundary is not easily determined or defined. In this numerical approach of PDE based image segmentation technique, the image is segmented in different sections/ parts to retrieve the meaningful information and extract the object from the inaccurate background. In this methodology the contour is determined and boundary is selected for the partitioning of the image to analyze the object information. The authors envisage the contour depending on the level set function considering the two criterions viz. one is outside the boundary and other is inside the boundary for the stipulated segmented region provided the zero level is set at the boundary.

ANN Based Segmentation

Artificial Neural Network (ANN) segmentation technique is very much useful for segmenting images for determination of the object from different noisy perspectives. Authors have used Optical Character Recognition (OCR) (Blumenstein et al., 1998) to retrieve the hand writing using the conventional algorithm along with the ANN based algorithm. Authors have segmented the scanned hand writing character in the height and width accordingly. After segregating the checking is done according to the column of pixels.

MULTILEVEL IMAGE THRESHOLDING

Gray scale image is generally considered as multilevel image. Image is segmented into the different regions depending on the intensity levels. For color image segmentation the intensity value is calculated from the color and for gray scale image segmentation, the intensity value is used from gray levels. (Mishra et al., 2014) design the thresholding technique using particle Swarm Optimization technique for multilevel image segmentation. Considering, the Kapur's entropy criterion method as fitness function to segment an image. In this method they think about the result as better when the swarm size small. Choice of threshold values of the image segmentation process is decided in different ways. Here authors discuss the two kinds of thresholding processes, one is Global Thresholding and another is Multilevel Thresholding.

Global Thresholding

In this segmentation process one threshold value is taken into account. There are two partitions one whose gray value is more than threshold (Mishra et al., 2014) and another is whose gray value is less corresponding to that threshold point. Two segmentation procedures are discussed in this section.

$$I^T(x,y) = 1 \quad (9)$$

for $I(x,y) \geq T$ and

$$I^T(x,y) = 0 \quad (10)$$

for $I(x,y) < 0$

Here, $I^T(x,y)$ and $I(x,y)$ are the segmented image and the pixel of the original image at the pixel point (x, y) . It is very easy to implement this type of design. But one problem arises when the intensity value of color image is same as that of gray scale intensity. Then the sharp pixel intensities are lost. Semi-thresholding is one kind (Mishra et al., 2014) of Global Thresholding technique where the procedure is same but the new intensity value is changed. The intensity value is more than that of original image pixel intensity. Lower intensity value of the pixels below the threshold limit generates a '0' value. As in this case two types of partitions are segregated, so this process is known as bi-level thresholding.

$$I^T(x,y) = I(x,y) \quad (11)$$

for $I(x,y) \geq T$ and

$$I^T(x,y) = 0 \quad (12)$$

for $I(x,y) < 0$

Multilevel Thresholding

To overcome the difficulty in the Global Thresholding process that is in the absence of sharp pixels, the Multilevel Thresholding process is adapted. More thresholding values are used to segment (Mishra et al., 2014) an image. For n number of threshold values, there will be $(n+1)$ partitions. From the mathematical relation one can implement the Multilevel Thresholding having two intensity values T_1 and T_2 for three portions of the segmented image as given below:

$$I^T(x,y) = \begin{cases} V_1 & \text{if } I(x,y) \geq T_2 \\ V_2 & \text{if } I(x,y) \leq I(x,y) < T_2 \\ V_3 & \text{if } I(x,y) \leq T_1 \end{cases} \quad (13)$$

MULTILEVEL SIGMOIDAL ACTIVATION FUNCTION (MUSIG)

For binary image extraction the MLSONN is competent and is able to extract the objects from a noisy environment using a bi-level sigmoidal activation function. It is extended to incorporate the segmentation of gray scale images using the multilevel sigmoidal activation function which is robust in structure and is easier to segment the gray scale images using the QMLSONN architecture. The MUSIG function generates multiple outputs at multiple gray levels to segment multilevel images. In this chapter authors describe the modification of the QMLSONN architecture which is used to gray scale object extraction by means of segmentation technique. The compact form of sigmoidal activation function (as shown in Figure 1) is defined as

$$y = f_M(x) = \frac{1}{\alpha_\gamma + e^{-\lambda(x-\theta)}} \quad (14)$$

where λ represents and decides the steepness of the function; α_γ controls the multilevel class responses (Bhattacharyya et al., 2010) and is defined as $\alpha_\gamma = \frac{C_N}{c_\gamma - c_{\gamma-1}}$. Here, γ is called the gray scale object index and its range is $(1 \leq \gamma < K)$. Here, $K =$ Number of gray scale object index or classes; $c_\gamma = \gamma^{\text{th}}$ gray scale contribution class and $c_{\gamma-1} = (\gamma - 1)^{\text{th}}$ gray scale contribution class. $C_N =$ Neighborhood gray scale contribution class. If we consider $\alpha_\gamma = 1$ then the function behaves as the standard bi-level sigmoidal activation function and is given by

$$y = f_{sig}(x) = \frac{1}{1 + e^{-\lambda(x-\theta)}} \quad (15)$$

$\theta =$ fixed threshold or bias value and is depend on the activation function behavior. From equation (14) one can determine the responses ($y_{s_{\alpha_\gamma}}$) of different subnormal function, where, $(0 \leq y_{s_{\alpha_\gamma}} \leq 1)$ by fixing the suitable parameter α_γ . To determine the ultimate multilevel activation function, we superimpose different subnormal responses, which is more useful for multi-polar responses. The generalized version of the MUSIG function is given below (Bhattacharyya et al., 2010):

$$f(x; \alpha_\gamma, c_\gamma) \leftarrow f(x; \alpha_\gamma, c_\gamma) + (\gamma - 1)f(\gamma c_\gamma), c_{\gamma-1} \leq x < \gamma c_\gamma;$$

Where,

$$f(x; \alpha_\gamma, c_\gamma) = \frac{1}{\alpha_\gamma + e^{-\lambda(x-(\gamma-1)c_{\gamma-1}-\theta)}} \quad (16)$$

The MUSIG function in closer form is given by

$$f_{MUSIG}(x) = \sum_{\lambda=1}^K x + (\lambda - 1)c_{\gamma-1}, c_{\gamma-1} \leq x < \gamma c_{\gamma} \quad (17)$$

Using equation (16), we get MUSIG function as

$$f_{MUSIG}(x; \alpha_{\gamma}, c_{\gamma}) = \frac{1}{\alpha_{\gamma} + e^{-\lambda(x-(\gamma-1)c_{\gamma-1}-\theta)}} \quad (18)$$

For the overall gray scale range, if c_{γ} is of equal values, then it generates the similar subnormal responses ($y_{s_{\alpha_{\gamma}}}$). The ultimate MUSIG activation function constitutes many identical subnormal responses. However, for different c_{γ} , it generates different subnormal lobes with different ranges and different shapes. Using the different values of α_{γ} , the different values of subnormal lobes are combined together to generate the continuity of the resultant multilevel sigmoidal activation function (MUSIG). MUSIG function also generates the bi-level sigmoidal function considering $\alpha_{\gamma}=1$. For the input image, the subnormal responses ($y_{s_{\alpha_{\gamma}}}$), can be obtained from the subnormal lobes generates the multilevel response.

To generate the number of transition lobes, it requires more number of class responses and can be obtained by using the gray scale contribution c_{γ} . The multilevel sigmoidal activation depends on the thresholding parameter θ . The thresholding aspect is discussed in the next article.

THRESHOLDING CONCEPTS OF MULTILEVEL SIGMOIDAL ACTIVATION FUNCTION (MUSIG)

As the threshold parameter θ is considered as a bias value, so, it depends on the design of the multilevel sigmoidal activation function. For better responses, here it is considered as a single fixed point thresholding parameter θ . It ensures that the images are homogeneous in nature. But in the real life situation, real life images are considered as a heterogeneous mixture. So, the thresholding strategy should to adapt to the heterogeneity by tuning the thresholding parameter θ so as to incorporate image information content. In the next subsection, these are elaborated.

Threshold Parameters: θ_{χ_1} and θ_{χ_2} realization of image intensity information based on Skewness

Variation of the intensity of the image pixels depends on the skewness. It is a similarity measurement of pixels having the same intensity or the different intensity levels for a particular image corresponding to a certain limit. Skewness equals to zero means equal distribution of pixels. That means there is a normal distribution. The threshold value of the MUSIG function depends upon the cumulative intensity contribution on the neighbor pixels as the pixel geometry is taken into account. The skewness distribution of relative contributive to each pixel furnishes the overall cumulative contribution. Two types of intensities are considered regarding the brightness controls, one is the brighter side another is the darker side. The scope of the skewness distribution to the brighter end specifies more number of brighter pixels than lesser number of darker pixels. That means more number of brighter pixel populations in the brighter

side than the darker one. Another way to scope the skewness distribution on the darker side specifies more number of darker pixels than lesser number of brighter pixels. Therefore the threshold values of the brighter and the darker pixels are different. For candidate pixels, the neighbors are arranged as having nearly equal types of skewness factor on the threshold. Bhattacharyya et al., 2010 defined the skewness factor χ_1 and χ_2 for the rearranged or sorted neighbor pixels intensity distribution as

$$\chi_1 = \tau_r - \tau_l \tag{19}$$

Here, τ_r and τ_l are the two cumulative skew numbers but having different relations regarding the pixels intensity levels. If we consider the average intensity level for the pixels to be Ω and any arbitrary pixel intensity levels is p , so we can write τ_r exists for $p < \Omega$ and τ_l exists for $p \geq \Omega$. For the second skewness factor χ_2 depends on the medium intensity levels (ν) as well as average intensity levels (Ω) and is given by the relation as

$$\chi_2 = \Omega - \nu . \tag{20}$$

After recognizing the skewness factor χ_1 and χ_2 , if χ_{12} be the resultant skewness factor, so the resultant threshold parameter $\theta_{\chi_{12}}$ can be written as

$$\theta_{\chi_{12}} = \theta \left[\frac{1 - \Omega \chi_{12}}{2\Omega} \right] \tag{21}$$

where, θ is the single fixed point uniform threshold parameter of the MUSIG activation function. Therefore the MUSIG activation function can be written as

$$f_{MUSIG}(x; \alpha_\gamma, c_\gamma) = \sum_{\gamma=1}^{K-1} \frac{1}{\alpha_\gamma + e^{-\lambda(x - (\gamma-1)c_\gamma - \theta_{\chi_{12}})}} \tag{22}$$

Threshold Parameters: θ_ζ realization of pixel neighborhood fuzzy subsets based on the fuzzy cardinality

According to the concept of fuzzy cardinality ξ , the degree of the containment is high when degree of cardinality is high. That means the elements are tightly bound in the fuzzy set. The determination of the pixels having high intensity levels in the fuzzy set of containment to determine the θ_ζ threshold parameters. The determination of the threshold parameters θ_ζ depends on the darker pixels and the brighter pixels having the cardinality values are ζ_d and ζ_b and i_s defined as under considering the single fixed point uniform threshold parameter θ as

$$\theta_{\xi} = \theta \left[1 - \frac{(\theta_b - \theta_d)}{(\theta_b + \theta_d)} \right] \quad (23)$$

Therefore the MUSIG activation function is determined according to the threshold parameter θ_{ξ} is specified as given below

$$f_{MUSIG}(x; \alpha_{\gamma}, c_{\gamma}) = \sum_{\gamma=1}^{K-1} \frac{1}{\alpha_{\gamma} + e^{-\lambda(x-(\gamma-1)c_{\gamma}-\theta_{\xi})}} \quad (24)$$

SEGMENTATION PERFORMANCE OF SEGMENTED GRAY SCALE IMAGES

Determination of the different types of the quality of segmentation is proposed by authors (Liu et al., 1994) using unsupervised manner is discussed here. Evaluation performance functions are designed in three different ways viz. $F(I)$, $F'(I)$, $Q(I)$.

Segmented Efficiency Measurement ($F(I)$)

$$F(I) = \sqrt{K} \sum_{n=1}^K \frac{e_n^2}{\sqrt{S_n}} \quad (25)$$

where, $F(I)$ = Evaluation performance function; K = no. of regions to be segmented; $S_n = |R_n|$ is the n^{th} region; e_n = error of the n^{th} gray scale region. The error of the gray scale region is defined as

$$e_n^2 = \sum_{x \in \gamma = g = b} \sum_{p \in R_n} (C_x(p) - \bar{C}_x(R_n))^2 \quad (26)$$

where, $\bar{C}_x(R_n)$ is defined as the mean value of the gray scale feature x of region n of p^{th} pixel and $C_x(p)$ is defined as

$$\bar{C}_x(R_n) = \frac{\sum_{p \in R_n} C_x(p)}{S_n} \quad (27)$$

$C_x(p)$ is known as the gray scale feature x of pixel p .

Segmented Efficiency Measurement ($F'(I)$)

The authors (Borsotti et al.,1998) have proposed the modified version of the segmentation efficiency, which is more useful to represent the gray scale segmented image and is defined as hereunder

$$F'(I) = \frac{1}{1000S_I} \sqrt{\sum_{a=1}^{Max_{Area}} (N(a))^{1+\frac{1}{a}} \times \sum_{k=1}^N \frac{e_n^2}{\sqrt{S_n}}} \quad (28)$$

Here, $N(a)$ =segmented number of the area a ; Max_{Area} =Maximum area of the estimated segmented region; S_I = Area of the gray scale segmented region of interest under consideration.

Segmented Efficiency Measurement ($Q(I)$)

Improvement of the gray scale image segmentation efficiency as disused in Equation 28, the performance is improved as indicated by Borsotti et al. (Borsotti et al., 1998) and also given by equation below:

$$Q(I) = \frac{1}{1000S_I} \sqrt{N \sum_{n=1}^N \left[\frac{e_n^2}{1 + \log S_I} + \left(\frac{N(S_I)}{S_I} \right)^2 \right]} \quad (29)$$

Here, $N(S_I)$ = no. of regions corresponding the area S_I .

EXPERIMENTAL RESULT AND ANALYSIS

Three types of segmented efficiency measurements are discussed on the basis of two types of gray scale images. One is Baboon image as shown in Figure 4 and another is Lena image as shown in Figure 5 respectively using three classes, viz. class 4, class 6 and class 8. Selected measurement values are shown in boldface type on the table. The values of the segmented efficiency (ν) F , F' and Q using QMLSONN architecture on gray scale Lena image of class 4 are 0.5770, 0.6811 and 0.7432 corresponding to extraction time 25.35s with respect to threshold parameter θ_x , where using MLSONN architecture, these values are 0.8558, 0.9007 and 0.9500 and corresponding to extraction time is 28.49s but when considering threshold parameter θ_c , the values of the segmented efficiency using the QMLSONN architecture are 0.5770, 0.6814 and 0.7432 with extraction time is 24.5s, and when using the MLSONN architecture these values are 0.8551, 0.9007 and 0.95 with corresponding time is 28.2s. All the outputs are collected and recorded as shown in the Table 1 for Lena image and in the Table 2 for Baboon image respectively. The segmented object outputs for class 4 corresponding to threshold parameter θ_x on Baboon image and Lena image as shown in Figure 6. Here, Figure 6 (a, c, e, g, i, k, m, o) shows segmented Baboon images and Figure 6 (b, d, f, h, j, l, n, p) shows Lena images respectively. In Figure 6 (a, b, c, d, e, f, g, h), the extracted object outputs are shown using the MLSONN architecture and Figure 6 (i, j, k, l, m, n, o, p), the extracted object outputs are shown using the QMLSONN architecture.

Grayscale Image Segmentation With Quantum-Inspired Multilayer Self-Organizing NN Architecture

The extracted object output as shown in Figure 7 for Baboon and Lena images using threshold parameter θ_ζ . Here, Figure 7 (a, b, c, d, e, f, g, h) shows the extracted object outputs using MLSONN architecture and Figure 7 (i, j, k, l, m, n, o, p) shows the extracted object outputs using QMLSONN architecture respectively. In Baboon image for class 4, the values of the segmented efficiency F , F' and Q are 0.6183, 0.6658 and 0.7413 respectively, using QMLSONN architecture with extraction time 22.75s for threshold parameter θ_ζ and using MLSONN architecture the values of the segmented efficiency are 0.8660, 0.9100 and 0.9223 with extraction time 27.89s. When the threshold parameter θ_ζ is considered, the value of the gray scale image segmented efficiency (ν) F , F' and Q using QMLSONN architecture, the values of are 0.6185, 0.6658 and 0.7413 with time 22.58s and in case of MLSONN architecture 0.8660, 0.91 and 0.9223 with time 28.1s.

Figure 4. Gray scale Baboon image



Authors have determined the values of segmented efficiency (ν) F , F' and Q are 0.4781, 0.4005 and 0.3486 corresponding to the extraction time 25.2s for gray scale Lena image for class 6 using QMLSONN architecture for threshold parameter θ_ζ where using MLSONN architecture the values of the efficiency are 0.8773, 0.7411 and 0.9221 with time 28.89s. Using the QMLSONN architecture, based on threshold parameter θ_ζ and experiment is performed on Lena image, the values of the segmented efficiency (ν) F , F' and Q are 0.4776, 0.4005 and 0.3487 with extraction time 27.72s but when it is performed using

Grayscale Image Segmentation With Quantum-Inspired Multilayer Self-Organizing NN Architecture

MLSONN architecture for threshold parameter θ_ζ , the values of the segmented efficiency (ν) F , F' and Q are 0.8772, 0.7419 and 0.9221 with time 33.94s. It is experimented using QMLSONN architecture on the gray scale Baboon image, for the threshold parameter θ_χ , the values of the segmented efficiency (ν) F , F' and Q for class 6 are 0.4500, 0.4899 and 0.5338 respectively with extraction time 27.13s and another values of the segmented efficiency 0.8596, 0.7710 and 0.9463 with time 29.05s, when using the threshold parameter θ_ζ . The values of the segmented efficiency are 0.4500, 0.4899 and 0.5338 with extraction time 26.58s for QMLSONN architecture and using the MLSONN architecture these values are 0.8596, 0.771 and 0.9462 with time 35.15s.

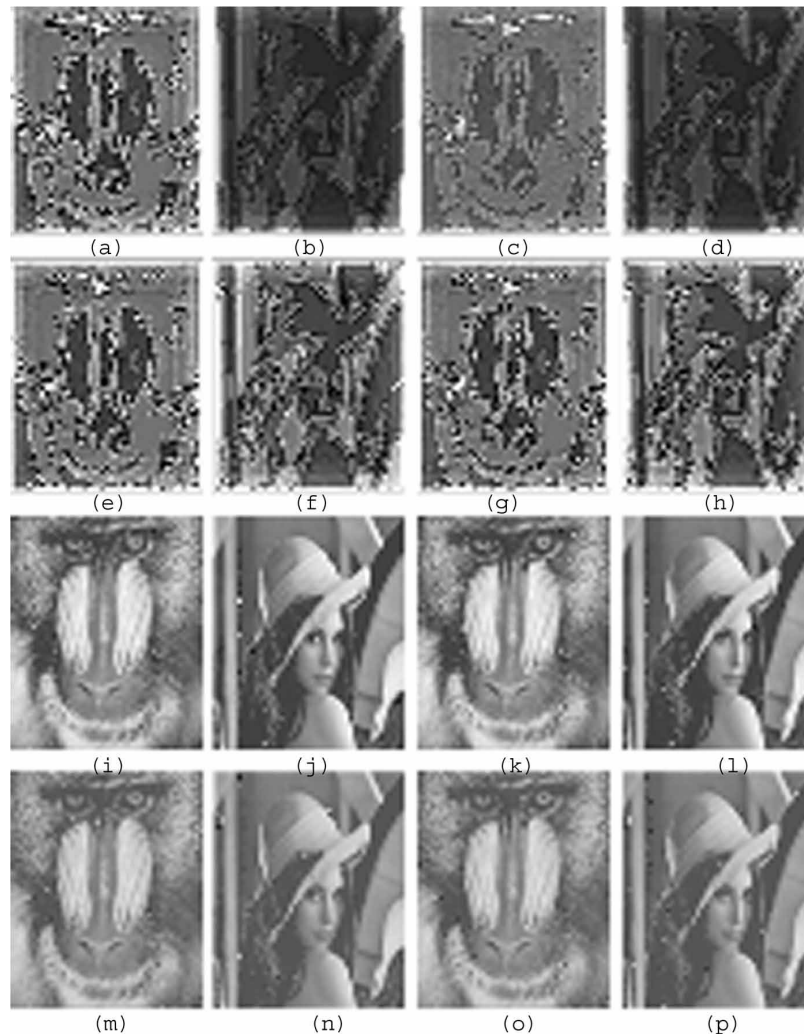
All the outputs are collected and presented for class 6 as shown in the Table 3 for Lena image and in the Table 4 for Baboon image respectively for both using the threshold parameters θ_χ and θ_ζ . The segmented output for class 6 corresponding to threshold parameter θ_χ on gray scale Baboon image and Lena image as shown in Figure 8. Segmented gray scale object outputs are for Baboon images and Lena images (Figure 8 (a, c, e, g, i, k, m, o) and Figure 8 (b, d, f, h, j, l, n, p)) respectively. Figure 8 (a, b, c, d, e, f, g, h) shows extracted segmented object outputs using MLSONN architecture and Figure 8 (i, j, k, l, m, n, o, p) shows the extracted object outputs using QMLSONN architecture. The extracted gray scale object output as shown in Figure 9 for Baboon and Lena images using threshold parameter θ_ζ for class 6. Figure 9 (a, b, c, d, e, f, g, h) shows extracted gray scale object outputs using MLSONN architecture and Figure 9 (i, j, k, l, m, n, o, p) shows extracted gray scale object outputs using QMLSONN architecture.

Figure 5. Gray scale Lena image



(b)

Figure 6. Class 4 segmented output using threshold parameter θ_χ

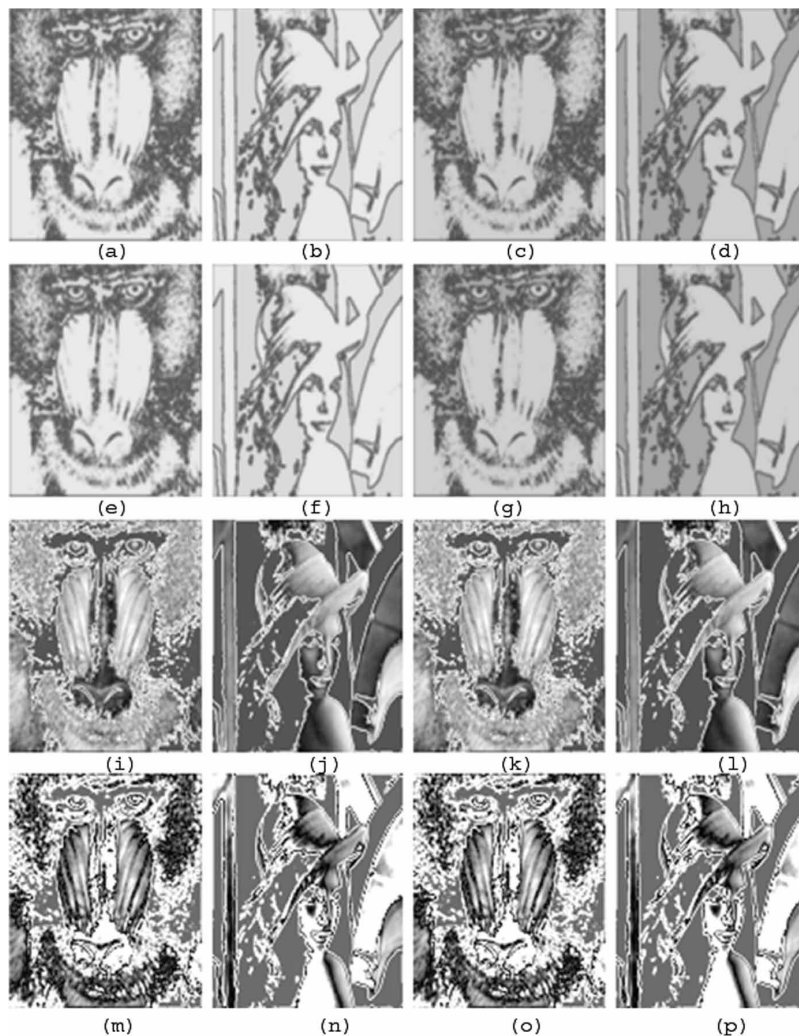


For class 8 using QMLSONN architecture on gray scale Lena image, the segmented efficiency (ν) F , F' and Q are 0.2797, 0.3270 and 0.4143 for threshold parameter θ_χ when the extracted time is 22.49s where as in MLSONN architecture, these are 0.6373, 0.5763 and 0.9534 with corresponding time is 31.38s but in case of threshold parameter θ_ζ , the values of the segmented efficiency for QMLSONN are 0.2810, 0.3272 and 0.4149 when the extracted time is 25.25s and in case of MLSONN architecture, these are 0.6236, 0.5785 and 0.9749 for corresponding time is 31.88s. All the outputs are collected placed as shown in the Table 5 for Lena image and in the Table 6 for Baboon image respectively using the threshold parameters θ_χ and θ_ζ . The segmented gray scale object output for class 8 corresponding to threshold parameter θ_χ for Baboon image and Lena images as shown in Figure 10. The Figure 10 (a, c, e, g, i, k, m, o) shows for Baboon images segmented output and Figure 10 (b, d, f, h, j, l, n, p) shows for Lena images segmented output respectively. Figure 10 (a, b, c, d, e, f, g, h) shows the extracted gray scale object outputs using MLSONN architecture and Figure 10 (i, j, k, l, m, n, o, p) shows the gray scale object outputs using QMLSONN architecture. The gray scale object output as shown in Figure 11

Grayscale Image Segmentation With Quantum-Inspired Multilayer Self-Organizing NN Architecture

for Baboon and Lena images using threshold parameter θ_{ζ} . Figure 11 (a, b, c, d, e, f, g, h) represents the gray scale object outputs using MLSONN architecture and Figure 11 (i, j, k, l, m, n, o, p) represents the gray scale object outputs using QMLSONN architecture for threshold parameter θ_{ζ} . The values of the segmented efficiency F , F' and Q on gray scale Baboon image for class 8 using QMLSONN architecture are 0.288, 0.3942 and 0.4477 with extraction time 24.93s considering the threshold parameter θ_{χ} and using the MLSONN architecture the values of the segmented efficiency are 0.6748, 0.6034 and 0.9731 with extracted time 30.58s. When the threshold parameter θ_{ζ} is considered the gray scale segmented efficiency (ν) F , F' and Q using QMLSONN architecture are 0.2873, 0.3953 and 0.4489 with extraction time 25.00s and in case of MLSONN architecture the corresponding values are 0.6749, 0.6041 and 0.9732 with time 31.22s.

Figure 7. Class 4 segmented output using threshold parameter θ_{ζ}



Grayscale Image Segmentation With Quantum-Inspired Multilayer Self-Organizing NN Architecture

The output corresponding class 8 gray scale Lena and Baboon images using the segmented efficiency (ν) are shown in Table 5 on Lena image and Table 6 on Baboon image respectively.

It is seen that the segmented efficiency using QMLSONN architecture has better response than that of MLSONN architecture.

Table 1. Quality of segmentation (ν) on MLSONN and QMLSONN architectures for Lena image

Quality of Segmentation (ν)			MLSONN Architecture for Lena Image				QMLSONN Architecture for Lena Image			
Class	ν	Set	θ_χ	Time (s)	θ_ξ	Time (s)	θ_χ	Time (s)	θ_ξ	Time (s)
4	F	s_1	0.9002	28.3	0.9002	28.1	0.6297	27.23	0.6291	25.61
		s_2	0.8917	28.01	0.8919	28.3	0.6108	27.11	0.6109	27.15
		s_3	0.8763	28.54	0.8768	28.11	0.5852	26.19	0.5852	25.22
		s_4	0.8558	28.49	0.8551	28.2	0.5770	25.35	0.5770	24.5
	F'	s_1	0.9518	28.3	0.952	28.1	0.7083	27.23	0.7085	25.61
		s_2	0.9400	28.01	0.9400	28.3	0.7117	27.11	0.7115	27.15
		s_3	0.9274	28.54	0.927	28.11	0.6900	26.19	0.69	25.22
		s_4	0.9007	28.49	0.9007	28.2	0.6811	25.35	0.6814	24.5
	Q	s_1	0.9879	28.3	0.9879	28.1	0.7904	27.23	0.7904	25.61
		s_2	0.9700	28.01	0.97	28.3	0.7750	27.11	0.7750	27.15
		s_3	0.9598	28.54	0.95	28.11	0.7578	26.19	0.7578	25.22
		s_4	0.9500	28.49	0.95	28.2	0.7432	25.35	0.7432	24.5

Table 2. Quality of segmentation (ν) on MLSONN and QMLSONN architectures for Baboon image

Quality of Segmentation (ν)			MLSONN Architecture for Baboon Image				QMLSONN Architecture for Baboon Image			
Class	ν	Set	θ_χ	Time (s)	θ_ξ	Time (s)	θ_χ	Time (s)	θ_ξ	Time (s)
4	F	s_1	0.9013	28.01	0.9013	27.91	0.6593	25.10	0.6591	25.00
		s_2	0.8916	28.2	0.8918	27.9	0.6470	27.13	0.6470	27.1
		s_3	0.8796	28.1	0.8796	28.3	0.6220	24.11	0.6217	23.03
		s_4	0.8660	27.89	0.8660	28.1	0.6183	22.75	0.6185	22.58
	F'	s_1	0.9300	28.01	0.9301	27.91	0.7193	25.10	0.7195	25.00
		s_2	0.9310	28.2	0.9311	27.9	0.7008	27.13	0.7008	27.1
		s_3	0.9115	28.1	0.9114	28.3	0.6861	24.11	0.6861	23.03
		s_4	0.9100	27.89	0.91	28.1	0.6658	22.75	0.6658	22.58
	Q	s_1	0.9550	28.01	0.9550	27.91	0.7803	25.10	0.78	25.00
		s_2	0.9489	28.2	0.9489	27.9	0.7794	27.13	0.7794	27.1
		s_3	0.9489	28.1	0.9329	28.3	0.7500	24.11	0.75	23.03
		s_4	0.9223	27.89	0.9223	28.1	0.7413	22.75	0.7413	22.58

Figure 8. Class 6 segmented output using threshold parameter $\theta\chi$



Figure 9. Class 6 segmented output using threshold parameter θ_ζ



Grayscale Image Segmentation With Quantum-Inspired Multilayer Self-Organizing NN Architecture

Table 3. Quality of segmentation (ν) on MLSONN and QMLSONN architectures for Lena image

Quality of Segmentation (ν)			MLSONN Architecture for Lena Image				QMLSONN Architecture for Lena Image			
Class	ν	Set	θ_χ	Time (s)	θ_ξ	Time (s)	θ_χ	Time (s)	θ_ξ	Time (s)
6	F	s_1	0.8856	28.9	0.8861	33.15	0.5611	25.21	0.5611	27.69
		s_2	0.9059	29.01	0.8973	43.15	0.5300	25.12	0.5301	27.54
		s_3	0.8806	28.84	0.8806	34.34	0.4800	25.14	0.4801	27.87
		s_4	0.8773	28.89	0.8772	33.94	0.4781	25.2	0.4776	27.72
	F'	s_1	0.7973	28.9	0.7978	33.15	0.4718	25.21	0.4718	27.69
		s_2	0.7891	29.01	0.7892	43.15	0.4511	25.12	0.4512	27.54
		s_3	0.7624	28.84	0.762	34.34	0.4297	25.14	0.429	27.87
		s_4	0.7411	28.89	0.7419	33.94	0.4005	25.2	0.4005	27.72
	Q	s_1	0.9621	28.9	0.963	33.15	0.3996	25.21	0.3996	27.69
		s_2	0.9590	29.01	0.959	43.15	0.3817	25.12	0.3822	27.54
		s_3	0.9341	28.84	0.9341	34.34	0.3486	25.14	0.3487	27.87
		s_4	0.9221	28.89	0.9221	33.94	0.3571	25.2	0.3571	27.72

Table 4. Quality of segmentation (ν) on MLSONN and QMLSONN architectures for Baboon image

Quality of Segmentation (ν)			MLSONN Architecture for Baboon Image				QMLSONN Architecture for Baboon Image			
Class	ν	Set	θ_χ	Time (s)	θ_ξ	Time (s)	θ_χ	Time (s)	θ_ξ	Time (s)
6	F	s_1	0.8997	29.13	0.8999	35.14	0.5598	27.2	0.561	26.51
		s_2	0.8895	29.11	0.8895	35.20	0.5218	27.15	0.522	26.55
		s_3	0.8659	29.07	0.8658	35.15	0.4595	27.12	0.4595	26.56
		s_4	0.8596	29.05	0.8596	35.15	0.4500	27.13	0.4500	26.58
	F'	s_1	0.7812	29.13	0.792	35.14	0.5794	27.2	0.5794	26.51
		s_2	0.7899	29.11	0.7889	35.20	0.5423	27.15	0.5423	26.55
		s_3	0.7798	29.07	0.7797	35.15	0.4978	27.12	0.4976	26.56
		s_4	0.7710	29.05	0.771	35.15	0.4899	27.13	0.4899	26.58
	Q	s_1	0.9811	29.13	0.9816	35.14	0.5998	27.2	0.5998	26.51
		s_2	0.9695	29.11	0.969	35.20	0.5724	27.15	0.5724	26.55
		s_3	0.9518	29.07	0.9519	35.15	0.5477	27.12	0.5476	26.56
		s_4	0.9463	29.05	0.9462	35.15	0.5338	27.13	0.5338	26.58

Figure 10. Class 8 segmented output using threshold parameter $\theta\chi$



Figure 11. Class 8 segmented output using threshold parameter θ_c



Grayscale Image Segmentation With Quantum-Inspired Multilayer Self-Organizing NN Architecture

Table 5. Quality of segmentation (ν) on MLSONN and QMLSONN architectures for Lena image

Quality of Segmentation (ν)			MLSONN Architecture for Lena Image				QMLSONN Architecture for Lena Image			
Class	ν	Set	θ_χ	Time (s)	θ_ξ	Time (s)	θ_χ	Time (s)	θ_ξ	Time (s)
8	F	s_1	0.7214	31.28	0.7276	31.21	0.3233	23.10	0.3317	24.19
		s_2	0.6891	30.58	0.6871	31.10	0.3073	23.52	0.3067	24.20
		s_3	0.6685	30.37	0.6598	31.70	0.2957	24.01	0.2961	25.18
		s_4	0.6373	31.38	0.6236	31.88	0.2797	22.49	0.2810	25.25
	F'	s_1	0.7279	31.28	0.7276	31.21	0.3891	23.10	0.3874	24.19
		s_2	0.5954	30.58	0.5789	31.10	0.3711	23.52	0.3699	24.20
		s_3	0.5763	30.37	0.587	31.70	0.3533	24.01	0.3521	25.18
		s_4	0.5806	31.38	0.5785	31.88	0.3270	22.49	0.3272	25.25
	Q	s_1	0.9534	31.28	0.9762	31.21	0.4695	23.10	0.4598	24.19
		s_2	0.9609	30.58	0.9749	31.10	0.4518	23.52	0.4635	24.20
		s_3	0.9582	30.37	0.9771	31.70	0.4394	24.01	0.4518	25.18
		s_4	0.9594	31.38	0.9768	31.88	0.4143	22.49	0.4149	25.25

Table 6. Quality of segmentation (ν) on MLSONN and QMLSONN architectures for Baboon image

Quality of Segmentation (ν)			MLSONN Architecture for Baboon Image				QMLSONN Architecture for Baboon Image			
Class	ν	Set	θ_χ	Time (s)	θ_ξ	Time (s)	θ_χ	Time (s)	θ_ξ	Time (s)
8	F	s_1	0.7351	30.21	0.7356	30.95	0.3308	24.11	0.3425	24.25
		s_2	0.6956	30.31	0.6943	31.02	0.3191	24.56	0.3188	24.56
		s_3	0.6804	30.22	0.6812	31.16	0.3039	25.42	0.3035	25.50
		s_4	0.6748	30.58	0.6749	31.22	0.288	24.93	0.2873	25.00
	F'	s_1	0.7197	30.21	0.7197	30.95	0.4742	24.11	0.4753	24.25
		s_2	0.6388	30.31	0.6387	31.02	0.4593	24.56	0.4598	24.56
		s_3	0.6297	30.22	0.6295	31.16	0.4435	25.42	0.4439	25.50
		s_4	0.6034	30.58	0.6041	31.22	0.3942	24.93	0.3953	25.00
	Q	s_1	0.9910	30.21	0.9911	30.95	0.4995	24.11	0.4987	24.25
		s_2	0.9858	30.31	0.9848	31.02	0.4892	24.56	0.4891	24.56
		s_3	0.9795	30.22	0.9794	31.16	0.4760	25.42	0.4761	25.50
		s_4	0.9731	30.58	0.9732	31.22	0.4477	24.93	0.4489	25.00

CONCLUSION AND REMARKS

In this chapter, a scheme for gray scale image segmentation using QMLSONN architecture is presented. Segmented efficiency and elapsed time are measured for three classes of Lena image and Baboon image using a context sensitive threshold value applied on the MUSIG activation function. A comparison is taken out between the classical technique MLSONN as well as the quantum computation technique QMLSONN. It is observed that the performance of QMLSONN architecture is better regarding time complexity and extraction efficiency with respect to the MLSONN architecture.

*This research was previously published in *Quantum-Inspired Intelligent Systems for Multimedia Data Analysis*; pages 141-177, copyright year 2018 by Engineering Science Reference (an imprint of IGI Global).*

REFERENCES

- Aytekin, C., Kiranyaz, S., & Gabbouj, M. (2013). Quantum Mechanics in Computer Vision: Automatic Object Extraction. *Proc. ICIP 2013*, 2489–2493. *10.1109/ICIP.2013.6738513*
- Bhattacharyya, S., & Dutta, P. (Eds.). (2013). *Handbook of Research on Computational Intelligence for Engineering, Science, and Business* (vol. 1). IGI Global.
- Bhattacharyya, S., Dutta, P., Maulik, U., & Nandi, P. K. (2007). Multilevel Activations For True Color Image Segmentation Using a Self Supervised Parallel Self Organizing Neural Network (PSOINN) Architecture: A Comparative Study. *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, 1(8).
- Bhattacharyya, S., Maulik, U., & Dutta, P. (2010). Multilevel Image Segmentation with Adaptive Image Context Based Thresholding. *Applied Soft Computing*, 11(1), 946–962. doi:10.1016/j.asoc.2010.01.015
- Bhattacharyya, S., Pal, P., & Bhowmick, S. (2014). Binary Image Denoising Using a Quantum Multilayer Self Organizing Neural Network. *Applied Soft Computing*, 24, 717–729. doi:10.1016/j.asoc.2014.08.027
- Blumenstein, M., & Verma, B. (1998). An artificial neural network based segmentation algorithm for off-line handwriting recognition. *Proceedings of the Second International Conference on Computational Intelligence and Multimedia Applications*.
- Bora, D. J., & Gupta, A. K. (2014). A Novel Approach Towards Clustering Based Image Segmentation. *International Journal of Emerging Science and Engineering*, 2(11).
- Bora, D. J., & Gupta, A.K. (2014). A Comparative study Between Fuzzy Clustering Algorithm and Hard Clustering Algorithm. *International Journal of Computer Trends and Technology*, 10(2), 108-113.
- Borsotti, M., Campadelli, P., & Schettini, R. (1998). Quantitative evaluation of color image segmentation results. *Pattern Recognition Letters*, 19(8), 741–747. doi:10.1016/S0167-8655(98)00052-X

- Das, D., & Mukhopadhyay, S. (2015). *A Pixel Based Segmentation Scheme for Fingerprint Images; Information Systems Design and Intelligent Applications. In Advances in Intelligent Systems and Computing* (Vol. 340, pp. 439–448). New Delhi: Springer; doi:10.1007/978-81-322-2247-7_45
- De, S., & Bhattacharyya, S. (2015). Color Magnetic Resonance Brain Image Segmentation by ParaOptiMUSIG Activation Function: An Application. *Hybrid Soft Computing Approaches*, 611, 185-214.
- De, S., Bhattacharyya, S., & Chakraborty, S. (2012). Color image segmentation using parallel OptiMUSIG activation function. *Applied Soft Computing*, 12(10), 3228–3236. doi:10.1016/j.asoc.2012.05.011
- De, S., Bhattacharyya, S., Chakraborty, S., Sarkar, B. N., Prabhakar, P. K., & Bose, S. (2012). Gray Scale Image Segmentation by NSGA-II Based OptiMUSIG Activation Function. *CSNT '12 Proceedings of the 2012 International Conference on Communication Systems and Network Technologies*, 104-108.
- De, S., Bhattacharyya, S., & Dutta, P. (2010). Efficient grey-level image segmentation using an optimized MUSIG (OptiMUSIG) activation function. *International Journal of Parallel, Emergent and Distributed Systems*, 26(1), 1–39.
- Ghosh, A., Pal, N. R., & Pal, S. K. (1993). Self organization for object extraction using a multilayer neural network and fuzziness measures. *IEEE Transactions on Fuzzy Systems*, 1(1), 54–68.
- Kang, S.D., Park, S.S., Shin, Y.G., Yoo, H.W., & Jang, D.S. (2008). Image Segmentation using Statistical approach via Perception-based Color Information. *International Journal of Computer Science and Network Security*, 8(4).
- Kapur, J. N., Sahoo, P., & Wong, A. K. C. (1980). A new method for gray-level picture thresholding using the entropy of the histogram. *Computer Vision Graphics and Image Processing*, 29(3), 273–285.
- Liu, J., & Yang, Y. H. (1994). Multi-resolution color image segmentation. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 16(7), 689–700. doi:10.1109/34.297949
- Mashford, J., Davis, P., & Rahilly, M. (2007). Pixel-Based Color Image Segmentation Using Support Vector Machine for Automatic Pipe Inspection. *Australasian Joint Conference on Artificial Intelligence: AI 2007: Advances in Artificial Intelligence*, 739-743.
- Mishra, D., Bose, I., De, U. C., & Pradhan, B. (2014). A Multilevel Image Thresholding Using Particle Swarm Optimization. *International Journal of Engineering and Technology*, 6(2), 1204-1211.
- Pal, N. R., & Pal, S. K. (1993). A Review on Image Segmentation Techniques. *Pattern Recognition*, 26(9), 1277–1294. doi:10.1016/0031-3203(93)90135-J
- Pantofaru, C., & Hebert, M. (2005). *A Comparison of Image Segmentation Algorithms, CMU-RI-TR-05-40, September 1, 2005*. Pittsburgh, PA: The Robotics Institute, Carnegie Mellon University.
- Ross, T.J., & Ross, T. (1995). *Fuzzy Logic with Engineering Applications*. McGraw Hill College Div.
- Saini, S., & Arora, K. (2014). A Study Analysis on the Different Image Segmentation Techniques. *International Journal of Information & Computation Technology*, 4(14), 1445-1452.
- Salman, N. (2006, April). Image Segmentation Based on Watershed and Edge Detection Techniques. *The International Arab Journal of Information Technology*, 3(2).

Grayscale Image Segmentation With Quantum-Inspired Multilayer Self-Organizing NN Architecture

Sharma, V. C. (2015). A Review: PDE based Segmentation Method and Color Models. *SSRG International Journal of Computer Science and Engineering*. Retrieved from www.internationaljournalsrg.org

Suetens P., Verbeeck R., Delaere D., Nuyts J., & Bijnens B. (1991). Model-Based Image Segmentation: Methods and Applications. *AIME*, 91, 3-24. DOI: . doi:10.1007/978-3-642-48650-0_1

Yogamangalam, R., & Karthikeyan, B. (2013). Segmentation Techniques Comparison in Image Processing. *International Journal of Engineering and Technology*, 5.

Zadeh, L. A. (1965). Fuzzy sets. *Information and Control*, 8(3), 338–353. doi:10.1016/S0019-9958(65)90241-X

Chapter 9

DNA Fragment Assembly Using Quantum-Inspired Genetic Algorithm

Manisha Rathee

Jawaharlal Nehru University, India

Kumar Dilip

Jawaharlal Nehru University, India

Ritu Rathee

Indira Gandhi Delhi Technical University for Women, India

ABSTRACT

DNA fragment assembly (DFA) is one of the most important and challenging problems in computational biology. DFA problem involves reconstruction of target DNA from several hundred (or thousands) of sequenced fragments by identifying the proper orientation and order of fragments. DFA problem is proved to be a NP-Hard combinatorial optimization problem. Metaheuristic techniques have the capability to handle large search spaces and therefore are well suited to deal with such problems. In this chapter, quantum-inspired genetic algorithm-based DNA fragment assembly (QGFA) approach has been proposed to perform the de novo assembly of DNA fragments using overlap-layout-consensus approach. To assess the efficacy of QGFA, it has been compared genetic algorithm, particle swarm optimization, and ant colony optimization-based metaheuristic approaches for solving DFA problem. Experimental results show that QGFA performs comparatively better (in terms of overlap score obtained and number of contigs produced) than other approaches considered herein.

DOI: 10.4018/978-1-7998-8593-1.ch009

1. INTRODUCTION

Understanding the functioning (as well as malfunctioning) of living beings require determination and interpretation of their genome sequences (Kikuchi & Chakraborty, 2006). The genome of an organism is made up of deoxyribonucleic acid (DNA) strands which encode its hereditary information and determine its body structure, functions and protein formation (Watson & Berry, 2003). DNA strands consist of two types of nitrogenous bases namely purines (adenine (A) and guanine (G)) and pyrimidines (cytosine (C) and thymine (T)). DNA has a double helical structure consisting of two strands running anti-parallel to each other and having complementary bases where a purine on one strand is paired with pyrimidine on the other and vice-versa in such a way that A is always paired with T and G is always paired with C (Watson & Berry, 2003; Watson & Crick, 1953). The process of determining the complete sequence of bases in all the strands of DNA (i.e. the genome) is termed as DNA sequencing. The genome sequences are generally very large ranging from few thousand base pairs for small viruses to 3×10^9 base pairs for humans, 1.7×10^{10} base pairs for wheat and 1.2×10^{11} base pairs for lily (Kikuchi & Chakraborty, 2006). A number of techniques are available for sequencing but none of the available techniques is capable of reading more than 1000 bases at a time, let alone reading an entire genome at once. This limitation of DNA sequencing methods is overcome by shotgun sequencing where the target DNA is replicated to generate multiple copies which are then randomly broken into a number of smaller fragments so that the fragments are short enough to be sequenced by any of the available sequencing techniques (Dorransoro, *et al.*, 2008). After sequencing, the sequenced fragments need to be combined back to obtain the original sequence as the whole genome sequence is required for phylogenetic and genomic research activities. But, as the fragments were generated randomly, the information about ordering of the fragments on the parent strand or the strand to which a particular fragment belongs is lost thereby resulting in the DNA fragment assembly problem (Meksangsouy & Chaiyaratana, 2003). DFA problem involves reconstruction of target DNA from several hundred (or thousands) of sequenced fragments by identifying the proper orientation and order of the sequenced fragments (Meksangsouy & Chaiyaratana, 2003). The sequenced fragments are called as reads and are provided as input to the assembly procedure.

DFA is proved to a NP-Hard combinatorial optimization problem (Medvedev, *et al.*, 2007). The complexity arises due to a very large search space as there are $2^k \times k!$ possible solutions in worst case for a set containing k fragments (Kubalik, *et al.*, 2010). Therefore obtaining exact solutions using traditional optimization techniques is not possible. Metaheuristic techniques have the capability to handle large search spaces and therefore well suited to solve the hard optimization problems. In this chapter, Quantum inspired genetic algorithm (QIGA) has been adapted for performing the de novo assembly of DNA fragments using overlap-layout-consensus approach. QIGA is a relatively recent metaheuristic technique which blends the principals of quantum computing with the concepts of genetic algorithm (Han & Kim, 2002). Due to the parallel processing capabilities of QIGA, it is capable of providing better solutions (in terms of diversity, quality and convergence) with a smaller population size. Also, QIGA has an edge over other metaheuristic techniques as very less number of parameters needs to be adjusted in case of QIGA.

Quantum inspired Genetic algorithm-based DNA Fragment Assembly (QGFA) has been proposed in this paper with the objective of maximizing the sum of overlaps between adjacent fragments in a layout. The main contribution of the proposed work is mentioned below:

- QIGA has been adapted for solving the DFA problem. To the best of our knowledge, none of the works existing in literature has used QIGA for solving the DFA problem.

- An improvement has been proposed in measuring operator so that only feasible solutions are generated and solution repairing is not required.
- A novel method has been proposed for computing the change in angle of rotation which is required for updating the Q-bit population in QIGA.
- Comprehensive comparison of proposed QGFA algorithm with genetic algorithm (GA), particle swarm optimization (PSO) and Ant Colony Optimization (ACO), Cuckoo Search (CS) based metaheuristic approaches for solving DFA. The experimental results show that proposed QGFA algorithm performs comparatively better in terms of overlap score and number of contigs.

The organization of the rest of the paper is as follows. DFA problem is discussed in detail and problem formulation is given in section 2. Related work is discussed in section 3. Proposed approach is presented in section 4. Experimental results are shown and discussed in section 5. Conclusion is presented in section 6.

2. DFA PROBLEM

Before proceeding into the particulars of the DFA problem, given below is the nomenclature needed for understanding the problem (Firoz, *et al.*, 2012):

1. **Fragment:** A short segment of DNA sequence of length 500-800 bps.
2. **Read:** A sequenced fragment.
3. **Prefix:** A substring consisting of first n characters of a read.
4. **Suffix:** A substring consisting of last n characters of a read.
5. **Overlap Score:** The number of matching bases between suffix of one read and prefix of another.
6. **Layout:** The order of fragments in which they must be joined to get the target sequence.
7. **Contig:** A sequence comprising contiguous overlapping fragments.
8. **Consensus:** The final sequence obtained by majority voting in each column of the layout.

As discussed previously, fragment assembly is a critical step in de novo sequencing of the genomes. DFA is concerned with determining the order and orientation of randomly generated fragments in order to construct the original DNA sequence. DFA is therefore similar to solving a large jigsaw puzzle which assembles the sequenced fragments for creating the original DNA sequence. DFA depends on the length of the sequenced fragments and the availability of the reference genome. On the basis of fragment length, DFA is categorized as Long read assembly (Chevreux, 2005; Huang, *et al.*, 2003; Huang & Madan, 1999; Sutton, *et al.*, 1995; <http://www.phrap.org/phredphrap/phrap.html>) and Short read assembly (Chaisson, *et al.*, 2004; Hernandez, *et al.*, 2008; Jeck, *et al.*, 2007; Simpson, *et al.*, 2009; Zerbino & Birney, 2008). On the basis of availability of reference genome, genome assembly is categorized as Comparative assembly (Pop, 2009; Phillippy, *et al.*, 2004) and De-novo assembly (Pop, 2009). Both long and short reads can be assembled by comparative as well as de-novo assembly. In this chapter, de-novo assembly is performed on long reads using Overlap-Layout-Consensus (OLC) approach which is well suited for longer reads. OLC approach views DFA problem as a Hamiltonian path problem in an undirected graph where reads are treated as vertices and edges exist between overlapping reads. The aim here is to combine the reads into contigs by finding a path that traverses each node exactly once.

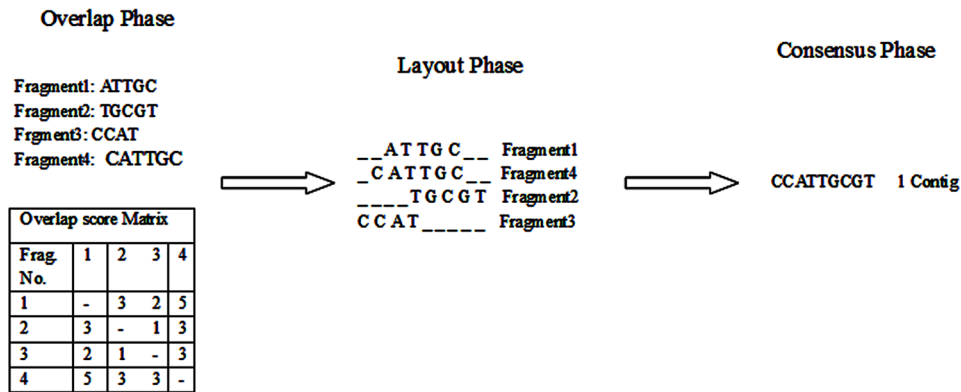
DNA Fragment Assembly Using Quantum-Inspired Genetic Algorithm

OLC approach consists of three phases as shown in Figure 1 and briefly discussed below:

Overlap Phase

In this phase, all-against-all, pair-wise comparison between the reads is carried out for computing the amount of overlap. It is assumed that higher the overlap score between reads, more are the chances that fragments originated from the same region of DNA and therefore need to be adjacent in the layout (Dorrnsoro, *et al.*, 2008).

Figure 1. Overlap layout consensus approach



Layout Phase

Based on the overlap score, this phase decides the order of fragments. This is the most complex part as it is difficult to decide the true overlap between the reads due to incomplete coverage, unknown orientation of fragments, base call errors and repeated regions (Dorrnsoro, *et al.*, 2008).

Consensus Phase

This is the final phase where consensus is generated by using majority vote for determining the base to be put in each column of layout (Dorrnsoro, *et al.*, 2008). The quality of consensus is decided by evaluating the distribution of the coverage. For any base location, coverage is defined as the number of fragments covering that location. Coverage measures the redundancy in the sequenced data. It computes the average number of fragments containing a given nucleotide and is defined as the total number of bases in the reads over the total length of the target DNA sequence (Setubal & Meidanis, 1997):

$$Coverage = \frac{\sum_{i=1}^N \text{length of fragment}_i}{\text{target sequence length}} \quad (1)$$

where N denotes the number of fragments. Higher coverage value leads to fewer gaps in the target sequence thereby resulting in a better solution. In order to reconstruct the original genome, coverage of $6\times$ to $10\times$ is required (Li, *et al.*, 1997).

2.1 Problem Formulation

Given a set of sequenced fragments \mathcal{F} consisting of N fragments $\mathcal{F} = \{f_1, f_2, f_3, \dots, f_N\}$, let the length of f_i be represented by ℓ_i overlap score between f_i and f_j be denoted by $\mathcal{W}_{i,j}$. Then DFA problem is an asymmetric optimization problem where $\mathcal{W}_{i,j}$ may not be same as $\mathcal{W}_{j,i}$. The aim is to reconstruct the original sequence in such a way that total overlap among the adjacent fragments is maximized.

The DFA is formulated as an optimization problem as follows (Parsons *et al.*, 1995):

$$\text{MAXIMIZE}(F) \tag{2}$$

where

$$F = \sum_{i=1}^{N-1} \mathcal{W}_{i,j} \text{ such that } j=i+1 \tag{3}$$

$$\mathcal{W}_{i,j} = g(f_i, f_j), \mathcal{W}_{i,j} \geq 0 \text{ and } \mathcal{W}_{i,j} \leq \min(\ell_i, \ell_j) \tag{4}$$

F is the sum of overlap scores between adjacent fragments in a layout. The overlap score between fragments is a function of fragments themselves. The value of $\mathcal{W}_{i,j}$ ranges from 0 to $\min(\ell_i, \ell_j)$. If $\mathcal{W}_{i,j} = \min(\ell_i, \ell_j)$, then one of the fragments is contained in the other fragment. The overlap score between fragments is calculated using a semi-global alignment algorithm presented in (Coull & Szymanski, 2008).

3. RELATED WORK

A large number of techniques including deterministic, stochastic and meta-heuristic have been proposed in literature to address the DFA problem. A qualitative review on DFA problem is presented by broadly categorizing the theme into non-metaheuristic and metaheuristic based approaches.

3.1 Non-Metaheuristic Approaches for DFA Problem

DFA was first introduced in (Staden, 1980; Huang, 1992) and was solved using a deterministic greedy search technique. Huang (1992) computed the overlap score using a local alignment algorithm proposed in (Smith & Waterman, 1981) and used a filtering technique presented in (Chang & Lawler, 1990) for discarding the fragments having overlap score below a given threshold. A deterministic branch-and-cut algorithm has been proposed in (Ferreira *et al.*, 2002) and a deterministic overlap graph based algorithm

has been presented in (Braga & Meidanis, 2002) for solving the DFA problem. In (Churchil *et al.*, 1993; Burks *et al.* 1994), simulated annealing algorithm, a stochastic search technique has been applied for addressing the DFA problem. Angeleri *et al.* (1999) have applied neural prediction technique for addressing the DFA problem. Bocicor *et al.* (2011) have used reinforcement learning approach for dealing with the DFA problem. Fullerton *et al.* (2015) have addressed the DFA problem using modified classical graph algorithms.

3.2 Metaheuristic Approaches for DFA Problem

As discussed earlier, metaheuristic techniques are well suited for solving hard combinatorial optimization problems. A large body of literature exists where metaheuristic techniques have been used for solving the DFA problem. The first approach based on metaheuristic was presented by Parsons *et al.* (1993, 1995) where GA has been used for solving the DFA problem. Already formed contigs have been preserved or extended by using edge recombination, order crossover, transposition and inversion operators. Kikuchi & Chakraborty (2006) have improved the GA by proposing two heuristics namely chromosome reduction (CRed) for improving the efficiency of search procedure and chromosome refinement (CRef) for improving the fitness locally. ISA, a simulated annealing based meta-heuristic has been proposed in (Alba, *et al.*, 2009) where inversion procedure is applied generating the neighbor solutions. A problem aware local search (PALS) algorithm has been presented in (Alba & Luque, 2007) where a number of contigs has been considered as the primary measure while overlap score has been taken as secondary measure for evaluating the quality of solutions. Determination of overlap score and number of contigs is computationally inexpensive as in each generation only the change in values is estimated. In (Alba, *et al.*, 2008), GA is presented where greedy strategy has been used for initializing 50% of starting population and order crossover and swap mutations are used for evolving the population. In (Alba & Dorronsoro, 2008), PALS has been used in conjunction with a cellular genetic algorithm (cGA) to reap the benefits of both cGA and PALS. Prototype optimization with evolved improvement steps, POEMS, is an iterative method presented in (Kubalik *et al.* 2010) where evolutionary strategy is applied for searching the best modification for current solution (called prototype). An ant colony based approach employing asymmetric ordering representation has been proposed by Meksangsouy & Chaiyaratana (2003) for addressing the DFA problem. Firoz *et al.* (2012) have considered both noisy and noiseless instances of the problem and proposed Queen Bee evaluation based on genetic algorithm (QEGA) and Artificial Bee Colony (ABC) algorithm for the same. Rathee & Kumar (2014) has formulated DFA as a bi-objective and tri-objective optimization problem and has solved it using a multi-objective GA namely NSGA-II. Huang *et al.* (2015) have proposed a memetic particle swarm optimization algorithm for addressing the DNA fragment assembly problem. Huang *et al.* (2016) have proposed a memetic gravitational search algorithm for solving the DFA problem where tabu search has been used for population initialization, two operators have been proposed for increasing the diversity of population and simulated annealing based variable neighborhood search is applied for finding better solutions. Kchouk & Elloumi (2016) have proposed a clustering approach for performing de-novo assembly on next generation sequencing data.

4. PROPOSED APPROACH

As discussed earlier, DFA problem is proved to be NP-Hard combinatorial optimization problem and therefore exact solutions are not possible to find within a reasonable amount of computational time. Recently, metaheuristic techniques have been shown performing better than their traditional counterparts for such problems. Due to their capability to handle large search spaces, metaheuristic techniques have been used by many researchers for solving hard optimization problems in diverse domains. In this chapter, Quantum inspired Genetic algorithm (QIGA) has been adapted for solving the DNA Fragment Assembly problem (QGFA) with the objective of maximizing the sum of overlap between adjacent fragments.

4.1 Overview of QIGA

Quantum inspired algorithms have recently been developed as a new class of artificial intelligence techniques. QIGA was proposed by Narayanan & Moore (1996) for the first time but first practical implementation and application of QIGA was discussed by Han & Kim (2002). QIGA combines the features of quantum computing with that of evolutionary computation in order to devise better solutions to the optimization problems. Quantum computing principles such as Q-bit, superposition and entanglement are blended with GA methodology of having an initial population, evaluating the fitness of population, performing crossover and mutation in order to evolve the population towards better regions of search space. This combined approach imparts QIGA the capability of global searching with a small population and faster convergence. QIGA and its variants have been applied in diverse domains for addressing a large class of combinatorial optimization problems (Zhang, 2011). QIGA variants can be broadly categorized as: real observation QIGA for numerical optimization (Zhang & Rong, 2007) and binary observation QIGA (bQIGA) for combinatorial optimization (Han & Kim, 2002). Since the DFA problem addressed in this chapter is a combinatorial optimization problem, bQIGA has been used in chapter.

In QIGA, chromosome is called as Q-bit chromosome and consequently the population is called as Q-bit population as Q-bits are used to represent genes in a chromosome instead of using binary, real or alphabetic representation for genes as done in the case of GA. Q-bits are smallest unit of information in quantum systems which can represent a 0 or 1 or any linear superposition of the two (Nielsen & Chuang, 2000). A pair of complex numbers (α, β) is used to denote a Q-bit as shown below

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (5)$$

Such that

$$|\alpha|^2 + |\beta|^2 = 1 \quad (6)$$

where $|\alpha|^2$ and $|\beta|^2$ are the probabilities that, when observed, Q-bit will lead to a 0 and 1 respectively. A string of Q-bits make a Q-bit chromosome. The observation of a Q-bit chromosome results in a classical chromosome which is basically the solution representation used by conventional GA. The fitness of classical chromosomes is computed using a fitness function. Based on the fitness value of classical population, the q-bit population is moved in the direction of the best solution by applying Q-gates as

DNA Fragment Assembly Using Quantum-Inspired Genetic Algorithm

variation operators. The most commonly used Q-gate operator in literature is Rotation gate operator which is defined as given below

$$U(\Delta\Phi_i) = \begin{pmatrix} \text{Cos}(\Delta\Phi_i) & -\text{Sin}(\Delta\Phi_i) \\ \text{Sin}(\Delta\Phi_i) & \text{Cos}(\Delta\Phi_i) \end{pmatrix} \quad (7)$$

where $\Delta\Phi_i$ denotes the change in angle of rotation of i^{th} Q-bit. Based on the sign of Φ , each Q-bit moves towards either 0 or 1. A generic quantum inspired algorithm is shown in Table 1 (Han & Kim, 2002).

Table 1. Generic quantum inspired algorithm

Algorithm 1: Generic Quantum Inspired Algorithm
Begin Initialize the Q-bit solutions While (not termination condition) Measure the Q-bit solutions. Evaluate Fitness Update Q-bit population using Q-gate operator. End End

4.2 QGFA

The proposed QGFA algorithm is discussed in this section. QGFA is a population based metaheuristic for solving DFA problem. Like any other evolutionary approach, QGFA also comprises of encoding the chromosomes (i.e. solution representation), evaluating the fitness of chromosomes and evolving the population towards better regions of search space.

4.2.1 Solution Representation

Solution representation is the first step in the process of optimization using metaheuristic techniques. In QIGA, Q-bits are used for representing the genes in a chromosome. The DFA problem addressed in this paper is a permutation combinatorial optimization problem where ordering and orientation of fragments in a layout needs to be determined. For a DFA problem having N fragments, each fragment is identified using an integer from 1 to N . A Q-bit solution for DFA problem is denoted by q and is encoded as shown in equation (8)

$$q = \begin{pmatrix} q(1,1) & q(1,2) & \dots\dots & q(1,N) \\ q(2,1) & q(2,2) & \dots\dots & q(2,N) \\ \vdots & \vdots & \dots & \vdots \\ q(N,1) & q(N,2) & \dots\dots & q(N,N) \end{pmatrix} \quad (8)$$

4.2.2 Population Initialization

Let the size of population be m . Then Q-bit population in j^{th} generation, $Q(j)$, is represented as:

$$Q_j = \{q_1^j, q_2^j, q_3^j, \dots, q_m^j\} \quad (9)$$

where

$$q_i^j = \begin{pmatrix} q_i^j(1,1) & q_i^j(1,2) & \dots & q_i^j(1,N) \\ q_i^j(2,1) & q_i^j(2,2) & \dots & q_i^j(2,N) \\ \vdots & \vdots & \dots & \vdots \\ q_i^j(N,1) & q_i^j(N,2) & \dots & q_i^j(N,N) \end{pmatrix} \text{ for } i=1,2,3,\dots,m \quad (10)$$

and

$$q_i^j(x,y) = \begin{bmatrix} \alpha_i^j(x,y) \\ \beta_i^j(x,y) \end{bmatrix} \text{ for } x, y = 1, 2, 3, \dots, N \quad (11)$$

$$|\alpha_i^j(x,y)|^2 + |\beta_i^j(x,y)|^2 = 1 \quad (12)$$

At the start of algorithm, $j = 0$ and therefore the initial population denoted by $Q(0)$ is given as

$$Q(0) = \{q_1^0, q_2^0, q_3^0, \dots, q_m^0\} \quad (13)$$

Such that

$$q_i^0(x,y) = \begin{bmatrix} \alpha_i^0(x,y) \\ \beta_i^0(x,y) \end{bmatrix} \text{ for } x, y = 1, 2, 3, \dots, N \quad (14)$$

$$\alpha_i^0(x,y) = \beta_i^0(x,y) = \sqrt{\frac{1}{2}} \text{ for } x, y = 1, 2, 3, \dots, N \text{ and } i = 1, 2, 3, \dots, m \quad (15)$$

Initially, every Q-bit in a chromosome is assigned a value of $\sqrt{\frac{1}{2}}$ so that all the fragments have equal chances of being placed at any position in a fragment layout.

4.2.3 Quantum Measurement

Q-bit chromosomes in the Q-bit population are measured or observed in order to generate a population of classical chromosomes as fitness evaluation can be performed only on classical chromosomes. The classical chromosome in QGFA is a binary matrix of size $N \times N$ where N is the number of DNA fragments. The binary population in j^{th} generation is represented by $B(j)$ as shown in equation (16).

$$B(j) = (b_1^j, b_2^j, \dots, b_m^j) \tag{16}$$

where

$$b_i^j = \begin{bmatrix} b_i^j(1,1) & b_i^j(1,2) \cdots & b_i^j(1,N) \\ b_i^j(2,1) & b_i^j(2,2) \cdots & b_i^j(2,N) \\ \vdots & \vdots & \vdots \\ b_i^j(N,1) & b_i^j(N,2) \cdots & b_i^j(N,N) \end{bmatrix} \text{ for } i = 1, 2, \dots, m \tag{17}$$

Such that

$$\forall x \forall y b_i^j(x, y) = 0 | 1 \tag{18}$$

$$\forall x \forall y \text{ if } x = y, b_i^j(x, y) = 0 \tag{19}$$

$$\forall x \sum_{y=1}^N b_i^j(x, y) = 1, \forall y \sum_{x=1}^N b_i^j(x, y) = 1 \tag{20}$$

$$\sum_{x=1}^N \sum_{y=1}^N b_i^j(x, y) = N \tag{21}$$

where $b_i^j(x, y) = 1$ is interpreted as, in i^{th} solution of j^{th} generation, fragment y is at x^{th} position in the fragment layout. Since the classical solution is in binary matrix form and DFA problem is a permutation problem, for evaluating fitness, the binary solutions need to be converted into numeric solutions. The measurement of Q-bit chromosome for constructing classical binary chromosome and conversion of binary representation to numeric representation are $O(N^2)$ operations. The procedure for measuring operator is presented in Table 2.

The measuring procedure has been modified in this chapter so that condition given in equation (20) is fulfilled and no infeasible solutions are generated.

Table 2. Procedure for measuring operator

Procedure 1: Measuring Operator
Input: Q-bit Chromosome q
Output: Classical Binary chromosome b
Begin for i=1:N for j=1:N if $random[0,1) < \beta(i,j) ^2$ if $b(i,1:j-1) = 0 \ \&\& \ b(1:i-1,j) = 0$ then $b(i,j) = 1$ else $b(i,j) = 0$ End

4.2.4 Fitness Function

Evaluating the quality of solutions is an important aspect of working of any evolutionary technique including QIGA. The fitness of a chromosome represents the probability of reproduction and survival to the next generation. Higher the fitness value, higher is the chance of producing offspring and therefore surviving to next generation. Fitness function, a heuristic specific to the problem being addressed, is used to evaluate the quality of solutions. In this chapter, the fitness function evaluates the performance of assembling the DNA fragments.

The efficiency of assembling the fragments by finding their proper order and orientation depends on the overlap score between adjacent fragments. Higher the overlap score better is the assembled sequence as it is assumed that fragments having higher overlap score are generated from the same region of DNA sequence and therefore needs to be adjacent in the fragment layout. Therefore, fitness of solutions is evaluated using equation (3).

4.2.5 Updating the Q-Bit Population

Q-gate operator is used to update the Q-bit population and make it evolve towards the best solution. In literature, rotation gate has been the most commonly used Q-gate operator. Therefore, in this chapter also Rotation gate operator is used for updating the Q-bits as shown below.

$$\begin{bmatrix} \alpha(x,y)^{j+1} \\ \beta(x,y)^{j+1} \end{bmatrix} = U(\Delta\phi_{x,y}) \begin{bmatrix} \alpha(x,y)^j \\ \beta(x,y)^j \end{bmatrix} \text{ for } x, y = 1, 2, \dots, N \quad (22)$$

where $U(\Delta\phi_{x,y})$ is the rotation operator as given in equation (7) and $\Delta\phi_{x,y}$ is the step size i.e. the angle by which Q-bit needs to be rotated. $\alpha(x,y)^{j+1}$ and $\beta(x,y)^{j+1}$ is the state of Q-bit after rotation and $\alpha(x,y)^j$ and $\beta(x,y)^j$ is the state before rotation.

Let b represents the current solution and best solution till current generation be represented by BS, then angle of rotation for $(x,y)^{th}$ Q-bit $\Delta\phi_{x,y}$ is computed using equation (23).

DNA Fragment Assembly Using Quantum-Inspired Genetic Algorithm

$$\Delta\phi_{x,y} = (BS_{x,y} - b_{x,y}) \left(\frac{F(BS) - F(b)}{F(BS)} \right) * 2\pi \quad (23)$$

where $BS_{x,y}$ and $b_{x,y}$ represent the $(x,y)^{th}$ bit and $F(BS)$ and $F(b)$ represent the fitness value of BS and b respectively.

The QGFA algorithm is presented in Table 3.

Table 3. QGFA algorithm

Algorithm 2: QGFA
Input: Set of fragments \mathcal{F} , Number of Fragments N , Maximum number of generations Gen_{max} , Population Size m , Overlap Score matrix \mathcal{W}
Output: Best layout of the fragments
<p>Begin Initialize generation number $j=0$ Initialize Q-bit population $Q(j) = \{q_1^j, q_2^j, q_3^j, \dots, q_m^j\}$ for $j=0$ Measure $Q(j)$ to generate $B(j) = \{b_1^j, b_2^j, b_3^j, \dots, b_m^j\}$ using Procedure 1 For each $b_i^j \in B(j), i = 1, 2, \dots, m$ Evaluate fitness value F_i of b_i^j using equation (3) End for Determine current best solution $CBS = b_i^j$ such that $F_i = \max_{j=1,2,\dots,m} F_j$ Initialize best solution $BS=CBS$ While $(j < Gen_{max})$ Update $Q(j)$ using equation (22) and (23) Measure $Q(j)$ to generate $B(j) = \{b_1^j, b_2^j, b_3^j, \dots, b_m^j\}$ using Procedure 1 For each $b_i^j \in B(j), i = 1, 2, \dots, m$ Evaluate fitness value F_i of b_i^j using equation (3) End for Determine current best solution $CBS = b_i^j$ such that $F_i = \max_{j=1,2,\dots,m} F_j$ if $F(CBS) > F(BS)$ $BS = CBS$ End if End while Return BS End</p>

5. EXPERIMENTAL RESULTS AND ANALYSIS

The experiments have been conducted on an Intel core i5 Processor with 4GB RAM in Windows8 environment. Real genome sequences frequently used for validating the models for DFA problem in existing literature have been used to test the effectiveness of proposed QGFA algorithm. The genome sequences used in this work have been taken from NCBI website. The details of the datasets are given in Table 4. Noiseless data has been used in this work. The pair wise overlap between fragments has been computed

using a semi-global alignment technique presented in (Coull & Szymanski, 2008). If the overlap score between the fragments is less than thirty then it not considered as real match.

Table 4. Details of dataset

Instances	Coverage	Mean Fragment Length	No. of Fragments	Original Sequence LENGTH (in bps)
X60189_4	4	395	39	3835
X60189_5	5	386	48	
X60189_6	6	343	66	
X60189_7	7	387	68	
M15421_5	5	398	127	10089
M15421_6	6	350	173	
M15421_7	7	383	177	
j02459_7	7	700	352	48502
BX842596_4	4	708	442	77292
BX842596_7	7	703	773	

The proposed QGFA approach has been compared with other metaheuristic approaches used for addressing the DNA fragment assembly problem which include GA, PSO and ACO. The comparison is performed on the basis of overlap score (F) and number of contigs (denoted by NC). The experimental setup for all these approaches is given in Table 5. Comparison based on overlap score is shown in Table 6. And comparison in terms of number of contigs is shown in Table 7.

Table 5. Experimental setup

Parameter	Value
Population size	100
Number of Generations	2000
Selection (GA)	Binary tournament
Crossover (GA)	Ordered two point crossover ($P_c=0.75$)
Mutation (GA)	Insertion ($P_m=0.10$)
Inertia weight (PSO)	0.65
Cognitive element (PSO)	2
Social parameter (PSO)	2
Pheromone importance α (ACO)	0.5
Heuristic importance β (ACO)	1
Evaporation coefficient ρ (ACO)	0.2

DNA Fragment Assembly Using Quantum-Inspired Genetic Algorithm

Table 6. Comparison in terms of overlap score

Instances	Overlap Score (F)			
	QGFA	GA	PSO	ACO
X60189_4	12428	11527	11976	12105
X60189_5	14731	13978	14433	14489
X60189_6	18836	18008	18291	18302
X60189_7	21685	20986	21489	21505
M15421_5	38791	37417	38578	38593
M15421_6	48412	47198	47582	47896
M15421_7	55896	52355	53498	54325
j02459_7	116109	108643	112557	113914
BX842596_4	227957	211135	217915	218332
BX842596_7	442861	418568	421186	426748

Table 7. Comparison in terms number of contigs

Instances	Number of Contigs (NC)			
	QGFA	GA	PSO	ACO
X60189_4	1	3	2	2
X60189_5	1	2	2	2
X60189_6	1	2	1	1
X60189_7	1	1	1	1
M15421_5	3	9	7	6
M15421_6	2	6	6	3
M15421_7	1	5	4	2
j02459_7	3	13	9	7
BX842596_4	5	16	11	11
BX842596_7	2	8	5	4

It can be inferred from Table 6 and Table 7 that QGFA produces DNA fragment layout having higher value of overlap score and smaller value of number of contigs. Therefore, QGFA performs comparatively better as compared to GA, PSO and ACO based DNA fragment assembly algorithms. The reason for QGFA performing better than others is that it has better exploration and exploitation capability even for smaller population sizes. Another advantage of using QGFA is that number of parameters to be adjusted is lesser in comparison to other techniques considered in this chapter. But the QGFA proposed in this chapter is computationally more expensive as compared to GA, PSO and ACO based approaches. This is due to the reason that solution representation is in matrix form which requires $O(N^2)$ computational time for quantum measurement, fitness evaluation and population updation operations while in the other techniques considered in this chapter solution representation is in vector form thus requiring only $O(N)$ computational time.

6. CONCLUSION AND FUTURE WORK

DNA fragment assembly is a critical step in whole genome sequencing using shotgun sequencing technique. Assembly process aims to reconstruct the original DNA sequence by determining the proper order and orientation of the fragments in a layout. DNA fragment assembly problem has been proved to be NP-Hard and therefore finding exact solutions is not possible. A number of techniques have been proposed in literature for addressing this problem but due to its importance and complexity, better techniques are still needed. In this chapter, Quantum inspired Genetic algorithm has been adapted to address the DNA Fragment Assembly problem (QGFA) as in literature quantum inspired metaheuristic techniques have been proved performing better than traditional metaheuristic techniques. The efficacy of proposed QGFA approach has been evaluated by comparing it with other metaheuristic approaches used for solving the DNA fragment assembly problem. Simulation results show that QGFA based assembly is comparatively better in terms of the overlap score and the number of contigs produced. But the proposed QGFA approach is computationally more expensive as compared to other approaches. This is due to the reason that solution is represented using a matrix due to which quantum measurement, fitness evaluation and updating the population operations become computationally expensive. Devising novel methods for solution representation which maintain the inherent capabilities of Q-bit representation and are computationally less expensive can be considered as a future work.

REFERENCES

- Alba, E., & Dorronsoro, B. (2008). *Cellular genetic algorithms*. Heidelberg, Germany: Springer-Verlag.
- Alba, E., & Luque, G. (2007). *A new local search algorithm for the DNA fragment assembly problem*. Paper presented in Evolutionary Computation in Combinatorial Optimization, EvoCOP'07, Valencia, Spain. doi:10.1007/978-3-540-71615-0_1
- Alba, E., Luque, G., & Minetti, G. (2008). Seeding strategies and recombination operators for solving the DNA fragment assembly problem. *Information Processing Letters*, 108(3), 94–100. doi:.ipl.2008.04.005 doi:10.1016/j
- Angeleri, E., Apolloni, B., de Falco, D., & Grandi, L. (1999). DNA fragment assembly using neural prediction techniques. *International Journal of Neural Systems*, 9(6), 523–544. doi:10.1142/S0129065799000563 PMID:10651335
- Bocicor, M. I., Czibula, G., & Czibula, I. G. (2011). A reinforcement learning approach for solving the fragment assembly problem. In *Proceedings of 13th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing* (pp. 191-198). Academic Press. 10.1109/SYNASC.2011.9
- Braga, M. D. V., & Meidanis, J. (2002). An algorithm that builds a set of strings given its overlap graph. *Lecture Notes in Computer Science*, 2286, 52–63. doi:10.1007/3-540-45995-2_10
- Burks, C., Engle, M., Forrest, S., Parsons, R. J., Soderlund, C., & Stolorz, P. (1994). *Stochastic optimization tools for genomic sequence assembly*. London, UK: Academic Press. doi:10.1016/B978-0-08-092639-1.50038-1

DNA Fragment Assembly Using Quantum-Inspired Genetic Algorithm

- Chaisson, M., Pevzner, P., & Tang, H. (2004). Fragment assembly with short reads. *Bioinformatics (Oxford, England)*, 20(13), 2067–2074. doi:10.1093/bioinformatics/bth205 PMID:15059830
- Chang, W., & Lawler, E. (1990). Approximate string matching in sublinear expected time. In *Proceedings of the 31st IEEE Symposium on Foundations of Computer Science* (pp. 118-124). IEEE. 10.1109/FSCS.1990.89530
- Chevreur, B. (2005). *MIRA: An automated genome and EST assembler* (Ph.D thesis). German Cancer Research Center, Heidelberg, Germany.
- Churchill, G., Burks, C., Eggert, M., Engle, M., & Waterman, M. (1993). *Assembling DNA sequence fragments by shuffling and simulated annealing (Tech. Rep. No. LAUR 93-2287)*. Academic Press.
- Coull, S. E., & Szymanski, B. K. (2008). Sequence alignment for masquerade detection. *Computational Statistics & Data Analysis*, 52(8), 4116–4131. doi:10.1016/j.csda.2008.01.022
- Dorransoro, B., Alba, E., Luque, G., & Bouvry, P. (2008). A self-adaptive cellular memetic algorithm for the DNA fragment assembly problem. In *Proceedings of IEEE Congress on Evolutionary Computation* (pp. 2651-2658). IEEE. 10.1109/CEC.2008.4631154
- Ferreira, C. E., de Souza, C. C., & Wakabayashi, Y. (2002). Rearrangement of DNA fragments: A branch-and-cut algorithm. *Discrete Applied Mathematics*, 116(1/2), 161–177. doi:10.1016/S0166-218X(00)00324-3
- Firoz, J. S., Rahman, M. S., & Saha, T. K. (2012). Bee algorithms for solving DNA fragment assembly problem with noisy and noiseless data. In *Proceedings of the Conference on Genetic and Evolutionary Computation, GECCO'12*. Philadelphia: GECCO. 10.1145/2330163.2330192
- Han, K., & Kim, J. (2002). Quantum inspired evolutionary algorithm for a class of combinatorial optimization. *IEEE Transactions on Evolutionary Computation*, 6(6), 580-593.
- Hernandez, D., Francois, P., Farinelli, L., Osteras, M., & Schrenzel, J. (2008). De novo bacterial genome sequencing: Millions of very short reads assembled on a desktop computer. *Genome Research*, 18(5), 802–809. doi:10.1101/gr.072033.107 PMID:18332092
- Huang, K. W., Chen, J. L., Yang, C. S., & Tsai, C. W. (2015). A memetic particle swarm optimization algorithm for solving the DNA fragment assembly problem. *Neural Computing & Applications*, 26(3), 495–506. doi:10.1007/00521-014-1659-0
- Huang, K. W., Chen, J. L., Yang, C. S., & Tsai, C. W. (2016). A memetic gravitation search algorithm for solving DNA fragment assembly problems. *Journal of Intelligent & Fuzzy Systems*, 30(4), 2245–2255. doi:10.3233/IFS-151994
- Huang, X. (1992). A contig assembly program based on sensitive detection of fragment overlaps. *Genomics*, 14(1), 18–25. doi:10.1016/S0888-7543(05)80277-0 PMID:1427824
- Huang, X., & Madan, A. (1999). CAP3 sequence assembly program. *Genome Research*, 9(9), 868–877. doi:10.1101/gr.9.9.868 PMID:10508846

- Huang, X., Wang, J., Aluru, S., Yang, S. P., & Hillier, L. (2003). PCAP: A whole-genome assembly program. *Genome Research*, 13(9), 2164–2170. doi:10.1101/gr.1390403 PMID:12952883
- Jeck, W. R., Reinhardt, J. A., Baltrus, D. A., Hickenbotham, M. T., Magrini, V., & Mardis, E. R. (2007). Extending assembly of short DNA sequences to handle error. *Bioinformatics (Oxford, England)*, 23(21), 2942–2944. doi:10.1093/bioinformatics/btm451
- Jones, D. F., Mirrazavi, S. K., & Tamiz, M. (2002). Multiobjective meta-heuristics: An overview of the current state-of-the-art. *European Journal of Operational Research*, 137(1), 1–9. doi:10.1016/S0377-2217(01)00123-0
- Kchouk, M., & Elloumi, M. (2016, December). A clustering approach for denovo assembly using Next Generation Sequencing data. In *Bioinformatics and Biomedicine (BIBM), 2016 IEEE International Conference on* (pp. 1909-1911). IEEE. 10.1109/BIBM.2016.7822812
- Kikuchi, S., & Chakraborty, G. (2006). Heuristically tuned GA to solve genome fragment assembly problem. In *Proceedings of IEEE Congress on Evolutionary Computation CEC'06* (pp. 1491-1498). IEEE. 10.1109/CEC.2006.1688485
- Kubalik, J., Buryan, P., & Wagner, L. (2010). Solving the DNA fragment assembly problem efficiently using iterative optimization with evolved hypermutations. In *Proceedings of the 12th Annual Conference on Genetic and Evolutionary Computation, GECCO'10*, (pp. 213-214). GECCO. 10.1145/1830483.1830522
- Li, P., Kupfer, K. C., Davies, C. J., Burbee, D., Evans, G. A., & Garner, H. R. (1997). PRIMO: A primer design program that applies base quality statistics for automated large-scale DNA sequencing. *Genomics*, 40(3), 476–485. doi:10.1006/geno.1996.4560 PMID:9073516
- Mallén-Fullerton, G. M., Quiroz-Ibarra, J. E., Miranda, A., & Fernández-Anaya, G. (2015). Modified Classical Graph Algorithms for the DNA Fragment Assembly Problem. *Algorithms*, 8(3), 754–773. doi:10.3390/a8030754
- McCombie, W. R., & Martin-Gallardo, A. (1994). Large-scale, automated sequencing of human chromosomal regions. In *Automated DNA sequencing and analysis*. San Diego, CA: Academic Press. doi:10.1016/B978-0-08-092639-1.50028-9
- Medvedev, P., Georgiou, K., & Myers, E. W. (2007). Computability and equivalence of models for sequence assembly. In *Proceedings of Workshop on Algorithms in Bioinformatics (WABI)*. WABI. 10.1007/978-3-540-74126-8_27
- Meksangsouy, P., & Chaiyaratana, N. (2003). DNA fragment assembly using an ant colony system algorithm. In *Proceedings of Congress on Evolutionary Computation CEC'03* (Vol. 3, pp. 1756-1763). CEC. 10.1109/CEC.2003.1299885
- Narayanan, A., & Moore, M. (1996). Quantum-inspired genetic algorithm. *Proceedings of IEEE International Conference on Evolutionary Computation*, 61–66. 10.1109/ICEC.1996.542334
- Nielsen, M., & Chuang, I. (2000). *Quantum computation and quantum information*. Cambridge University Press.

DNA Fragment Assembly Using Quantum-Inspired Genetic Algorithm

- Parsons, R. J., Forrest, S., & Burks, C. (1993). Genetic algorithms for DNA sequence assembly. *ISMB-93 Proceedings, 1*, 310-318.
- Parsons, R. J., Forrest, S., & Burks, C. (1995). Genetic Algorithms, operators and DNA fragment Assembly. *Machine Learning, 21*(1/2), 11–33. doi:10.1023/A:1022613513712
- Phillippy, P. M., Delcher, A. L., & Salzberg, S. L. (2004). Comparative genome assembly. *Briefings in Bioinformatics, 5*(3), 237–248. doi:10.1093/bib/5.3.237 PMID:15383210
- Pop, M. (2009). Genome assembly reborn: Recent computational challenges. *Briefings in Bioinformatics, 10*(4), 354–366. doi:10.1093/bib/bbp026 PMID:19482960
- Rathee, M., & Kumar, T. V. (2014). Dna fragment assembly using multi-objective genetic algorithms. *International Journal of Applied Evolutionary Computation, 5*(3), 84–108. doi:10.4018/ijaec.2014070105
- Setubal, J., & Meidanis, J. (1997). *Introduction to computational molecular biology*. PWS Publishing Company.
- Simpson, J. T., Wong, K., Jackman, S. D., Schein, J. E., Jones, S. J. M., & Birol, I. (2009). ABYSS: A parallel assembler for short read sequence data. *Genome Research, 19*(6), 1117–1123. doi:10.1101/gr.089532.108 PMID:19251739
- Sivanandan, S. N., & Deepa, S. N. (2008). *Introduction to genetic algorithms*. Springer.
- Smith, T., & Waterman, M. (1981). Identification of common molecular subsequences. *Journal of Molecular Biology, 147*(1), 195–197. doi:10.1016/0022-2836(81)90087-5 PMID:7265238
- Staden, R. (1980). A new computer method for the storage and manipulation of DNA gel reading data. *Nucleic Acids Research, 8*(16), 3673–3694. doi:10.1093/nar/8.16.3673 PMID:7433103
- Sutton, G. G., White, O., Adams, M., & Kerlavage, A. (1995). TIGR assembler: A new tool for assembling large shotgun sequencing projects. *Genome Science & Technology, 1*(1), 9–19. doi:10.1089/gst.1995.1.9
- Waston, J. D., & Crick, F. H. C. (1953). Molecular structure of nucleic acids: A structure for deoxyribose nucleic acid. *Nature, 171*(4356), 737–738. doi:10.1038/171737a0 PMID:13054692
- Watson, J. D., & Berry, A. (2003). *DNA: The secret of life*. Knopf.
- Zerbino, D. R., & Birney, E. (2008). Velvet: Algorithms for de novo short read assembly using de Bruijn graphs. *Genome Research, 18*(5), 821–829. doi:10.1101/gr.074492.107 PMID:18349386
- Zhang, G. (2011). Quantum-inspired evolutionary algorithms: A survey and empirical study. *Journal of Heuristics, 17*(3), 303–351. doi:10.1007/10732-010-9136-0
- Zhang, G. X., & Rong, H. N. (2007). Real-observation quantum-inspired evolutionary algorithm for a class of numerical optimization problems. In *Lecture Notes in Computer Science: Vol. 4490. ICCS2007, Part IV* (pp. 989-996). Springer.

This research was previously published in Exploring Critical Approaches of Evolutionary Computation; pages 80-98, copyright year 2019 by Engineering Science Reference (an imprint of IGI Global).

Section 2

Cryptography, Encryption, and Security

Chapter 10

Quantum Internet and E–Governance: A Futuristic Perspective

Manan Dhaneshbhai Thakkar

U. V. Patel College of Engineering, Ganpat University, India

Rakesh D. Vanzara

 <https://orcid.org/0000-0002-6629-350X>

U. V. Patel College of Engineering, Ganpat University, India

ABSTRACT

We are leaving in the era where almost everyone in the world uses internet for the communication over social media site, shopping, E-commerce, online transaction and many more. The exponential growth in usage of internet resulted in security related challenges. Since last several years, traditional cryptography algorithms are found working well. Evolution of quantum computer and its high computing capability can break existing cryptography algorithms. To handle the security constraints, this chapter provides details on evolution of quantum cryptography, components involved to design network architecture for quantum internet, quantum key exchange mechanism and functionality wise stages for quantum internet. This chapter also includes challenges involved in evolution of quantum internet. Further, chapter also contains the details on e-governance, challenges in e-governance and solution using quantum cryptography.

INTRODUCTION

Quantum cryptography, is the way of encrypting messages by applying principles of quantum mechanism, in contrast with the traditional cryptography mechanism to encrypt the messages by applying the mathematical function over actual message (Maria Korolov, Doug Drinkwater, 2019). Main purpose of this quantum cryptography is to encrypt message in such a way that no outsider recipient can even read that message. Quantum communication is to be considered more secured than any existing information relay

DOI: 10.4018/978-1-7998-8593-1.ch010

system. If quantum communications were like sending a letter, entangled photons are like the envelope, they carry the message and keep it secure. It is expected that by 2030 (Sophia Chen, 2017), quantum communications will spread almost in all countries and that would be an era of quantum Internet. It means, all kind of communications (i.e. multimedia, text, voice) would happen by means of quantum signals compared to traditional digital signal (i.e. 0 and 1).

Quantum Internet provides new Internet technologies to us to solve the tasks which are impossible to achieve over classical Internet (Kimble, H. Jeff, 2008). As it's a new technology which is yet to explore fully, thus we cannot expect all the sectors making its usage initially. But, it provides good enough applications containing security related concern over Internet, to justify its importance. Basic elements of quantum Internet do not look much different from a classical one (Vesna Monojlovic, 2017). The way classical Internet is having one of component as end node, this quantum Internet also needed end node. But, that end node should support quantum Internet. So, as a node we cannot use normal laptop, phone or computer, but we need to make use of quantum computer. The way we have switch type of component in classical Internet as an intermediate point to establish connection, for the quantum Internet we need kind of switch which is capable to transmit qubits. Table-I depicts the comparison of classical and quantum Internet.

Table 1. Comparison between classical internet and quantum internet

Classical Internet	Quantum Internet
• End node: traditional computer, phone, laptop	• End node: Quantum system
• Switch	• Quantum switch
• Repeater	• Quantum repeater
• Data in the form of digital signal with combination of 0 and 1	• Data in the form of qubits
• Threat of cyber attack	• Secure

Electronic governance (E-governance) playing an important role in integrating information, science and technology within the administrative and management systems of an organization (Das, S. R., & Chandrashekhar, R., 2007). E-governance is the key to organize everything in public domain to increase the accessibility, efficiency, transparency and openness to the stakeholders. E-governance concept was basically designed to improve citizen's access to government information and services (Faraj, Sufyan T., M. Sagheer Ali, 2011). The concept of E-governance has found its wide range of applications by including several governmental domains like education, health care, security, power, citizen services and many more. In order to make information excessive and open for all, security threat is a major concern and information must be protected from unauthorized access (Faraj, Sufyan T., M. Sagheer Ali, 2011). Security is a major concern for successful implementation of E-Governance and transaction based services. Some of the security issues in E-Governance are: Authenticity, Confidentiality, Non-repudiation, Integrity. The important thing to understand is, how to solve security related challenges by using the concept of quantum cryptography and quantum key exchange. Many industries and government sectors are currently trying to build the quantum computer which will avoid many computing and security related problems (Faraj, Sufyan T., M. Sagheer Ali, 2011).

BACKGROUND

Due to more and more usage of technologies and user's seamless connectivity with Internet, it has become playground for hackers to perform malicious tasks (Anil Ananthaswamy, 2019). From data stored on cloud or any other storage device for communication, insecurity and vulnerability are everywhere. But, quantum physics have their own way to protect against these challenges. Classical computers work with traditional bit system with value 0 and 1 (Wehner, S., Elkouss, D., & Hanson, R., 2018), but with the help of qubits we can have more storage for information. In future, quantum network may replace classical network.

As per the classical policy of encryption, it highly depends on keys to encrypt the message. Based upon type of key used, there are two types of mechanisms: symmetric key cryptography and asymmetric key cryptography. Cryptography using symmetric key works using a single shared secret key (Wehner, S., Elkouss, D., & Hanson, R., 2018). To crack such type of key requires double the computing power after every increment in bit size of key. Thus, longer the size of key, more and more powerful computing system require and require larger amount of time to crack. On the other hand, cryptography using asymmetric key uses pair of public and private key that needs to be generated mathematically (Wehner, S., Elkouss, D., & Hanson, R., 2018). Though it's very tough to crack with asymmetric key, but it is not the impossible task and key can be cracked by applying mathematical formula or more computing power behind it. No matter which type of approach used for encryption, but it is necessary to keep some private information secret. One threat related to security is in key exchange step. In order to secretly exchange keys among users, one possible way is by using quantum cryptography. The mechanism of exchanging key secretly using quantum mechanism is known as Quantum Key Distribution (QKD) (Wehner, S., Elkouss, D., & Hanson, R., 2018).

The Internet has a revolutionary impression across the globe. The vision and mission behind quantum Internet is to bring future Internet technology by evolving quantum communication between any two nodes across the world. As with the rapid changes in technology, it is very hard to make everyone to use futuristic quantum Internet in replacement of a classical Internet. Due to its high range of secure environment, it finds application in various domains like quantum key exchange, secure identification, two party cryptography, position verification, secure access to quantum computers in cloud, secure exchange of information across the globe, clock synchronization, quantum sensor network and many more. Essence of all these applications is the ability of a quantum Internet to transmit qubits compared to bits in traditional Internet.

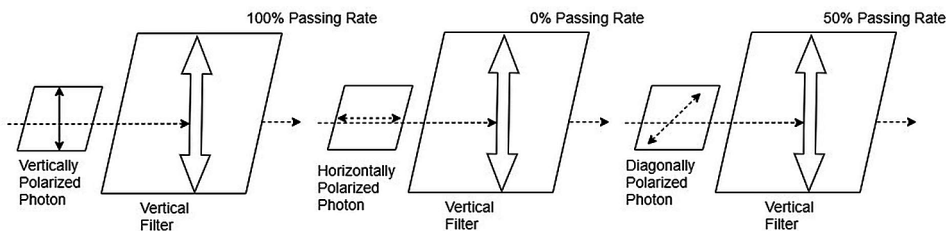
The biggest question to understand importance of quantum is: What makes the transmission of qubits so powerful than what we have today? One of the important feature of qubits is that, they cannot be copied, which makes them ideal for security applications. Anyone who tries to attempt this, can be easily identified. Qubits can be entangled among each other, that brings high level of and stronger correlations in contrast with that of classical information. This is the reason which makes qubits as one of the most suitable thing for security related applications. Though qubits are well suited but it also brings rapidly new concept in terms of technological components, which is also more challengeable. Early effort in development of quantum network, bring network with capacity to handle few qubits, But, as time elapsed, it evolved with more advanced network with more capacity and it also brings need of a unified framework for researchers.

Quantum Bits

There is a difference in a bit and a qubit. As per the traditional cryptography, we are used to transmit all the information in the 1s and 0s form. Whereas, qubits have a little different approach when we send and receive that. In case of traditional cryptography, the encryption-decryption key remains same, irrespective of how one read it (Nils Jacob Sand, 2018). Whereas, in case of quantum cryptography the value of key bit depends on how the value of qubit is measured. In case of quantum computer beam of photons transmitted and it gets represented in the form of 0s and 1s. Each of these particle is known as qubit.

Figure 1. Quantum bit transmission scenario

Source: (Nils Jacob Sand, 2018)



To send the qubits, we need to send photons via polarizer as shown in Figure 1. In this Figure, example of only vertical filter is included along with different types of polarized photons. At the receiver end, the value of received bit is determined based on the filter used (Nils Jacob Sand, 2018). In real world, qubits would have to be stored by atoms, ions (atoms with few or many electrons) or electrons and photons (Chris Woodford, 2019).

Quantum Cryptography - Overview

Quantum cryptography is the mechanism to allow users to interact or exchange information using safe and secure approach compared to traditional cryptography. The term Quantum Cryptography was firstly mentioned by Stephen Weisner in early 1970s as a part of their work 'conjugate coding' (Jorge Ortiz, Adam Sadovsky, and Olga Russakovsky, 2004). BB84 was very first quantum cryptography protocol developed in 1984. In 1991, very first experimental evaluation was carried out using quantum cryptography by operating it for a distance of 32 centimeters. Later, this experiment has been refined and executed for a distance of few kilometers.

The very first computer network using secure quantum cryptography approach for communication is up and running in Cambridge, Massachusetts. In 2003, entangled photons were transmitted at University of Vienna across the Danube river. As a part of real world application, first money transfer between two Austrian bank was carried out using quantum keys in April, 2004 (Jorge Ortiz, Adam Sadovsky, and Olga Russakovsky, 2004).

Purpose of quantum cryptography is not to replace traditional cryptography, but to provide more secure way of exchanging quantum keys useful for encryption and decryption purpose. The information transmitted through quantum cryptography is not large or fast, but it's very secure. To transmit data as

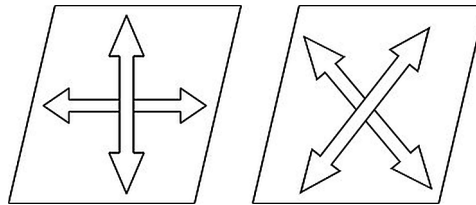
quickly as possible, it is good to achieve key exchange mechanism by using quantum cryptography and then encrypting and sending the data using traditional methods.

In quantum cryptography, data is converted into 0s and 1s to transfer using polarized photons. Afterwards, sender put photons into specific quantum state and these photons are observed by the recipient. A photon can be in one of the four polarizations: 0, 45, -45 and 90 degrees. These photons can be measured by using three different polarizer: rectilinear (vertical or horizontal), diagonal and circular (left or right circular) (Jorge Ortiz, Adam Sadovsky, and Olga Russakovsky, 2004). The receiver can discriminate between a 0 and 90, or 45 and -45 degree polarization for each signal. As per the principle of physics, a measurement of photons must destroy it (Jorge Ortiz, Adam Sadovsky, and Olga Russakovsky, 2004). So, it is not at all possible to carry observation without affecting its state. To understand the mechanism of quantum cryptography, BB84 protocol for quantum cryptography is an important reference (Brilliant.org, 2019).

BB84 protocol was designed in 1984 for quantum cryptography and named after Charles Bennett and Gilles Brassard. When sender generates photons, receiver does not aware about the type of polarizer used by sender. So, receiver randomly pick any one type of beam splitter as shown in Figure 2 (Brilliant.org, 2019).

Figure 2. Types of polarization

Source: (Nils Jacob Sand, 2018)



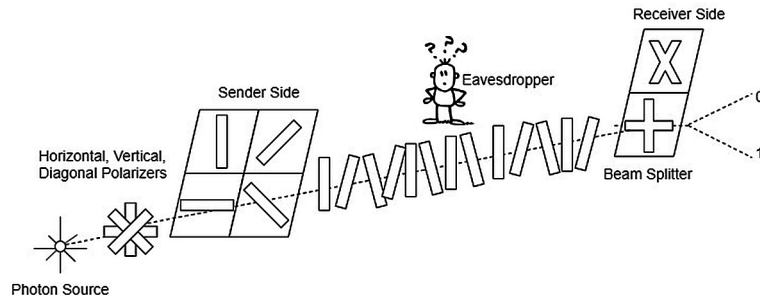
Whenever sender sends horizontal or vertical polarized photon, receiver does not aware about which splitter to use. Receiver can choose between '+' and 'x' beam splitters and this result in choosing right beam splitter only 50% of time. If receiver select '+' beam splitter for horizontal or vertical polarized photon, then receiver detects 0 or 1. Whereas, if receiver select 'x' beam splitter, then polarized photon will detect -45 or 45 degree which also corresponds to 0 or 1.

After receiving all the photons, receiver will be having key of bits also called raw bits. Afterwards, sender announces over insecure channel regarding sequence of beam splitters instead of 1s or 0s. After comparing beam splitters, sender and receiver discards the beam splitters which are not matching at both the side. As receiver randomly selected beam splitters, it has to generally discard half of the beam splitters used.

After shifting the set of bits, sender and receiver keeps only fraction of their key by comparing them on public channel to see if they have same value. The fraction of keys having same value are selected as secure quantum key (Jorge Ortiz, Adam Sadovsky, and Olga Russakovsky, 2004). If the eavesdropper tries to detect or intercept while transmitting set of bits, eavesdropper may pick up correct beam transmitter half of the times as there is 50% chances of picking up right one. There is no way for interceptor to alter the beam as after reaching at receiver that would be altered. This can be determined at the end

Figure 3. Photon transmission scenario

Source: (Nils Jacob Sand, 2018)



when sender and receiver compare it. If the result does not match the polarization of the photon, that means that someone might have observed the signal prior (Jorge Ortiz, Adam Sadovsky, and Olga Russakovsky, 2004).

Example – Step-by-Step Cryptography

Consider the step by step role of sender Alice, receiver Bob, Eve as an eavesdropper and error correction mechanism (Jorge Ortiz, Adam Sadovsky, and Olga Russakovsky, 2004).

- Alice needs to identify the polarization (rectilinear, diagonal or circular) of every single photon which Alice is looking to transfer towards Bob. Many information will get discarded at the receiver side, this polarization detection step needs to be done properly. The purpose of key exchange is to make both parties (sender and receiver) agree on a key.
- A light source from a LED or a laser is filtered to produce the desired photons.
- At the receiver side (Bob), it randomly generates multiple polarizer (rectilinear, diagonal or circular) and measures the polarization of each photon.
- Receiver publicly tells the sender regarding polarizer used at the receiver end without worrying about other people.
- Sender also publicly tells to receiver about which polarizer randomly chosen at sender side.
- Receiver discards all the incorrect observations received at the end.
- The remained observations need to be converted into binary code.
- To identify and resolve the error in the received bits, the strings of bits are partitioned into K blocks with each block of small size to minimize error in bits of block. If Alice's string is 110010 and Bob's string is 110111, the parity in both the case is same, though there are multiple bits in error.
- Alice and Bob exchange the computed parities of each block. This information also shared publicly but to avoid problem of Eve an eavesdropper, last bit of each block is then discarded. Reason to discard last bit is to make information meaningless for Eve.
- The above error corrected mechanism repeated for multiple number of times by increasing block size to discover multiple errors.

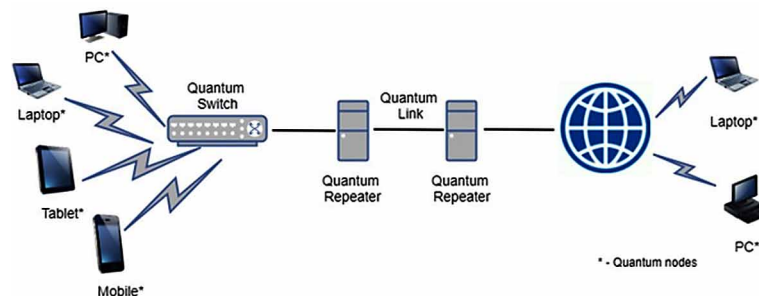
Quantum Internet and E-Governance

- At last, to detect any more errors, sender and receiver performs other random check. Alice and Bob publicly agree on a random assortment of half the bit positions in their string and compare parities. In this case also, they discard the last digit of string.
- If the strings are not same, both the parties do not agree on that.
- After repeating the above steps for r number of times, by agreeing on received strings always, both Alice and Bob can conclude that their strings disagree with $r/2$ probability.

HARDWARE COMPONENTS TO BUILD QUANTUM NETWORK

Figure 4 depicted the framework to establish quantum network with required network components. Each component of the framework is briefly explained in following subsections.

Figure 4. Framework to establish quantum network with network components
Source: (Johan Dubbeldam, 2019)



Link

As information needs to be transmitted in the form of qubits, it cannot be handled by traditional communication links. To transmit qubits between end nodes or node and repeater, photonic channels needed to be established. There are two types of photonic channels available: fiber based channels and free space channels. Both the types of available channels are having their own advantages and disadvantages. Thus, future Internet can be a combination of both the types of channels. Our ultimate need is to ensure kind of channel which exhibits minimal loss of qubits.

Quantum Nodes - Quantum Computer

Purpose of end node is to send and receive information. Quantum node for the purpose of quantum key distribution can be designed by using photodetector combined with telecommunication laser and parametric down-conversion. Sometimes these quantum nodes can be containing only beam splitters and photodetectors (Liam Critchley, 2018).

Before getting about quantum computer, it is necessary to define classical computer first. The essential part of classical computer is its integrated circuits. Over integrated circuits, we can find several

transistors and these transistors can be used to construct classical bits. These bits are used to perform calculation with the nodes (ScienceDaily, 2019). Quantum mechanics can offer unique phenomena by including superposition, interference and entanglement. Quantum computer generates high computing power with its promise to outperform today's and tomorrow's supercomputer. In classical computer interpreted values are either a 0 or a 1, Whereas, in quantum computer quantum bit or qubit can take both the values together at a time. The secret behind ability of quantum computer is to generate multiple qubits. To generate and manage these qubits, is a challenging task. The challenge is to find suitable platform for these qubits and have all the electronics to perform operations with these qubits. Quantum mechanical efforts are usually associated with small energy scales. These qubit systems build in the very special fridges offering temperature around 0 kelvin (-273°C) (Mohammad Choucair, 2016). Though such types of care have been taken while building qubits, still it does not work correctly. As a one of the solution to handle error correction is by building one large physical qubit by combining multiple copies of qubits. We don't need many logical qubits to build a powerful quantum computer, since many quantum algorithms provide an exponential speedup as compared to their classical counterpart. The thing which we need is, many physical qubits to build logical qubits. Thus, quantum computer may contain millions of qubits.

In 2000, David P. DiVincenzo listed out five key criteria for quantum computer:

- It must be scalable.
- It must be possible to initialize the qubits.
- Good qubits are needed, so the quantum state cannot be lost.
- We need to have a universal set of quantum gates. Which means, one can do the operation needed to execute a quantum algorithm.
- We need to be able to measure all qubits.

Quantum Switch

Quantum computer enables quantum bits to get transmitted simultaneously among multiple space time trajectories. Now, whatever quantum information transmitted through carrier can travel through multiple communication channels and arrives in a different order (Caleffi, M., & Cacciapuoti, A. S., 2019). So, relative time order of communication channels becomes unfixed. This thing can be managed by the device called quantum switch. The proper utilization of a quantum switch provides numerous benefits for the purpose of quantum computation, quantum information processing and many more with different applications (Caleffi, M., & Cacciapuoti, A. S., 2019).

Quantum Repeater

In most of the communication medium including optical fibre, there could be a loss of signal whenever there is a long communication distance to travel for a message. In classical Internet, in order to boost the signal to travel long distance, amplifiers were used. But, these amplifiers cannot handle qubits as it cannot be copied as per the no cloning principle. Thus, to mimic the features of amplifier, complete flying qubit would be needed, which is not desirable and bit difficult (Lisa Zyga, 2018).

The quantum repeater can be found as an alternative to handle this challenge of end to end transmission of qubits (Lisa Zyga, 2018). In the transmission of a quantum key, one has to rely on intermediate trusted quantum repeater. After exchanging key with both the node, key distribution protocols can be

used to test for the entanglement. Hence, while exchanging keys, the sender and receiver are secured even if they do not trust the quantum repeater.

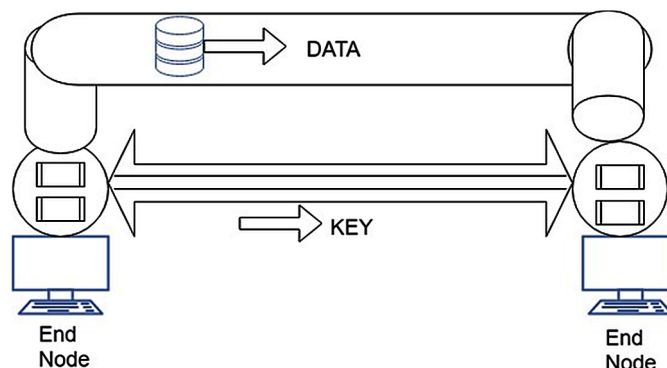
QUANTUM KEY EXCHANGE

In order to protect important data from external user, encryption is an important mechanism. It protects confidential information by shielding from exposure of attacks. Before one should transmit data or file, or store that over cloud, security related mechanism must be applied. One of the most widely used approach to perform encryption is the symmetric key cryptography (Quantum-Safe Security Working Group, 2015). The main challenge that has been faced while working with symmetric key is the secure share of the keys among sender and receiver. In order to make secure communication between two parties, it is necessary to exchange cryptographic keys among both parties. In classical encryption and key exchange mechanism, the most commonly used algorithms are Diffie-Hellman key exchange algorithm, RSA, ECC etc. upon which all gets agree (Quantum-Safe Security Working Group, 2015). As these encryptions are based upon some mathematical formula, it requires some amount of mathematical function to decrypt that. Though, it is possible to decrypt by applying all possible combination of keys, but due to very large number of bits for the purpose of encryption key, it requires very high and infeasible computing power.

As it is possible to crack this encrypted message, which plays one big challenge as a security threat with powerful computing system. The emerging infrastructure in the form of a quantum computer will make classical encryption unsafe. Thus, the continuous growth of quantum information processing makes it necessary to think again on, how to exchange symmetric cryptographic key securely? One of the most powerful technique against any high computational power, quantum computer or any new algorithm, is Quantum Key Distribution (QKD) which tries to handle the secret key exchange related challenge (Quantum-Safe Security Working Group, 2015). QKD relies on generating a random key and securely transmitting it on a separate channel from where encrypted data transmitted. Key data is generated by quantum engine and transmitted as a stream of photons through optical fiber quantum link. The key is completely random which contains quantum information that can be successfully interpreted by the designated recipient (Quantum-Safe Security Working Group, 2015).

Figure 5. Exchange links for quantum key and encrypted data

Source: (Yongli Zhao, Yuan Cao, Xiaosong Yu and Jie Zhang, 2018)



For example, consider the person 'A' transmitting confidential information over the Internet to the bank and their quantum engine generates a random key. Data on how to reconstruct the key is then transmitted through the quantum link to the bank. Figure 5 depicted the scenario of key and data.

The QKD end node (transmitter) at the source node end establishes a QKD link with the node at forthcoming end (receiver) by making use of QKD transmitter in the intermediate node (Yongli Zhao, Yuan Cao, Xiaosong Yu and Jie Zhang, 2018). These end nodes transmit or receive qubits that would have to be stored by atoms, ions (atoms with few or many electrons) or electrons and photons (Chris Woodford, 2019). To transmit or receive qubits, there will be a need of quantum node. While transmitting data, it is possible that any interceptor person (hacker) can intercept the confidential information. But, interceptor cannot recreate the key to decrypt the confidential information. This is because, when the hacker tries to intercept the photons stream passed on a separate quantum channel, any interruption or change over photon channel will alert the system about the unauthorized access. The benefit of using secure fiber channel makes sense in all protected communications. However, photon transmission is limited to about 60 miles (Quantum XC¹, 2019). This problem of signal getting weakens is solved by creating a chain of QKD trusted nodes (including quantum repeaters) spread across the globe. These nodes allow us to share keys over long distances and among multiple users.

As this way of exchanging QKD comes out as one of the promising approach, there are two different types of quantum key distributions that have been emerged. The first variant is called Discrete Variable QKD (DV-QKD) (Josue Aaron Lopez-Leyva et al., 2018) This DV-QKD encodes the quantum information in discrete variables and make use of a single photon detectors to calculate the quantum states. The protocols emerged for this DV-QKD are the BB84 and the E91 protocol (Josue Aaron Lopez-Leyva et al., 2018). Another variant of QKD is Continuous Variable QKD (CV-QKD). In this CV-QKD type, quantum detail is encrypted onto the amplitude and phase quadrature of a coherent laser, and can then be measured by the receiver using homodyne detectors. The protocols arisen for this CV-QKD are the Silberhorn and the Grangier protocol (Quantum-Safe Security Working Group, 2015).

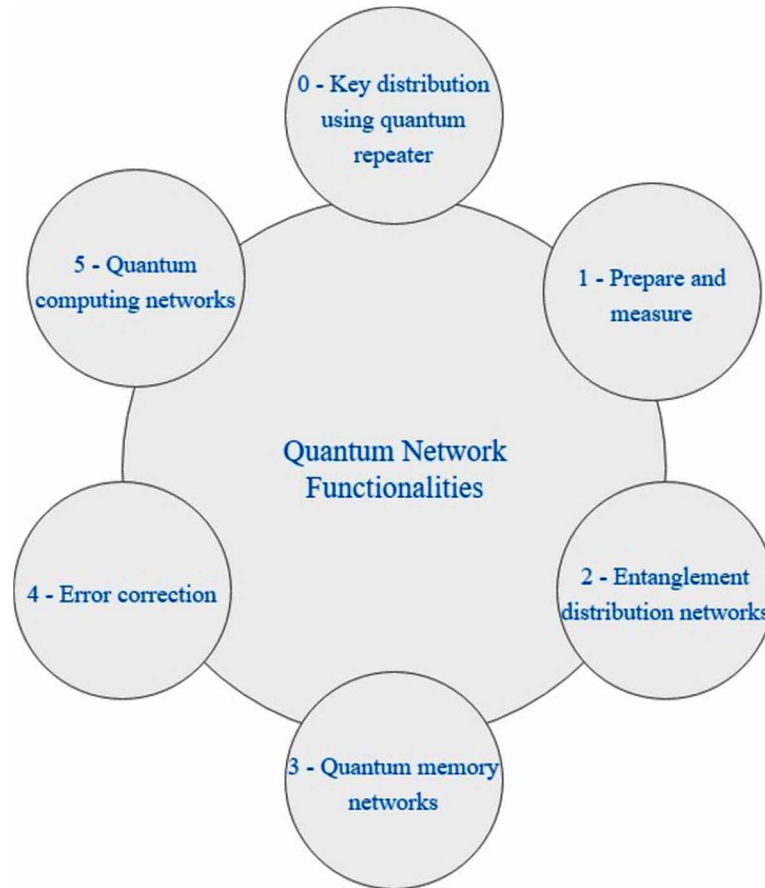
STAGES OF QUANTUM INTERNET DEVELOPMENT

In order to understand how quantum Internet works along with its application, it is necessary to understand the functionality wise stages of quantum Internet. There are total six stages and each stage is different from other based on amount of functionality. Here, every new stage not only improves the functionality of previous stage, but it brings new functionalities (Wehner, Stephanie, David Elkouss, Ronald Hanson, 2018). Figure 6 depicted six stages of Quantum Internet Development.

Apart from the challenge for newer infrastructure development, quantum Internet also brings challenge as well as research opportunity to for the quantum related software developer to design new protocols, understand and design functionality of all the associated stages. While understanding the functionality of each stage, the need of hardware component including communication link, quantum node and quantum repeater can also be realized. Researchers have identified following six stages of futuristic quantum Internet at which it might reach with functionalities available for user at each level:

Figure 6. Functionalities of quantum network

Source: (Davide Castelvecchi, 2018)



Key Distribution Using Quantum Repeater

This is the very first stage of quantum Internet which is different from others by not allowing end to end transmission of qubits. Quantum repeater came out as one of the trusted network component which allow securely exchange of quantum key. Generally, quantum repeater has at least two nodes directly connected with it with very short distance link connecting end node or any other intermediary quantum repeater (Wehner, Stephanie, David Elkouss, Ronald Hanson, 2018) (Davide Castelvecchi, 2018) (Johan Dubbeldam, 2019).

Consider the two end nodes M and N, and a trusted repeater R in between two nodes. Before M and N exchange quantum key KMN, initially M and R exchange quantum key KMR. Similarly, R and N exchange quantum key KRN. Now, M and N can exchange key KMN. M send KMN to R encrypted using the key KMR. R decrypts that to obtain quantum key KMN. Then after R re-encrypts quantum key KMN using the key KRN and sends it to N. Finally, N decrypts that encrypted key using KRN. This indicates that, KMN is not only known to M and N, but trusted repeater is also aware about this quantum key. Thus, it creates end to end communication securely until intermediate repeater is trusted (Wehner, Stephanie, David Elkouss, Ronald Hanson, 2018).

Prepare and Measure

In above stage we have to keep trust on intermediate repeater to ensure security. It is also sufficient to perform end to end quantum key exchange without keeping trust on intermediate repeater nodes. In the other word, this level allows any node to prepare a one qubit state and send that resulting state to other node. The node on the receiving end measure it. This level allows two or more end user to share a private key once they know each other and users can share their password or any confidential details without revealing it (Wehner, Stephanie, David Elkouss, Ronald Hanson, 2018) (Davide Castelvecchi, 2018) (Johan Dubbeldam, 2019).

Consider the two nodes p and q , with any one qubit state Ψ and any one qubit measurement M . Then, there exists a way for p to prepare Ψ , transfer it to q in such a way that q performs measurement M on Ψ or q can conclude that the qubit was lost (Wehner, Stephanie, David Elkouss, Ronald Hanson, 2018).

Entanglement Distribution Networks

This third level of quantum Internet development allows end to end creation of deterministic quantum entanglement and make user to get entangled states. The important thing to observe is, the end node does not need quantum memory for this level. The term deterministic quantum entanglement refers to the fact that the process succeeds with probability closure to one (Wehner, Stephanie, David Elkouss, Ronald Hanson, 2018) (Davide Castelvecchi, 2018) (Johan Dubbeldam, 2019).

Quantum Memory Networks

This fourth level justifies the capability of end nodes to have local quantum memory to get and store entangled qubits. This storage allows the implementation of complex protocols which sometimes needed to store quantum state for further communication (Wehner, Stephanie, David Elkouss, Ronald Hanson, 2018) (Davide Castelvecchi, 2018) (Johan Dubbeldam, 2019). For any two node m and n , the quantum network allows the entanglement generation and some additional tasks as specified below by using the quantum memory (Wehner, Stephanie, David Elkouss, Ronald Hanson, 2018):

- Preparation of a one qubits with qubits state generated Ψ by end node m and n
- As seen in level 2, at any node it permits measurements of any qubits
- It permits storage of qubits for minimum of $k \cdot ld \cdot t$ time. Here, t is the amount of time needed to generate one ERP pair and transmit a classical message from node m to n , k is the number of rounds, d is the circuit depth, ld is the amount of time taken to execute depth d quantum circuit at the end node.

Error Correction

The next stage allows devices (quantum computers) on the network to handle error correction and provides fault tolerance on transferred data. Fault tolerance property is necessary for many quantum Internet protocols. Apart from this error correction related benefit, it also allows the execution of quantum computation of high circuit depth. As a cost of this benefit, it brings arbitrary extension of storage time

to execute protocols with different rounds (Wehner, Stephanie, David Elkouss, Ronald Hanson, 2018) (Davide Castelvecchi, 2018) (Johan Dubbeldam, 2019).

Quantum Computing Networks

The problems that were identified with classical computers and for which it has no solution, can now be solved with quantum computing networks. This network provides facility to arbitrarily transfer quantum communication. It permits number of qubits to get efficiently transmitted through quantum computer (Wehner, Stephanie, David Elkouss, Ronald Hanson, 2018) (Davide Castelvecchi, 2018) (Johan Dubbeldam, 2019).

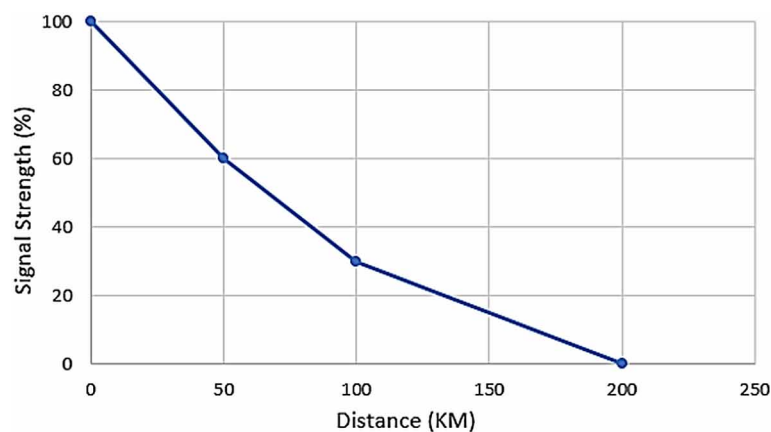
CHALLENGES WITH QUANTUM NETWORKS

For the globally acceptance of quantum Internet, it has to overcome several challenges alongside of its applications (Abhishek Sharma, 2018).

Quantum Signal Weakens After Certain Distance

In order to establish connection and communication at the global level, one of the biggest challenge is with long distance. Generally, photons get transmitted through the air or optical fiber. After travelling through these mediums for about 60 miles, majority of quantum signal dies. After a travel of about few hundred kilometers, 99.99% signal get vanished and signal becomes too weak to travel and communicate for a long distance. Variation of signal strength with distance is illustrated in Figure 7.

Figure 7. Unviable view of signal strength variation with distance



Network Infrastructure

In order to transit from classical network to quantum network, new technological infrastructure must be needed. Very first need in order to establish the communication over transmission medium (quantum channel) is support for transmission of qubits. As per the very first challenge where signal becomes weaker after travelling a long distance, classical network uses amplifier type of equipment to boost the signal strength. But, because of no cloning theorem used with qubits, it cannot be copied and ultimately amplifier cannot be used in quantum network. As per the theoretical proof, to overcome this long distance problem, quantum repeaters can be used in optical fiber at certain distance. One more and important network component of any network is end point host, i.e., quantum processor connected to quantum Internet. This node may vary with its processing capability from simple node with capability to measure single qubits to large and complex quantum computer.

Quantum Memory

As with the memory used for the storage purpose in classical computer, quantum memory is the need of quantum computer. For the storage and transmission of a single photon quantum, photonic quantum memories are available. But to handle more photon quantum, development of powerful quantum memory is still one big challenge as it requires perfectly matched photon-matter quantum interface. Few researchers already have worked and come up with more efficient memory compared to traditional one. The need of such powerful quantum memory is must there as single photon is too weak and can be easily mislaid.

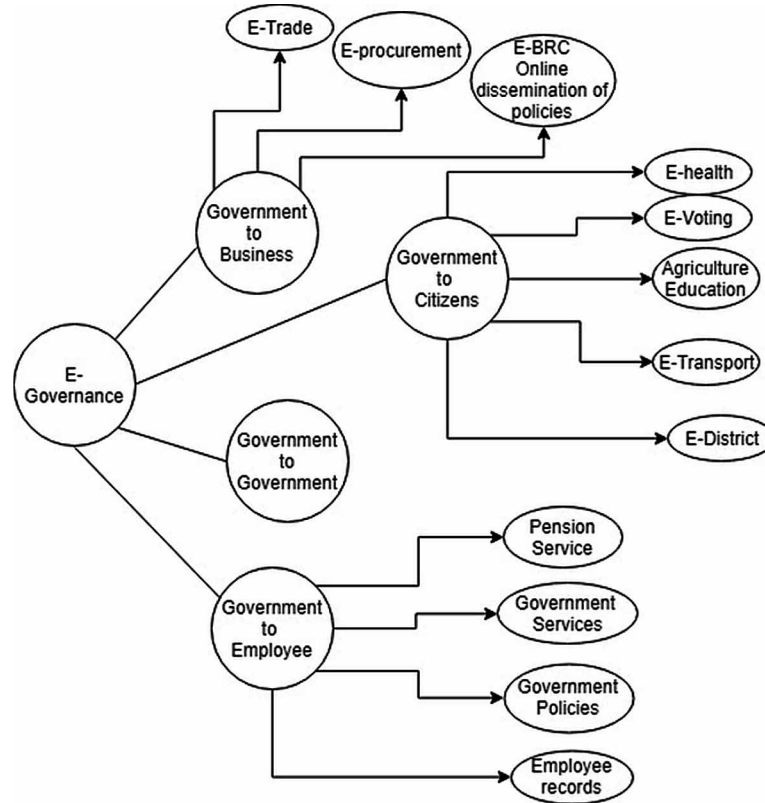
E-Governance

The E-governance called as Electronic governance or Electronic government sometimes can be understood as a collection of new technology tools used to improve the current working scenario of government (Kumar, Manish, and Omesh Prasad Sinha, 2007). E-governance can be treated as publicly representation of the conclusion of governmental interactions, governmental policies, the public services, policy development, service delivery and many more. It is not only restricted towards openness of governmental dataset in front of public, but it also uses adoption of new Information and Communication Technology (ICT) to improve the services, enhance mode of service delivery and include better newer services for the betterment of citizen (Kumar, Manish, and Omesh Prasad Sinha, 2007). This E-governance concept can also be referred to as smart governance, online governance or digital governance.

The E-governance can be applied by governmental administrative, legislative or judiciary departments to improve the current process and efficiency. Based upon the bodies who are connected with governmental dataset, E-governance model can be classified into 4 categories: Government to Government (G2G), Government to Business (G2B), Government to Customer (G2C) and Government to Employees (G2E) (Kumar, Manish, and Omesh Prasad Sinha, 2007). As our aim is to discuss Internet based governmental services, but before that consider the list of some of non-internet (offline) governmental services and technologies as, Fax, SMS (Short Message Service), MMS (Multimedia Messaging Service), Telephone, Biometric, Identity cards, voting system, CCTV (Closed Circuit Television), RFID (Radio Frequency Identification), Smart cards, Bluetooth, email, Tracking system, radio, newsgroups and many more (Kumar, manish, and omesh prasad sinha, 2007). there is a strong need to implement these services in some better way to fulfil the dream of e-governance.

Figure 8. E-Governance model

Source: (E-SPIN, 2017)



There is a one important subset of e-governance and that is m-governance (kumar, manish, and omesh prasad sinha, 2007). in case of m-governance, the use of governmental services is restricted with mobile phones or wireless cellular devices instead of ict. with the advent of usage of mobile phone devices, m-governance found its wide spread popularity by helping general public by providing governmental services and information available anywhere and anytime. the citizens will be benefitted as their energy and valuable time will get saved by accessing the needed service using the device connected with internet. consider the example set by developing country malaysia by adopting e-governance and m-governance (kumar, manish, and omesh prasad sinha, 2007). in malaysia, citizens can verify their voting card related details including parliament and place where they have to vote by sitting at a very long distance by using ict or sms service. their citizens are also permitted to access a real time information or any latest governmental figures with the one click. in california also, their government had designed service for their users, where after registering, their users can get traffic updates, lottery result details, any governmental notification, any new services, any governmental articles etc (kumar, manish, and omesh prasad sinha, 2007). e-governance not only came as blessing to get efficient service, but it also makes active citizens by their continuous involvement into governmental policies. in philippines also, one can take benefit by using anti-pollution service to complaint against person smoking in public transport, to avoid illegal drugs, to fight against crime etc (kumar, manish, and omesh prasad sinha, 2007).

Critical Issues With E-Governance

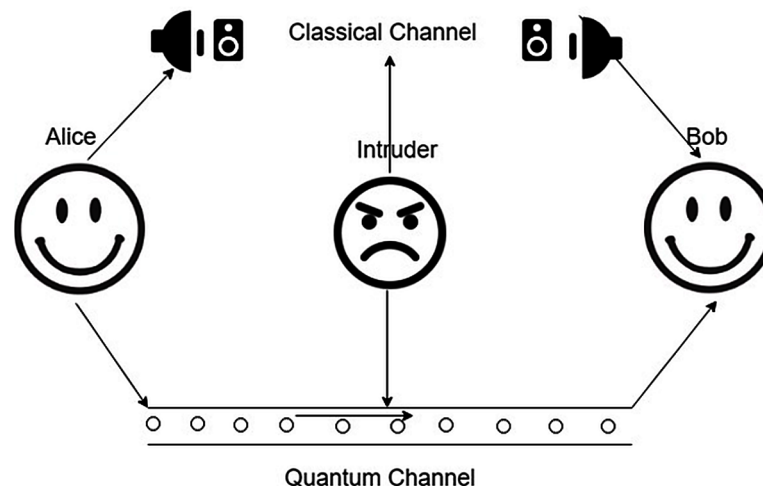
As everyone trying to inject traffic over internet, there is a threat of inception. some unethical persons (hackers) may try to spy over wireless networks to scan e-mail contents, documents and any other confidential information (kumar, manish, and omesh prasad sinha, 2007). as wireless networks use public airways to transmit the signals, which are vulnerable. to transmit confidential data over network, it must be strongly encrypted and key to decrypt that message must also be securely exchanged. even though classical encryption technique is already available and worked satisfactorily till date. but, because of the development of powerful computing platform capable of resolving mathematical based encryption using classical encryption, that strategy becomes vulnerable. quantum compute with its tremendous computing power, can resolve decryption key quickly by applying all possible combination of keys. in order to get access over 802.11b networks, specific type of programs have been developed and available, working using the wired equivalent privacy (wep) encryption system (kumar, manish, and omesh prasad sinha, 2007). there are also tools namely wepckrack and airtsnort are available that are used to grab the password and other confidential information.

Quantum Cryptography – The Solution

Quantum cryptography is the mechanism of using properties of quantum mechanics to perform encryption tasks. the best thing to justify secureness of quantum cryptography is its quantum key distribution (qkd) which offers secure solution to the classical key exchange problem (paolo comi, 2018). the advantage of quantum cryptography can be understood by the fact that the security related solutions which are possible by using quantum cryptography that are proven impossible by using classical cryptography (paolo comi, 2018). because of qubits instead of numerical bit and due to entanglement, no cloning principle and qkd, quantum cryptography recognized to be secured. quantum cryptography, by extension, simply uses the principles of quantum mechanics to encrypt data and transmit it in a way that cannot be hacked. figure 9 depicted difference between classical encryption and quantum encryption.

Figure 9. Classical encryption vs quantum encryption

Source: (Nils Jacob Sand, 2018)



Quantum Internet and E-Governance

Though at a very first glance, definition looks simpler, but the complex parts that have to be taken care behind the principle of quantum cryptography are as (Quantum XC, 2019):

- The particle through which data gets transmitted called as qubits makes the universe uncertain by being in more than one state simultaneously and can also be transmitted simultaneously.
- Photons are generated randomly in one of two quantum states.
- Nobody is permitted to change or read the property of quantum bits without affecting or altering it.
- It is possible to clone some quantum property, but cloning the entire quantum is not possible.

The mathematical equation and large size of key requires larger amount of time like months or years to break and determine the actual message. However, because if powerful Shor's algorithm running behind quantum computer make it to break that encryption in moments. Instead of using encryption by applying mathematical formula, quantum cryptography uses quantum mechanics which makes them non vulnerable and secured from hackers. Quantum cryptography along with quantum key distribution (QKD), makes use of photons to transmit the data from one location to another over a fiber optic cable. In order to understand this process in better way, it is good to break it down in smaller steps (Quantum XC, 2019):

- After transmitting photons randomly through filter, it can provide one of four divergences and bit designations including Vertical (One bit), Horizontal (Zero bit), 45 degrees right (One bit), or 45 degrees left (Zero bit).
- While travelling to a receiver, the photons uses either horizontal/vertical and diagonal beam splitters, to read the polarization of every photon. But, as the receiver does not know from that two beam splitters, which one to use. Thus, it has to guess from available two which is to be used.
- After receiving the beam splitters, the receiver tells the sender which beam splitter was used for every single photon sent in the sequence by sender. Then after sender compares that received information with the sequence of polarization used to transmit the key. After comparison, the photons which found with wrong beam splitter are discarded. The remaining sequence of bits can be treated as key.
- The eavesdropper who tries to read or copy the photon, that photon's state will get changed. This changes will get immediately detected by the endpoint. In other words, without getting detected, one will not be able to read or copy the photon.

CONCLUSION AND FURTHER RESEARCH DIRECTIONS

The evolution of quantum computer brings high computing power which will be capable enough to compute any key of classical cryptography algorithms. As a part of this challenge, quantum cryptography brings revolutionary approach in cryptography. It solves the key exchange issue as with classical cryptography, by using quantum key exchange mechanism. Our government is also turning into e-governance by keeping records of every governmental department. The security issues associated with e-governance can also be resolved by using quantum cryptography. This quantum cryptography can be considered as pioneer of new and secure network architecture. Chapter presented all the components required for quantum internet and cryptography approaches and challenges to overcome. In future, it would be interesting to

create test-bed of quantum networks and test all the mechanisms of cryptography for the challenges posed in the Chapter. Further, it would pave the way to have quantum cryptography in all IT based systems to have robust mechanisms as far as the security is concerned.

REFERENCES

- Ananthaswamy, A. (2019). *The Quantum Internet Is Emerging, One Experiment at a Time*. Scientific American. Retrieved from <https://www.scientificamerican.com/article/the-quantum-internet-is-emerging-one-experiment-at-a-time/>
- Caleffi, M., & Cacciapuoti, A. S. (2019). Quantum Switch for the Quantum Internet: Noiseless Communications through Noisy Channels.
- Castelvecchi, D. (2018). *Here's what the quantum internet has in store*. Nature. Retrieved from <https://www.nature.com/articles/d41586-018-07129-y>
- Chen, S. (2017). *Quantum Internet Is 13 Years Away. Wait, What's Quantum Internet?* Wired; Retrieved from wired.com/story/quantum-internet-is-13-years-away-wait-whats-quantum-internet/
- Choucair, M. (2016). *All you need for quantum computing at room temperature is some mothballs*. Phys.org. Retrieved from <https://phys.org/news/2016-07-quantum-room-temperature-mothballs.html>
- Comi, P. (2018). *Integration of classic cryptography with QKD*. Italtel. Retrieved from <https://www.italtel.com/focus-integration-of-classic-cryptography-with-qkd/>
- Critchley, L. (2018). *What are Quantum Networks?* AZO Quantum. Retrieved from <https://www.azo-quantum.com/Article.aspx?ArticleID=96>
- Das, S. R., & Chandrashekhar, R. (2007). Capacity-Building for e-Governance in India. *Regional Development Dialogue*, 27(2), 75.
- Dubbeldam, J. (2019). *The quantum Internet - A glimpse into the future*. Network Pages. Retrieved from <https://www.networkpages.nl/the-quantum-internet-a-glimpse-into-the-future/>
- E-SPIN. (2017). *Definition and type of E-government*. Retrieved from <https://www.e-spincorp.com/definition-and-type-of-e-government/>
- Faraj, S. T., & Ali, M. S. (2011). Enhancement of E-Government Security Based on Quantum Cryptography. In *Proceeding of the International Arab Conference on Information Technology (ACIT'2011)* (pp. 11-14). Academic Press.
- Kimble, H.J. (2008). The quantum internet. *Nature*, 453(7198), 1023–1030. doi:10.1038/nature07127 PMID:18563153

Quantum Internet and E-Governance

Korolov, M. & Drinkwater, D. (2019). *What is quantum cryptography? It's no silver bullet, but could improve security*. CSO Online. Retrieved from <https://www.csoonline.com/article/3235970/what-is-quantum-cryptography-it-s-no-silver-bullet-but-could-improve-security.html>

Kumar, M., & Sinha, O. P. (2007). M-government–mobile technology for e-government. In *Proceedings of the International conference on e-government* (pp. 294-301). Academic Press.

Lopez-Leyva, J., Talamantes-Alvarez, A., Ponce-Camacho, M., Garcia, E., & Alvarez-Guzman, E. (2018). *Free-Space-Optical Quantum Key Distribution Systems: Challenges and Trends*. In *Quantum Cryptography*. IntechOpen. Retrieved September 30, 2019 from <https://www.intechopen.com/books/quantum-cryptography-in-advanced-networks/free-space-optical-quantum-key-distribution-systems-challenges-and-trends>

Monojlovic, V. (2017). *Introduction to the Quantum Internet*. Retrieved from <https://labs.ripe.net/Members/becha/introduction-to-the-quantum-internet>

Ortiz, J., Sadovsky, A., & Russakovsky, O. (2004). *Modern Cryptography: Theory and Applications*. Retrieved from <https://cs.stanford.edu/people/eroberts/courses/soco/projects/2004-05/cryptography/quantum.html>

Quantum XC. (2019). *What is Trusted Node Technology, and Why Does It Matter?* Retrieved from <https://quantumxc.com/what-is-trusted-node-technology-and-why-does-it-matter/>

Quantum XC. (2019). *Quantum Cryptography, Explained*. Retrieved from <https://quantumxc.com/quantum-cryptography-explained/>

Quantum Cryptography by Brilliant.org (2019). *Quantum Cryptography*. Retrieved from <https://brilliant.org/wiki/quantum-cryptography/>

Quantum-Safe Security Working Group. (2015). *What is Quantum Key Distribution?* Retrieved from <https://www.quintessencelabs.com/wp-content/uploads/2015/08/CSA-What-is-Quantum-Key-Distribution-QKD-1.pdf>

Sand, N.J. (2018). *Introduction to Quantum Cryptography*. Norwegian Creations. Retrieved from <https://www.norwegiancreations.com/2018/11/introduction-to-quantum-cryptography/>

ScienceDaily. (2019). *Quantum Computer*. Retrieved from https://www.sciencedaily.com/terms/quantum_computer.htm

Sharma, A. (2018). *The Quantum Internet Is Still A Futuristic Dream, At Least A Decade Away*. Analytics India Mag. Retrieved from <https://www.analyticsindiamag.com/the-quantum-internet-is-still-a-futuristic-dream-at-least-a-decade-away/>

Wehner, S., Elkouss, D., & Hanson, R. (2018). Quantum internet: A vision for the road ahead. *Science*, 362(6412).

Woodford, C. (2019). *Quantum computing*. Explain That Stuff. Retrieved from <https://www.explainthatstuff.com/quantum-computing.html>

Zhao, Y., Cao, Y., Yu, X., & Zhang, J. (2018). *Quantum Key Distribution (QKD) over Software-Defined Optical Networks*. IntechOpen. Retrieved from <https://www.intechopen.com/books/quantum-cryptography-in-advanced-networks/quantum-key-distribution-qkd-over-software-defined-optical-networks>

Zyga, L. (2018). *New quantum repeater paves the way for long-distance big quantum data transmission*. Phys.org. Retrieved from <https://phys.org/news/2018-02-quantum-paves-long-distance-big-transmission.html>

This research was previously published in Quantum Cryptography and the Future of Cyber Security; pages 109-132, copyright year 2020 by Information Science Reference (an imprint of IGI Global).

Chapter 11

Post-Quantum Cryptography and Quantum Cloning

Amandeep Singh Bhatia

Center for Quantum Computing, Peng Cheng Laboratory, China

Shenggen Zheng

Center for Quantum Computing, Peng Cheng Laboratory, China

ABSTRACT

In the last two decades, the field of post-quantum cryptography has had an overwhelming response among research communities. The ability of quantum computers to factorize large numbers could break many of well-known RSA cryptosystem and discrete log-based cryptosystem. Thus, post-quantum cryptography offers secure alternatives which are implemented on classical computers and is secure against attacks by quantum computers. The significant benefits of post-quantum cryptosystems are that they can be executed quickly and efficiently on desktops, smartphones, and the Internet of Things (IoTs) after some minor software updates. The main objective of this chapter is to give an outline of major developments in privacy protectors to reply to the forthcoming threats caused by quantum systems. In this chapter, we have presented crucial classes of cryptographic systems to resist attacks by classical and quantum computers. Furthermore, a review of different classes of quantum cloning is presented.

INTRODUCTION

In cryptography, several public-key cryptosystems are based on hard problems (not easily tractable on classical computers) such as discrete logarithms and integer factorization. Over the years, number of cryptography algorithms have been introduced and played a crucial role in cybersecurity such as Rivest-Shamir-Adleman (RSA) cryptosystem, Diffie-Hellman key exchange, elliptic curve cryptosystems (ECC) and digital signature algorithm (DSA). Nowadays, quantum computing is an exceptionally hot area of research. The era of quantum computing is nearly upon us, and quantum computers will be able to perform certain operations more quickly and efficiently than classical ones. It is based on quantum mechanical principles of superposition and entanglement. Feynman (1982) stated that the simulation

DOI: 10.4018/978-1-7998-8593-1.ch011

of quantum mechanics was performed on a classical computer. Initially, it was thought to be only a theoretical interest, but now the race to develop a truly useful quantum computer is on among major IT companies and research communities.

Shor (1994) developed a polynomial quantum algorithm which can solve the above intractable problems easily on a quantum computer. As the rapid advancement in quantum computers is catching up, Shor’s factorization algorithm will completely end the RSA encryption. It takes $O(\log n)$ space complexity and $O(\log n)^2 \cdot \log \log n$ time on a quantum computer and $O(\log n)$ time on a classical computer to find factors of a large number n . Therefore, current popular public-key cryptosystems can be attacked in polynomial time. Bernstein (2009) shows the status of several present public-key cryptosystems, given in Table 1.

Table 1. The present status of public-key cryptosystems

Cryptosystems	Cracked by Quantum algorithms?
Diffie-Hellman key-exchange by Diffie and Hellman (1976)	Yes
McEliece public-key encryption by McEliece (1978)	No
Algebraically Homomorphic by Rivest et al. (1978)	Yes
RSA public-key encryption by Rivest et al. (1978)	Yes
Algebraically Homomorphic by Rivest et al. (1978)	Yes
Elliptic curve cryptography by Koblitz (1987)	Yes
Buchmann-Williams key-exchange by Buchmann and Williams (1988)	Yes
Lattice-based public-key encryption by Cai and Cusick (1998)	No
NTRU public-key encryption by Hoffstein et al. (1998)	No

Till now, various public-key cryptosystems have been introduced to reply to security concerns with quantum systems in the post-quantum era. Post-quantum cryptography provides secure substitutes. The objective is to unfold different public-key cryptosystems, which can be adaptable to present communication networks and resist the attacks by both classical and quantum computers. Besides, RSA, DSA, and Elliptic curve digital signature algorithm (ECDSA), there exist several crucial classes of cryptographic systems which consist of code-based, hash-based, lattice-based, and multivariate-quadratic-equations. Indeed, Shor’s algorithm has not been employed in these classes yet.

Although there exist several challenges for the implementation of the post-quantum algorithms. The requirement is to expand the effectiveness and make practicable these algorithms. Secondly, the time is required to get assuredness in post-quantum algorithms. Recently, Bhatia and Kumar (2019) mentioned that these challenges need to be focused before shifting completely to the post-quantum era. In this chapter, the details of different post-quantum cryptosystems to resist completely every attack are given. Moreover, the various classes of quantum cloning are described.

Basic Notations

In this section, some basic notations and terminologies are given, which will be used in the rest of this chapter.

Post-Quantum Cryptography and Quantum Cloning

- **Hamming Distance:** A Hamming distance $d_H(x, y)$ is the number of positions in which two codewords (x, y) differ. Let C be a $[n, k]$ linear code over F_q^n and $x = (x_1, x_2, \dots, x_n), y = (y_1, y_2, \dots, y_n)$ are codewords by Löndahl et al. (2016).

$$d_H(x, y) = |\{i: x_i \neq y_i, 1 \leq i \leq n\}| \quad (1)$$

- **Hamming Weight:** A Hamming weight $wt_H(x)$ is defined as the number of non-zero positions in the codeword x . Let C be a $[n, k]$ linear code over F_q^n and $x = (x_1, x_2, \dots, x_n)$ is a codeword by Löndahl et al. (2016), such that

$$wt_H(x) = |\{i: x_i \neq 0, 1 \leq i \leq n\}| \quad (2)$$

- **Generator Matrix:** A generator matrix for C is a $k \times n$ matrix G having the vectors of $V = (v_1, v_2, \dots, v_k)$ as rows, which forms a basis of C such that

$$C = \{mG : m \in F_q^k\}, G = \begin{bmatrix} v_1 \\ v_2 \\ \dots \\ v_k \end{bmatrix} \quad (3)$$

The matrix G generates the code as a linear map: for each message $m \in F_q^k$, the corresponding codeword mG is obtained by Bhatia and Kumar (2019).

- **Parity Matrix:** A $(n-k) \times n$ generator matrix H is called a parity-check matrix for codeword C defined by Löndahl et al. (2016), which is described by

$$C = \{m \in F_q^n : mH^T = 0\} \quad (4)$$

- **Lattice (L):** It is defined as a set of all integer combinations of linearly independent vectors (a_1, a_2, \dots, a_n) of length n in R^n , which are called basis in a lattice by Peikert (2016).

$$L(a_1, a_2, \dots, a_n) = \left\{ \sum_{i=1}^n x_i a_i \mid x_i \in Z \right\} \quad (5)$$

It can be represented in matrix form such that $A = (a_1, a_2, \dots, a_n) \in R^{n \times n}$, columns act as basis vectors.

- **Polynomial Ring:** Let R be a commutative ring, then

$$R[x] = \{a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0\},$$

is called the ring of polynomials over R in the intermediate x , where x is the set of polynomials with a_0, a_1, \dots, a_n coefficients and $n \in \mathbb{Z}$ and defined by Buchmann (2013).

CODE-BASED CRYPTOGRAPHY

Code-based cryptography refers to the study of public-key cryptosystems based on error-correcting codes to resist the attacks by quantum computers. It is among the most popular post-quantum algorithms. The error code is added intentionally to a message and syndrome is computed corresponding to the parity matrix of a code. The main public-key code-based cryptosystems are McEliece and Niederreiter. These algorithms provide a significant trade-off between security and efficiency.

McEliece Cryptosystem

In the 1950s, the concept of Golay code was proposed and has got an overwhelming response in the last two decades. Based on extended binary Golay code [24, 12, 8], McEliece cryptosystem provides a unique way to encode 12 bits of data into 24-bit long word and can correct up to 3 bits of error. A public-key cryptosystem based on binary Goppa codes is developed by McEliece (1978). It is one of the oldest asymmetric encryption algorithms and considered to be post-quantum secure. The security of McEliece cryptosystem depends upon the decoding algorithm to decode the linear block of code unknowing the internal structure.

Till now, several modified variants of the original McEliece cryptosystem were introduced on the basis of a family of error-correcting codes such as Reed-Muller codes, Reed-Solomon codes, sub-codes of Reed-Solomon codes, Gabidulin codes, concatenated codes, and convolutional codes. The McEliece cryptosystem based on the concept of extended Golay code is proposed, and its security is analyzed by Bhatia and Kumar (2018). The description of the original McEliece cryptosystem algorithm is given in Table 2. The working of McEliece public-key cryptosystem is shown in Figure 1.

Sendrier (1998) mentioned that the original McEliece algorithm is unbroken today no doubt. But, there are some of its disadvantages. It is not symmetric in nature. The size of the key is large, which can influence its execution process. The transmission rate is also very low. Due to the enlarging bandwidth size, the implementation can be exposed to errors.

Security

The McEliece algorithm is observed to be fully secure based on decoding algorithm and rigorous search on key. There exist two types of attacks, namely decoding and structural attacks on original McEliece public-key cryptosystem:

Figure 1. Encryption and decryption process of a McEliece public-key cryptosystem

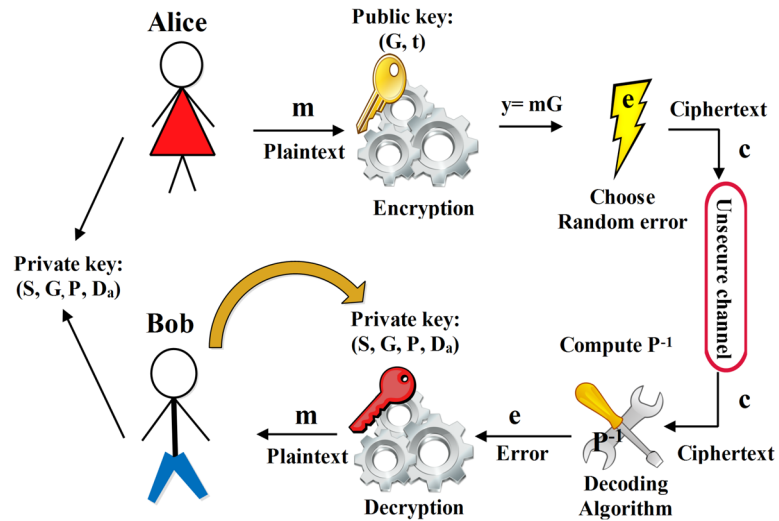


Table 2. McEliece public-key cryptosystem

The McEliece cryptosystem is defined as a triple (KeyCr, Encr, Decr):
Key Creation (KeyCr)
<ul style="list-style-type: none"> • Choose a random $[n, k, 2t+1]$ decodable linear code C. • Compute the matrix $(k \times n) G' = SG$, where G is $(k \times n)$ generator matrix, S $(k \times k)$ and P $(n \times n)$ are randomly chosen non-singular and permutation matrix respectively. • The private key: (S, G, P, D_a) and public key: (G', t).
Encryption (Encr)
<ul style="list-style-type: none"> • Select a random vector $c \in \{0,1\}^n$ consists of exactly t ones. • Encrypt the k-length message $m \in \{0,1\}^k$. Finally, compute the ciphertext $c = mG' + e$.
Decryption (Decr)
<ul style="list-style-type: none"> • The inverse of the permutation matrix P^{-1} is computed. • Compute $cP^{-1} = mSG + eP^{-1}$. • An efficient decoding algorithm (D_a) is used to decrypt $c_1 = cP^{-1}$ to m. • Retrieve the original message $m = m'S^{-1}$.

1. Decoding attacks

As the name suggests, the attack consists of decrypting the ciphertext. In case, it becomes successful; then the plaintext can be retrieved easily. Loidreau (2000) has determined that on considering 1024-length of code, the requirement is to compute total 2^{64} binary operations for decoding ciphertext in addition to 524 key-size and 50 error-correcting capability. Hence, as the computational power grows, the original McEliece cryptosystem will not remain secure.

2. Structural attacks

The main attempt in structural attacks is to recreate the definite form of code from the public key. It is easy to retrieve the private key after the successful structural attack, which results in broken of the complete cryptosystem. On considering 1024-length of code, the need is to scan 2^{466} codes with 524-key size and 50 error-correcting capability. The internal structure of generator matrix G after the attack on the original McEliece cryptosystem was revealed by Loidreau and Sendrier (2001). So far, several structural attacks have been tried on different versions of McEliece cryptosystem.

Niederreiter Cryptosystem

In 1986, Niederreiter introduced the public-key cryptosystem based on Reed-Solomon codes. From a security perspective, it is similar to McEliece cryptosystem. The only difference lies in the illustration of codes, where McEliece uses a generator matrix, and Niederreiter utilizes a parity check matrix. Sidelnikov et al. (1992) proved that Niederreiter cryptosystem is insecure with Goppa and Reed-Solomon codes. Till now, several researchers tried to reduce the size of the public key of original McEliece cryptosystem. But, all existing variants remain ineffective and insecure on comparison with McEliece public-key cryptosystem. The description of Niederreiter cryptosystem is given in Table 3.

Table 3. Niederreiter cryptosystem

The Niederreiter cryptosystem is defined as a triple (KeyCr, Encr, Decr):
Key Creation (KeyCr)
<ul style="list-style-type: none"> Choose a random $[n, k, 2t+1]$ decodable linear code C. Compute the matrix $(n-k) \times n \ H^1 = SHP$, where H is $(n-k) \times n$ parity-check matrix, S $(n-k) \times (n-k)$ and P $(n \times n)$ are randomly chosen a binary non-singular matrix and permutation matrix respectively. The Private key: (S, H, P, D) and public key: (H^1, t)
Encryption (Encr)
<ul style="list-style-type: none"> Encrypt the k-length message $m \in \{0,1\}^k$ of weight t, compute the ciphertext $c = mH^{1T}$.
Decryption (Decr)
<ul style="list-style-type: none"> The inverse of non-singular matrix S^{-1} is computed. Compute $S^{-1}c^T = HPm^T$ Find a vector (v) such that $Hv^T = HPm^T$ Employ an efficient decoding algorithm D_a on v to retrieve the original message m.

In Niederreiter cryptosystem, the plaintext m is demonstrated as an error of C rather than the original word. Besides, the decoding of code can be implemented more efficiently as compared to original McEliece cryptosystem. It can be noted that the generator matrix can be easily calculated from the party matrix and vice versa. Therefore, McEliece and Niederreiter cryptosystems are dual to each other. Niederreiter cryptosystem is useful to represent a digital signature scheme.

LATTICE-BASED CRYPTOGRAPHY

The construction of lattice-based cryptosystems holds strong security proofs on the basis of worst-case resistance of lattice problems, which offers efficient execution and simplicity. Moreover, such cryptosystems are reliable and secure against the attacks of quantum computers. Basically, a lattice representing arbitrary basis is given as input and expected the output to be the shortest non-zero vector. The concept of lattice-based cryptosystem for the shortest vector problems is proposed by Lenstra et al. (1993). It runs in polynomial time. It is the most extensively studied algorithm for lattice problems, but later on, its various extensions have been introduced. The main lattice-based cryptosystems are described that have been introduced so far. Begin with the NTRU cryptosystem, which is the most well-known practically implemented lattice-based encryption scheme till now.

NTRU Algorithm

Hoffstein, Pipher, and Silverman (1998) proposed ring-based public-key cryptosystem. Since the NTRU algorithm is introduced, numerous researchers tried to enhance its security and to speed up the procedure. It contains q -ary sub lattices which are closed under linear modification. Furthermore the different attacks attempted to find the private key instead of retrieving the original message. So far, several variants have been introduced and evaluated on the basis of selected variables. The description of NTRU algorithm is given in Table 4.

The decryption of NTRU algorithm can be executed successfully, if the selected parameters (n, p, q, d) satisfy that $q > (6d+1)p$. It has been demonstrated that NTRU algorithm can be implemented efficiently in hardware and software by Bu and Zhou (2009) and Hoffstein, Pipher and Silverman (1998). In NTRU, the less memory is needed, and keys can be produced quickly. Therefore, it can be practically implemented for devices with less memory, for example, mobile phones and smart cards (integrated circuits).

On comparing with the most popular public-key cryptosystems ECC and RSA, the NTRU algorithm is effective and secure. Several attacks are attempted on NTRU algorithms such as alternate secret keys, simultaneously transmission attack and brute force attack to decode the original message m . Thus, NTRU takes less time as compared to RSA and ECC and more time as compared to McEliece public-key cryptosystem for key creation, encryption, and decryption process.

Goldreich-Goldwasser-Halevi (GGH)

It is the most instinctive encryption scheme based on lattices. There exist many components of GGH encryption scheme in other lattice-based cryptosystems, but original GGH is practical, which offers simplicity. Goldreich, Goldwasser, and Halevi (1997) introduced lattice equivalent of McEliece cryptosystem in which short orthogonal vectors used as a private key. It acts as a good lattice basis. Till now, asymptotically good attack to GGH public encryption scheme is not identified because the security and correctness depend upon the selection of private basis and error vector. It is based on solving the problem "Close vector problem (CVP)" in a lattice, i.e., finds the lattice point closest to a given vector. As compared to RSA, Diffie-Hellman, and ElGamal, it offers high performance due to simple matrix operations.

Table 4. NTRU cryptosystem

Public Parameters
<ul style="list-style-type: none"> Operations are formed on objects in a polynomial ring (R) that is truncated having coefficients to a certain degree such that $R=Z[X]/(X^N - 1)$. Choose two moduli p and q relatively prime in R. The moduli q is smaller than N and p is smaller than q such that $\gcd(p,q) = 1$.
<ul style="list-style-type: none"> Additional parameters, d_f is set of polynomial in R having exactly d -1's and $(d+1)$ 1's; d_s and d_r is set of polynomials in R having exactly similar d -1's and d 1's and d_m is set of polynomials in R_p such that coefficients are in between $-1/2(p+1)$ and $1/2(p+1)$.
Key Creation
<ul style="list-style-type: none"> Choose a random $\hat{f}d_f$ and invertible in $R=Z[X]/(X^N - 1) \bmod p$ and q. In case, if does not satisfy, then new random f is selected.
<ul style="list-style-type: none"> Compute the inverse of $f \bmod p$ and $f \bmod q$ such that $f_q^{-1} \cdot f \equiv 1 \bmod q$ and $f_p^{-1} \star f \equiv 1 \bmod p$.
<ul style="list-style-type: none"> Hence, the pair (f, f_q^{-1}) is a private key.
<ul style="list-style-type: none"> For the public key h, compute the polynomial $h = f_q^{-1} \star g(\bmod q)$.
Encryption
<ul style="list-style-type: none"> Select a polynomial randomly $\hat{r}d_r$.
<ul style="list-style-type: none"> Select a message $\hat{m}d_m$.
<ul style="list-style-type: none"> Calculate the ciphertext (c): $c = pr \star h + m \pmod{q}$.
Decryption
<ul style="list-style-type: none"> Evaluate a polynomial a using private key polynomial such that $a = f \star c \pmod{q}$.
<ul style="list-style-type: none"> Calculate $b=a(\bmod q)$ and reduces each of the coefficients of $b \bmod p$.
<ul style="list-style-type: none"> Determine $z = f_p^{-1} \star b \pmod{p}$ by using private key polynomial f_p^{-1} to get the original message m.

The security of GGH cryptosystem depends upon selecting a suitable perturbation vector r . If it is selected very small, then the closest vector v can be easily retrieved without any difficulty. If it is selected very large, then it may be not possible to decrypt using the private key. Hence, the perturbation vector r must be chosen balanced, i.e., relatively small as compared to the vectors in public key W . Following are the advantages of lattice-based cryptography: Till now, any quantum attacks do not exist to break lattice-based cryptosystems. It is one of chief substitute for post-quantum cryptosystems. Nguyen and Regev (2009) analyzed that lattice-based cryptosystems are not employed much yet due to security reasons. NTRU is efficient in implementation but lack of security.

Nguyen and Regev (2009) shown the imperfection in design of GGH cryptosystem. The challenges in the execution of GGH are solved and came with partial information about the lattice. No doubt, GGH cryptosystem offers security with a suitable selection of parameters. But, on selecting the high dimension of lattice, it provides great improvement. Although the key size increases quadratically. Micciancio (2001) demonstrated that GGH cryptosystem promises security if the lattice dimension is larger than 350.

Table 5. GGH cryptosystem

Construction of Keys
<ul style="list-style-type: none"> For private key: Choose a full-column rank integer matrix V such that columns are orthogonal to each other.
$V = [v_1, v_2, v_3, \dots, v_n], v_j \in Z^n, 1 \leq j \leq n$
<ul style="list-style-type: none"> Select a random $n \times n$ unimodular matrix (U), such that $\det(U) = \pm 1$.
<ul style="list-style-type: none"> For public key: compute a matrix $W = VU$.
Encryption
<ul style="list-style-type: none"> Choose a perturbation vector r, i.e., acts as an ephemeral key
<ul style="list-style-type: none"> Select a plaintext message m of the same dimension, belongs to a lattice.
<ul style="list-style-type: none"> Encrypt the message m using public key W and ephemeral key r, compute the ciphertext
$c = Wm + r$
Decryption
<ul style="list-style-type: none"> Decrypt the closest vector v belongs to a lattice of ciphertext (c) using private key V and any decoding algorithm.
<ul style="list-style-type: none"> Compute the inverse of V to decrypt the ciphertext such that $x = c \cdot V^{-1}$.
<ul style="list-style-type: none"> Then, retrieve the original message m by multiplying with the inverse of a unimodular matrix such as $m = x \cdot U^{-1}$. At the end, its correctness can be checked by differentiating m with hashed value.

MULTIVARIATE CRYPTOGRAPHY

Over finite fields, Multivariate cryptosystems are based on non-linear equations that are difficult to solve. Thus, it is said to be very light-weight cryptography which is effective and efficient to be employed in embedded devices (microcontrollers). The security of multivariate cryptosystems is based on the NP-hardness of the problem. In the last two decades, an enormous development occurs in multivariate cryptography. It is defined as the study of public-key cryptosystem (Diffie and Hellman) in which one-way trapdoor function is based on the mapping of multivariate quadratic equations. There exist several multivariate public-key cryptography schemes such as Oil and vinegar signature scheme by Patarin (1997), Quartz signature scheme (2, 129, 103, 3, 4) by Patarin et al. (2001), and Rainbow signature scheme (2⁸, 18, 12, 12) by Ding and Schmidt (2005). These multivariate public key encryption algorithms are developed in several ways and all have their own benefits and drawbacks. It can also be called as trapdoor multivariate quadratic because most of the schemes are constructed using higher-order quadratic polynomial equations. Generally, the public key is a set of quadratic polynomials over a finite field

$$\begin{aligned}
 p_1(x_1, \dots, x_n) &= \sum_{1 \leq i < j \leq n} a_{ij}^1 x_i x_j + \sum_{1 \leq i \leq n} b_i^1 x_i + c^1 \\
 p_2(x_1, \dots, x_n) &= \sum_{1 \leq i < j \leq n} a_{ij}^2 x_i x_j + \sum_{1 \leq i \leq n} b_i^2 x_i + c^2 \\
 &\vdots \\
 p_m(x_1, \dots, x_n) &= \sum_{1 \leq i < j \leq n} a_{ij}^m x_i x_j + \sum_{1 \leq i \leq n} b_i^m x_i + c^m
 \end{aligned} \tag{6}$$

where p_1, p_2, \dots, p_m are m quadratic polynomials with n variables such as x_1, x_2, \dots, x_n . Chen et al. (2016) investigated that the multivariate public key cryptosystem encrypts the message faster as compared to RSA and ECC. The security depends upon the multivariate quadratic polynomial problem (MQP) where the need is to find a vector $x' = (x'_1, x'_2, \dots, x'_n)$ such that $p_1(x') = \dots = p_m(x') = 0$. It has been demonstrated that such MQP problem is NP-hard over any field (Fraenkel and Yesha, 1979). The following are the multivariate public key cryptosystems:

Oil and Vinegar Signature Scheme (OV)

The first method of multivariate quadratic systems, namely oil and vinegar (OV) signature scheme is introduced by Patarin (1997). The logic behind the name oil and vinegar is that they cannot be blended in terms of quadratic variables.

Let oil (o) and vinegar (v) are two integers, and k be a finite field, such that $n = o + v$. Then, set $O = \{v+1, \dots, n\}$ and $V = \{1, \dots, v\}$, where x_{v+1}, \dots, x_n and x_1, \dots, x_v are oil and vinegar variables, respectively. It was indicated to choose $o=v$, then it is known as balanced OV scheme, if $v > 0$, then it is named as unbalanced OV scheme. The key generation consists a mapping $F: k^{o+v} \rightarrow k^o$ such that o quadratic polynomials is in form

$$f^k(x) = \sum_{i \in V} \sum_{j \in V} a_{ij}^k x_i x_j + \sum_{i \in V} \sum_{j \in O} b_{ij}^k x_i x_j + \sum_{i \in O \cup V} c_i^k x_i + d^k \quad (7)$$

where $x_j, j=1, \dots, o$ and $x_i, i=1, \dots, v$ are oil and vinegar variables and $a_{ij}^k, b_{ij}^k, c_i^k x_i$ and d^k are randomly selected coefficients. It can be noted that mapping $F = (f_{v+1}(x), \dots, f_n(x))$ is simply invertible. Firstly, select vinegar variables randomly. Further, solve the linear equations with o variables by using Gaussian elimination method. If in case, we do not get any solution, then the need is to select vinegar variables again.

Quartz Signature Scheme $(F, d, n, a, v) = (2, 129, 103, 3, 4)$

Patarin et al. (2001) introduced the Quartz signature scheme based on the HFEv-trapdoor function. It was designed to produce very short signatures i.e. of only 128 bits. It has been designed for specific applications. Although, there are already exists several classical algorithms (RSA, ECC, DSA etc) which can generate signatures of length greater than equal to 320 bits. The public and private keys are HFEv that maps with the following parameters: $(F, d, n, a, v) = (GF(2), 129, 103, 3, 4)$, where F represents finite field, d denotes the polynomial degree, n signifies the size of an extended field, a is used to denote the number of removed equations and v signifies the vinegar variables.

In quartz algorithm, the public key (Pu_k) is used which maps quadratic equations from F^{107} to F^{100} and give input $n-a=100$ bits. Firstly, compute four signatures for the messages

$$m_0 = SHA - 1(m), SHA - 1(m_0 || 0x00), SHA - 1(m_0 || 0x01)$$

and $SHA-(m_0\|0x02)$, where SHA stands for secure hash algorithm. Then, combine all of them in to one 128-bit long signature. During its verification, apply public key (Pu_k) four times. Generally, there are two known attacks MinRank proposed by Kipnis and Shamir (1999) and direct algebraic attacks. It has not been used much practically because of slow process of signature generation and production of short signatures.

Rainbow Signature Scheme

$$f^k(x) = \sum_{i \in V_l} \sum_{j \in V_l} a_{ij}^k x_i x_j + \sum_{i \in V_l} \sum_{j \in O_l} b_{ij}^k x_i x_j + \sum_{i \in O_l \cup V_l} c_i^k x_i + d^k \quad (8)$$

where $l \in \{1, 2, \dots, u\}$ such that $k \in O_l$. The steps of rainbow signature scheme's construction are explained as follows:

- **Key Creation:** Public-key contains k and map of the form $P(x) = S_1 \circ F \circ S_2(x)k^n, \rightarrow k^m$ where S_1, S_2 are two invertible or linear maps $S_1: k^m \rightarrow k^m$ and $S_2: k^n \rightarrow k^n$. A private-key contains (F, S_1, S_2) , where $F = (f^{v_1+1}, \dots, f^n)$ is central rainbow map.
- **Signature a Document:** To sign a document d , the need is to observe a solution of an equation

$$S_1 \circ F \circ S_2(x_1, x_2, \dots, x_n) = F'(x_1, x_2, \dots, x_n) = T'$$

On applying inverse of S_1 ,

$$F \circ S_2(x_1, x_2, \dots, x_n) = S_1^{-1}T' = T''$$

The equation is computed recursively to the inverse of F such that

$$F(x_1, x_2, \dots, x_n) = T'' = (y_1'', \dots, y_{n-v_1}'')$$

In the end, apply the inverse of S_2 such that $z = S_2^{-1}(y)$, which gives us the signature T' of document d i.e. $T' \in k^n$.

- **Verification:** To demonstrate the authenticity of signature d , check $F'(x_1', x_2', \dots, x_n') = T'$.

If there is a need to sign a large size document, then apply the hash function and compute the hash value to verify its authenticity. The rainbow signature scheme offers simplicity due to simple matrix operations (multiplication and inversion) over a finite field. It is more efficient than oil and vinegar scheme due to small key and concise signatures in size. Although, there exists several attacks MinRank attack by Kipnis and Shamir (1999) and Rainbow-Band-Separation attack by Fraenkel and Yesha (1979), which find the linear mapping to change the polynomials into quadratic mapping.

HASH-BASED CRYPTOGRAPHY

The security of currently used digital signature algorithms is based on the hardness of factorization of sizeable composite numbers. Such algorithms are not quantum resistant. Therefore, hash-based cryptography is based on the cryptographic hash function. as an alternative solution and its security depends upon the collision resistance of hash function. Hash-based cryptosystems are the prominent candidate of post-quantum cryptography due to their minimal security requirements. There exist various hash-based cryptography schemes which are beneficial for an era of quantum such as Lamport-Diffie one-time signature scheme (LD-OTS) introduced by Lamport (1979), Winternitz one-time signature scheme (W-OTS) by MERkle (1989). These one-time digital signature schemes are not suitable for practical states because every pair of a key can be utilized per signature only. Hence, Merkle defined MERkle's tree authentication scheme based on a complete binary hash tree to lessen the validity of one-time verification keys

Lamport-Diffie One-Time Signature Scheme (LD-OTS)

A one-time signature scheme (LD-OTS) is proposed by Lamport (1979). For security reasons, most of the signature schemes are based on hash functions, whereas the security of Lamport signature scheme is based on one-way functions $f: \{0,1\}^n \rightarrow \{0,1\}^n$ and cryptographic hash function $h: \{0,1\}^n \rightarrow \{0,1\}^n$. The construction of Lamport-Diffie one-time signature scheme is explained as follows:

- **Key Creation:** The signature key (S_k) and verification key (V_k) are selected randomly which consists of $2n$ bit strings of length n such that

$$S_k(x) = \{x_{n-1}[0]x_{n-1}[1], \dots, x_1[0]x_1[1], x_0[0]x_0[1]\} \in \{0,1\}^{(n,2n)} \quad (9)$$

$$V_k(y) = \{y_{n-1}[0]y_{n-1}[1], \dots, y_1[0]y_1[1], y_0[0]y_0[1]\} \in \{0,1\}^{(n,2n)} \quad (10)$$

where $y_j[k]=f(x_j[k])$, for $0 \leq j \leq n-1, k=0,1, \dots$. Thus, key generation needs $2n$ assessments of f .

- **Signature Generation:** Consider a document $d \in \{0,1\}^*$ which is signed by exploiting signature key (S_k). Suppose a message digest be a $g(D) = M\{m_{n-1}, \dots, m_0\}$. Then, its signature becomes

$$\sigma = \{x_{n-1}[d_{n-1}], \dots, x_1[d_1], x_0[d_0]\} \in \{0,1\}^{(n,n)} \quad (11)$$

where σ is group of n bit strings of length n , which are selected as a $f(D)$. So, the length of signature becomes n^2 .

- **Verification:** To verify the signature (σ), the verifier determines the message digest $M = \{m_{n-1}, \dots, m_0\}$. It needs n evaluations of f to check equality such that

$$(f(\sigma_{n-1}), \dots, f(\sigma_0)) = (y_{n-1}[d_{n-1}], \dots, y_0[d_0]) \quad (12)$$

Winternitz One-Time Signature Scheme (W-OTS)

After the introduction of LD-OTS, MERkle has written that Winternitz suggested him the method and named it as Winternitz one-time signature scheme. The main notion is to use a string in (S_k) to sign various bits in message digest at same time. It uses same one-way functions and cryptographic functions like LD-OTS and produces shorter signatures efficiently. The construction of original W-OTS is explained as follows:

- **Key Creation:** Firstly, set the number of bits to be signed at same time i.e. w^2 . Then, compute

$$t_1 = \left\lceil \frac{n}{w} \right\rceil, t_2 = \left\lceil \frac{\lceil \log_2 t_1 \rceil + 1 + w}{w} \right\rceil, t = t_1 + t_2 \quad (13)$$

The signature key (S_k) is selected at random such that

$$S_k(x) = (x_{t-1}, \dots, x_1, x_0) \in \{0, 1\}^{(n,t)} \quad (14)$$

and the verification key (V_k) is computed by applying one-way function $f: \{0, 1\}^n \rightarrow \{0, 1\}^n$, $2^w - 1$ times to each bit string in S_k .

$$V_k(y) = (y_{t-1}, \dots, y_1, y_0) \in \{0, 1\}^{(n,t)} \quad (15)$$

where $y_i = f^{2^w - 1}(x_i)$ for $0 \leq i \leq t-1$.

- **Signature Generation:** Consider a message digest $g(D) = M = (m_{n-1}, \dots, m_0)$ to be signed. In order to divide the message digest d with w , prepend the minimum number of 0's to it. Now, the string d is split into $t-1$ bit strings such that $d = a_{t-1} \parallel \dots \parallel a_{t-t_1}$, where \parallel signifies concatenation of strings and a_i are integers belong to $(0, 1, \dots, 2^w - 1)$. Next, the checksum is computed

$$c = \sum_{i=t-t_1}^{t-1} (2^w - a_i) \quad (16)$$

Then, in order to divide a binary representation by w , prepend a minimum number of 0's, and the string is split into t_2 groups such that

$$c = a_{t_2-1} \parallel \dots \parallel a_0 \quad (17)$$

In the end, the signature is calculated as

$$\sigma = \{f^{a_{t-1}}(x_{t-1}), \dots, f^{a_1}(x_1), f^{a_0}(x_0)\} \tag{18}$$

- **Verification:** In order to verify the signature above, the bit strings a_{t-1}, \dots, a_1, a_0 are computed and check the equality such that

$$(f^{2^w-1-a_{t-1}}(\sigma_{n-1}), \dots, f^{2^w-1-a_0}(\sigma_0)) = (y_{n-1}, \dots, y_0) \tag{19}$$

If the computed signature is logically correct, then, the following equation holds such that

$$f^{2^w-1-a_i}(\sigma_i) = f^{2^w-1}(x_i) = y_i \tag{20}$$

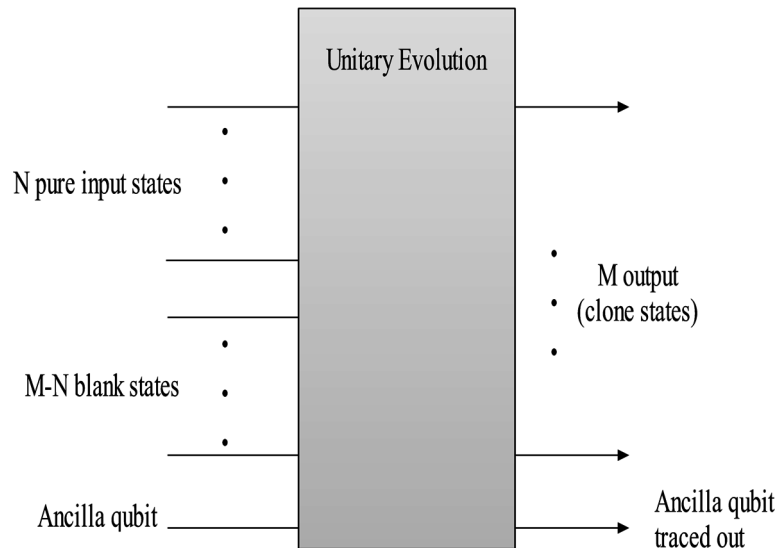
where $i=t-1, \dots, 0$. It needs $t(2^w-1)$ assessment of f in the worst case.

Till now, various generalizations of W-OTS has been occurred, such as W-OTS (used in MAC) and W-OTS⁺ introduced by Hülsing (2013). The main purpose is to upgrade the W-OTS to increase the security and shorten the size of signatures.

QUANTUM CLONING

Until the mid-1990s, the people did not acknowledge the concept of quantum cloning due to no-cloning theorem. The concept of “Universal Quantum Cloning Machine” is introduced by Buzek and Hillery (1996). It generates imperfect copies of a qubit, where the quality of the cloned state is not dependent

Figure 2. $N \otimes M$ deterministic quantum cloning with the ancilla qubit



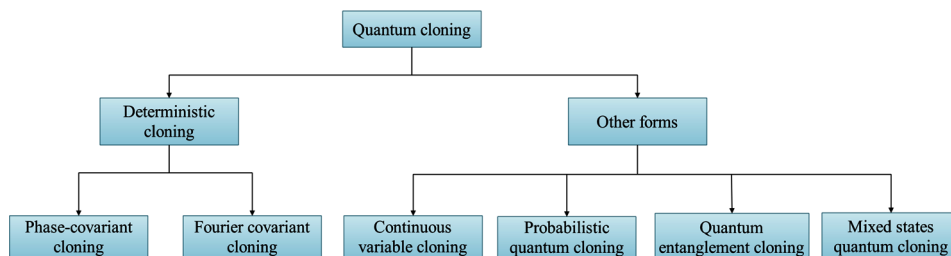
on the input state. The no-cloning theorem states that there is no such quantum operation exists that can exactly produce a priori unknown pure state $|\varphi\rangle$, such that $U|\varphi\rangle|0\rangle = |\varphi\rangle|\varphi\rangle$, i.e., there is no unitary operator exists for pure state $|\varphi\rangle$. The “quantum cloning machines” are crucial to study eavesdropping on quantum cryptosystems and state estimation. There exist several versions of universal quantum cloning, but the main objective is to produce a cloned state of the arbitrary pure state in a finite-dimensional Hilbert space.

In 2005, the deterministic cloning of arbitrary pure states was mapped as a linear trace-preserving completely positive (TPCP). Scarani et al. (2005) indicated that the exchange of quantum information between the systems is intermediate with the ancilla qubit, which can redistribute the information among numerous quantum systems. Thus, the process of deterministic quantum cloning of an input state is investigated as follows:

$$\left(|\varphi\rangle^{\otimes N}\right) \otimes \left(|0\rangle^{\otimes M-N}\right) \otimes |C\rangle \xrightarrow{U} |\Psi\rangle \tag{21}$$

where N denotes the input states and $M-N$ represent the blank copies associated with an ancilla qubit and performs a unitary operator U into the final state. Initially, the universal quantum cloning machine is introduced for optimal $1 \otimes 2$ qubits, which generates two clones from an input state of the same fidelity. Later on, the extended variant for $N \otimes M$ qubits is proposed. If the quality of all output (cloned states) M is equivalent, the quantum machine is referred as symmetric, else asymmetric. The different classes of quantum cloning are shown in Figure 3.

Figure 3. Classification of quantum cloning



State-Dependent Quantum Cloning

When the quality of output (cloned states) is generated by the cloning evolution depends on the input state, the evolution of the cloning process is said to be state-dependent quantum cloning. In fact, the quality of output is produced by state-dependent cloning is better than the universal quantum cloning machine, but at the cost of poor cloning of other states. In state-dependent cloning, it is possible to improve the quality of output cloned states by getting some information about the initial state.

It should be noted that the information about the initial state does not always result in superior cloning. Bruss et al. (1998) stated that the universal quantum cloning machine can be used for the six-state

quantum key distribution protocol. It is stated that it is not possible to produce exact output (clone states) of the six-state protocol using state-dependent cloners. Consider two input states $|\alpha\rangle$ and $|\beta\rangle$, related by $\langle\alpha|\beta\rangle = z$, where z can be 0 or 1. It is investigated that the perfect cloning can be attained for z , and results shown that minimum fidelity ($F=0.987$) is achieved for $z=1/2$. The find the minimum input sets for defining the universal cloning machine is a problem. Jing et al. (2012) explored that the minimum four states on the vertices of the polyhedron are required for cloning $1\otimes 2$ states optimally.

Phase-Covariant Cloning

In phase-covariant cloning, the quality of cloned states is not controlled by phase. Consider a pure state of form

$$|\varphi\rangle = \left(|\varphi\rangle + e^{i\phi} |1\rangle \right) / \sqrt{2} \quad (22)$$

The qubits of such form are equatorial qubits of the Bloch sphere, i.e., the Bloch vector is confined to xy -plane only, and z -component is zero. The parameter $\phi \in [0, 2\pi)$ defines the angle between x -axis and Bloch vector. The output of phase-covariant cloners does not depend upon the value of phase ϕ . It can be symmetric or asymmetric. Fuchs et al. (1997) and Fan et al. (2001) described the major difference with the universal quantum cloning. It has been demonstrated that phase-covariant cloning depends upon global fidelity or single-copy.

Initially, the concept of phase-covariant cloner as an eavesdropping attack on the most popular quantum key distribution protocol BB84 is studied by Fuchs et al. (1997) with respect to single-copy fidelity. The phase-covariant $1\otimes M$ was studied for qubits. Till now, the optimal $1\otimes 2$ phase-covariant cloner for qudits (It can have 10 or more quantum states simultaneously compared to just two for qubits). It has been demonstrated by different researchers Buscemi et al. (2005) and Fan et al. (2003), but the $N\otimes M$ phase-covariant cloner for qudits is not introduced yet. The phase-covariant cloners can be constructed economically without using ancilla qubit.

The economical phase-covariant cloners (symmetric and asymmetric) for a pure state (given in Eq. 22) are introduced by Niu and Griffiths (1999) and compared with the counterparts based on the same fidelity. Fan et al. (2014) stated that the clone states of phase-covariant cloners and economical cloners can be different, even they have the same fidelity. It has been determined on several occasions that state-dependent cloners are superior to the universal quantum cloners. The phase-covariant $1\otimes 3$ quantum clone machines attain $5/6$ fidelity, as similar to $1\otimes 2$ universal quantum clone machines. Although, the third clone with the same fidelity is obtained for equatorial input states.

Fourier-Covariant Cloning

As the name indicates, the covariant evolutions are covariant with regards to a Fourier-transform and clones are mutually unbiased bases to each other. The eigenstates of Pauli matrices are used to produce clones of three qubits mutually unbiased bases. Thus, the phase covariant cloner can be generated with the states of two mutually unbiased bases. In two-dimensional Hilbert space, all pairs of mutually unbiased based are unitarily identical. Hence, Cerf et al. (2006) stated that Fourier-covariant cloner is

Post-Quantum Cryptography and Quantum Cloning

corresponding to phase-covariant cloner. It has been investigated that the fidelity of Fourier-covariant cloner is more than phase-covariant cloner in case of three-level $1 \otimes 2$ qutrit asymmetric cloner. Later on, the $1 \otimes 2$ qutrit cloner is expanded in arbitrary finite dimension by Cerf et al. (2002).

Other Forms

The aforementioned classes of cloning are focusing on cloning of states deterministically. The following are the other forms of quantum cloning.

Continuous-Variable Quantum Cloning

In infinite-dimensional Hilbert space, the continuous-variable quantum cloning is the most studied quantum cloning. Universal quantum cloning machine for coherent states is not widely studied. Initially, Gaussian cloner and produced similar copies of two conjugate variables for $1 \otimes 2$ cloning evolution is presented by Cerf et al. (2000). Till now, the concept of Gaussian continuous-variable cloning has been considered enormously. Further, the fidelity of $N \otimes M$ Gaussian cloner based on coherent states is determined by Cerf et al. (2000). It has been demonstrated that Gaussian cloner can be used to produce clones of squeezed states optimally with minor changes.

The $N \otimes M$ Gaussian cloner using beam splitter network and linear phase-sensitive amplifier is implemented by Braunstein et al. (2001). The cloning evolution relies on global or single-copy fidelity. Cerf et al. (2005) shown that continuous-variable quantum cloning is Gaussian with respect to global fidelity, but if the number of cloned states (M) is finite, then the quantum cloners are non-Gaussian with respect to single-copy fidelity.

Probabilistic Quantum Cloning

The cloning transformation of probabilistic quantum cloning consists of unitary operator and measurement. There is less than 1% probability of producing exact clone; otherwise, it is unsuccessful. In the end, the measurement is carried out on ancilla qubit, which shows whether the process of cloning evolution is successful or not. Regardless of higher fidelity than deterministic cloning schemes, it can produce cloned copies approximately.

The concept of probabilistic cloning was proposed independently by Duan and Guo (1998) and Chefles and Barnett (1998). It has been determined that a perfect copy of linearly independent states can be produced with some probability. Later on, the concept of Probabilistic cloning is expanded to infinite-dimensional space and stated that the quality of cloned states by universal quantum cloning machine could not be enhanced by probabilistic cloning machine. Although, Hardy and Song (1999) investigated that it can be helpful if the number of states is limited. Probabilistic cloning plays a crucial role in quantum information processing. Duan and Guo (1998) described the relationship in state discrimination and probabilistic cloning, and can be applied in the security analysis of quantum key distribution protocols.

Quantum Entanglement Cloning

Quantum entanglement and superposition are fundamental principles of quantum mechanics and play an important role in quantum information processing. Koashi and Imoto (1998) determined that the exact

clone copies of quantum entanglement cannot be produced due to the principles of quantum mechanics. So far, several methods were presented on quantum entanglement cloning. It has been shown that the copies of two-qudit state cannot be generated exactly. Furthermore, the fidelity of 1@2 quantum entanglement cloners over the $n \times n$ -dimensional entangled states is studied by Karpov et al. (2005).

Mostly, the concept of quantum entanglement is demonstrated under local operations and classical communication (LOCC). Under the effect of LOCC, the entanglement cannot be expanded. It has been stated that the perfect cloning of a pair of Bell states can be performed. Therefore, the cloning of 1@2 is shown with LOCC by Bennett et al. (1996). Later on, the possibility to produce clone copies of unknown Bell state without the supervision of LOCC is presented. It can be performed using CNOT gates and entangled ancilla qubits.

Mixed States Quantum Cloning

It is known that the broadcast of non-commuting mixed states is not possible. As a result, most researchers studied the concept of cloning for pure quantum states until now. Initially, Barnum et al. (1996) proved that the no-cloning theorem can also be used for mixed states. Rastegin (2003) determined that the global fidelity for state-dependent mixed state and stated that the cloning evolutions are cannot be generated for mixed states. The mixed-state quantum cloning for qubits is presented and proved that $N @ M$ universal quantum clone machine is optimal by Aiano et al. (2005). Further, it has been determined that 1@M universal quantum cloning machine is not available based on fidelity as the parameter. It has been proved that the probabilistic cloning of mixed states can be performed by Li et al. (2009).

CONCLUSION

After the introduction of Shor's algorithm, quantum computing can decrypt any data secured by present algorithms. Post-quantum cryptosystems are focused on defending the encrypted data against the attacks of classical and quantum computers in the future. Due to lack of hardware and resources for their implementation, more efforts are needed to build confidence for using post-quantum cryptosystems extensively. Hence, there exist several essential questions that need to be addressed. Although, there are several tech giants already conducting experiments with promising post-quantum cryptography algorithms. The requirement is to reduce the public-key size and the actual implementation of post-quantum algorithms in quantum-safe systems. In this chapter, numerous post-quantum public-key cryptosystems are illustrated. Moreover, the classes of quantum cloning machines are described for several quantum information processing tasks.

REFERENCES

Barnum, H., Caves, C. M., Fuchs, C. A., Jozsa, R., & Schumacher, B. (1996). Noncommuting mixed states cannot be broadcast. *Physical Review Letters*, 76(15), 2818–2821. doi:10.1103/PhysRevLett.76.2818 PMID:10060796

Post-Quantum Cryptography and Quantum Cloning

- Bennett, C. H., Bernstein, H. J., Popescu, S., & Schumacher, B. (1996). Concentrating partial entanglement by local operations. *Physical Review A*, *53*(4), 2046–2052. doi:10.1103/PhysRevA.53.2046 PMID:9913106
- Bernstein, D. J. (2009). *Introduction to post-quantum cryptography*. *Post-quantum cryptography* (pp. 1–14). Berlin: Springer. doi:10.1007/978-3-540-88702-7
- Bhatia, A. S., & Kumar, A. (2018). McEliece Cryptosystem Based On Extended Golay Code.
- Bhatia, A. S., & Kumar, A. (2019). Post-Quantum Cryptography. In *Emerging Security Algorithms & Techniques* (1st ed.). New York: Chapman and Hall/CRC Press. doi:10.1201/9781351021708-9
- Braunstein, S. L., Cerf, N. J., Iblisdir, S., van Loock, P., & Massar, S. (2001). Optimal cloning of coherent states with a linear amplifier and beam splitters. *Physical Review Letters*, *86*(21), 4938–4941. doi:10.1103/PhysRevLett.86.4938 PMID:11384386
- Bruß, D., DiVincenzo, D. P., Ekert, A., Fuchs, C. A., Macchiavello, C., & Smolin, J. A. (1998). Optimal universal and state-dependent quantum cloning. *Physical Review A*, *57*(4), 2368–2378. doi:10.1103/PhysRevA.57.2368
- Bu, S., & Zhou, H. (2009). A secret sharing scheme based on NTRU algorithm. In *Proceedings of the 5th International Conference on Wireless Communications, Networking and Mobile Computing, WiCom'09*. IEEE. 10.1109/WICOM.2009.5302743
- Buchmann, J. (2013). *Introduction to cryptography*. Springer Science & Business Media.
- Buchmann, J., & Williams, H. C. (1988). A key-exchange system based on imaginary quadratic fields. *Journal of Cryptology*, *1*(2), 107–118. doi:10.1007/BF02351719
- Buscemi, F., D'Ariano, G. M., & Macchiavello, C. (2005). Economical phase-covariant cloning of qudits. *Physical Review A*, *71*(4), 042327. doi:10.1103/PhysRevA.71.042327
- Bužek, V., & Hillery, M. (1998). Universal optimal cloning of arbitrary quantum states: From qubits to quantum registers. *Physical Review Letters*, *81*(22), 5003–5006. doi:10.1103/PhysRevLett.81.5003
- Cai, J. Y., & Cusick, T. W. (1998). A lattice-based public-key cryptosystem. In *Proceedings of the International Workshop on Selected Areas in Cryptography* (pp. 219–233). Springer.
- Cerf, N., Durt, T., & Gisin, N. (2002). Cloning a qutrit. *Journal of modern optics*, *49*(8), 1355–1373.
- Cerf, N. J., Bourennane, M., Karlsson, A., & Gisin, N. (2002). Security of quantum key distribution using d-level systems. *Physical Review Letters*, *88*(12), 127902. doi:10.1103/PhysRevLett.88.127902 PMID:11909502
- Cerf, N. J., & Fiurasek, J. (2006). Optical quantum cloning. *Progress in Optics*, *49*, 455–545. doi:10.1016/S0079-6638(06)49006-5
- Cerf, N. J., & Iblisdir, S. (2000). Optimal N-to-M cloning of conjugate quantum variables. *Physical Review A*, *62*(4). doi:10.1103/PhysRevA.62.040301
- Cerf, N. J., Ipe, A., & Rottenberg, X. (2000). Cloning of continuous quantum variables. *Physical Review Letters*, *85*(8), 1754–1757. doi:10.1103/PhysRevLett.85.1754 PMID:10970606

- Cerf, N. J., Krüger, O., Navez, P., Werner, R. F., & Wolf, M. M. (2005). Non-Gaussian cloning of quantum coherent states is optimal. *Physical Review Letters*, *95*(7), 070501. doi:10.1103/PhysRevLett.95.070501 PMID:16196769
- Chefles, A., & Barnett, S. M. (1998). Quantum state separation, unambiguous discrimination and exact cloning. *Journal of Physics. A, Mathematical and General*, *31*(50), 10097–10103. doi:10.1088/0305-4470/31/50/007
- Chen, A. I. T., Chen, M. S., Chen, T. R., Cheng, C. M., Ding, J., Kuo, E. L. H., & Yang, B. Y. (2009). SSE implementation of multivariate PKCs on modern x86 CPUs. In *Cryptographic Hardware and Embedded Systems-CHES* (pp. 33–48). Berlin: Springer. doi:10.1007/978-3-642-04138-9_3
- D'Ariano, G. M., Macchiavello, C., & Perinotti, P. (2005). Superbroadcasting of mixed states. *Physical Review Letters*, *95*(6), 060503. doi:10.1103/PhysRevLett.95.060503 PMID:16090933
- Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, *22*(6), 644–654. doi:10.1109/TIT.1976.1055638
- Ding, J., & Schmidt, D. (2005). Rainbow, a new multivariable polynomial signature scheme. In *Proceedings of the Conference on Applied Cryptography and Network Security ACNS 2005* (pp. 164–175). Springer. doi:10.1007/11496137_12
- Duan, L. M., & Guo, G. C. (1998). Probabilistic cloning and identification of linearly independent quantum states. *Physical Review Letters*, *80*(22), 4999–5002. doi:10.1103/PhysRevLett.80.4999
- Fan, H., Imai, H., Matsumoto, K., & Wang, X. B. (2003). Phase-covariant quantum cloning of qudits. *Physical Review A*, *67*(2). doi:10.1103/PhysRevA.67.022317
- Fan, H., Matsumoto, K., Wang, X. B., & Wadati, M. (2001). Quantum cloning machines for equatorial qubits. *Physical Review A*, *65*(1), 012304. doi:10.1103/PhysRevA.65.012304
- Fan, H., Wang, Y. N., Jing, L., Yue, J. D., Shi, H. D., Zhang, Y. L., & Mu, L. Z. (2014). Quantum cloning machines and the applications. *Physics Reports*, *544*(3), 241–322. doi:10.1016/j.physrep.2014.06.004
- Feynman, R. P. (1982). Simulating physics with computers. *International Journal of Theoretical Physics*, *21*(6), 467–488. doi:10.1007/BF02650179
- Fraenkel, A. S., & Yesha, Y. (1979). Complexity of problems in games, graphs and algebraic equations. *Discrete Applied Mathematics*, *1*(1-2), 15–30. doi:10.1016/0166-218X(79)90012-X
- Fuchs, C. A., Gisin, N., Griffiths, R. B., Niu, C. S., & Peres, A. (1997). Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy. *Physical Review A*, *56*(2), 1163–1172. doi:10.1103/PhysRevA.56.1163
- Goldreich, O., Goldwasser, S., & Halevi, S. (1997). Public-key cryptosystems from lattice reduction problems. In *Proceedings of the Annual International Cryptology Conference* (pp. 112–131). Springer.
- Hardy, L., & Song, D. D. (1999). No signalling and probabilistic quantum cloning. *Physics Letters. [Part A]*, *259*(5), 331–333. doi:10.1016/S0375-9601(99)00448-X

Post-Quantum Cryptography and Quantum Cloning

- Hoffstein, J., Pipher, J., & Silverman, J. H. (1998). NTRU: a ring based public key cryptosystem. In *Proceedings of ANTS-III* (pp. 267-288). Springer. 10.1007/BFb0054868
- Hülsing, A. (2013). W-OTS+—shorter signatures for hash-based signature schemes. In *Proceedings of the International Conference on Cryptology* (pp. 173-188). Springer. 10.1007/978-3-642-38553-7_10
- Jing, L., Wang, Y. N., Shi, H. D., Mu, L. Z., & Fan, H. (2012). Minimal input sets determining phase-covariant and universal quantum cloning. *Physical Review A*, 86(6), 062315. doi:10.1103/PhysRevA.86.062315
- Karpov, E., Navez, P., & Cerf, N. J. (2005). Cloning quantum entanglement in arbitrary dimensions. *Physical Review A*, 72(4), 042314. doi:10.1103/PhysRevA.72.042314
- Kipnis, A., & Shamir, A. (1999). Cryptanalysis of the HFE public key cryptosystem by relinearization. In *Proceedings of the Annual International Cryptology Conference* (pp. 19-30). Springer. 10.1007/3-540-48405-1_2
- Koashi, M., & Imoto, N. (1998). No-cloning theorem of entangled states. *Physical Review Letters*, 81(19), 4264–4267. doi:10.1103/PhysRevLett.81.4264
- Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177), 203–209. doi:10.1090/S0025-5718-1987-0866109-5
- Lamport, L. (1979), Constructing digital signatures from a one-way function. SRI International Computer Science Laboratory.
- Lenstra, A. K., & Hendrik Jr, W. (1993). The development of the number field sieve. Springer Science & Business Media. doi:10.1007/BFb0091534
- Li, L., Qiu, D., Li, L., Wu, L., & Zou, X. (2009). Probabilistic broadcasting of mixed states. *Journal of Physics. A, Mathematical and Theoretical*, 42(17), 175302. doi:10.1088/1751-8113/42/17/175302
- Loidreau, P. (2000). Strengthening McEliece cryptosystem. In *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security* (pp. 585-598). Springer.
- Loidreau, P., & Sendrier, N. (2001). Weak keys in the McEliece public-key cryptosystem. *IEEE Transactions on Information Theory*, 47(3), 1207–1211. doi:10.1109/18.915687
- Löndahl, C., Johansson, T., Shooshtari, M. K., Ahmadian-Attari, M., & Aref, M. R. (2016). Squaring attacks on McEliece public-key cryptosystems using quasi-cyclic codes of even dimension. *Designs, Codes and Cryptography*, 80(2), 359–377. doi:10.1007/10623-015-0099-x
- McEliece, R. J. (1978). A public-key cryptosystem based on algebraic coding theory. *Deep Space Network Progress Report*, 44, 114–116.
- Merkle, R. C. (1989). A certified digital signature. In *Proceedings of the Conference on the Theory and Application of Cryptology* (pp. 218-238). Springer.
- Mersin, A. (2007). The comparative performance analysis of lattice based NTRU cryptosystem with other asymmetrical cryptosystems [Master's thesis]. İzmir Institute of Technology.


- Micciancio, D. (2001). Improving lattice-based cryptosystems using the Hermite normal form. In *Cryptography and lattices* (pp. 126–145). Berlin: Springer. doi:10.1007/3-540-44670-2_11
- Nguyen, P. Q., & Regev, O. (2009). Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures. *Journal of Cryptology*, 22(2), 139–160. doi:10.1007/00145-008-9031-0
- Niederreiter, H. (1986). Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory*, 15, 19–34.
- Niu, C. S., & Griffiths, R. B. (1999). Two-qubit copying machine for economical quantum eavesdropping. *Physical Review A*, 60(4), 2764–2776. doi:10.1103/PhysRevA.60.2764
- Patarin, J. (1997). The oil and vinegar signature scheme. *Presented at the Dagstuhl Workshop on Cryptography*. Academic Press.
- Patarin, J., Courtois, N., & Goubin, L. (2001). Quartz, 128-bit long digital signatures. In *Cryptographers' Track at the RSA Conference* (pp. 282–297). Springer.
- Peikert, C. (2016). A decade of lattice cryptography. *Foundations and Trends in Theoretical Computer Science*, 10(4), 283–424. doi:10.1561/04000000074
- Rastegin, A. E. (2003). Upper bound on the global fidelity for mixed-state cloning. *Physical Review A*, 67(1), 012305. doi:10.1103/PhysRevA.67.012305
- Rivest, R. L., Adleman, L., Dertouzos, M. L. (1978). On data banks and privacy homomorphisms. *Foundations of secure computation*, 4(11), 169–180.
- Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120–126. doi:10.1145/359340.359342
- Scarani, V., Iblisdir, S., Gisin, N., & Acin, A. (2005). Quantum cloning. *Reviews of Modern Physics*, 77(4), 1225–1256. doi:10.1103/RevModPhys.77.1225
- Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings of 35th Annual Symposium on Foundations of Computer Science* (pp. 124–134). IEEE. 10.1109/SFCS.1994.365700
- Sidelnikov, V. M., Vladimir, M., & Shestakov, S. O. (1992). On insecurity of cryptosystems based on generalized Reed-Solomon codes. *Discrete Mathematics and Applications*, 2(4), 439–444. doi:10.1515/dma.1992.2.4.439

This research was previously published in Quantum Cryptography and the Future of Cyber Security; pages 1-28, copyright year 2020 by Information Science Reference (an imprint of IGI Global).

Chapter 12

A Quantum Secure Entity Authentication Protocol Design for Network Security

Surjit Paul

 <https://orcid.org/0000-0002-2213-1752>
IIT Kharagpur, Kharagpur, India

Sanjay Kumar

NIT Jamshedpur, Jamshedpur, India

Rajiv Ranjan Suman

NIT Jamshedpur, Jamshedpur, India

ABSTRACT

Authentication is one of the significant issues for all kinds of network communications. Most of the authentication protocols designed and implemented so far for entity authentication are based on classical cryptographic techniques to prevent themselves from different types of attacks. These protocols use either password or challenge for authentication. In this article, the design of the proposed quantum secure entity authentication protocol is shown. The proposed protocol is based on the challenge response method. Due to quantum computer capability to break mathematical complexity-based cryptographic techniques, the proposed protocol uses the one-time pad (OTP) to secure itself from attacks, i.e., eavesdropping, reply attack, password guessing attack, man-in-the-middle attack, brute-force attack, quantum computer attack, etc. Security of the proposed protocol was analyzed, and it shows that the proposed protocol may prevent itself from different types of attacks. Further, analysis for quantum Secure was carried out. From the analysis, it is found that if the OTP key is truly random and cannot be reused, then a computer with infinite capacity or quantum computer cannot break the encrypted challenge and response. The proposed protocol may be used for entity authentication for the client, server, process, and user.

DOI: 10.4018/978-1-7998-8593-1.ch012

1. INTRODUCTION

Due to the extensive use of information and communication technology, protecting resources from unauthorized users are essential nowadays. Authentication plays a vital role in protecting resources from malicious attempts by attackers to breach the security. Most organizations depend on the security measures at the perimeter of network using firewalls, in order to secure their information technology (IT) infrastructure. Several authentication protocols have been designed and implemented to secure systems from unauthorized access. Entity authentication is used to safeguard digital devices from attacks like eavesdropping, man-in-the-middle attack, reply attack etc. Initially, password-based authentication protocol was developed. In this protocol, the password was used for authentication and password was sent as plaintext through the communication channel. This protocol suffered from replay attack, password guessing attack, and dictionary attacks, etc. Later on, Challenge-handshake authentication protocol was developed based on the challenge response paradigm. In this technique, a challenge contained a hash of a random string concatenated with the key using MD5 or SHA algorithms. When claimant got the challenge, then it sent the response to the verifier. Later, on the Extensible Authentication Protocol (EAP) (Aboba et al., 2004), KERBEROS (Kohl & Neuman, 1993), RADIUS (Rigney et al., 2000), DIAMETER (Calhoun et al., 2003) protocol, zero knowledge-based entity authentication protocols were developed. The classical authentication schemes are based on hardness of the mathematical equation.

Due to the advent of high-performance computers and quantum computers, any security mechanism based on mathematical complexity could be broken easily. Hence, the quantum secure authentication protocol is the utmost requirement for the next decade to protect resources from attacks.

One time pad (OTP) is the classical cryptographic algorithm that is almost unbreakable if it is appropriately implemented. In OTP, the ciphertext is generated by using XORing of plaintext and shared OTP between entities. In this paper, the design of a proposed entity authentication protocol to secure authenticated data from quantum computer attacks is discussed.

The rest of the paper is organized as follows: Section 2 deals with related work; Section 3 describes the proposed quantum secure authentication protocol; Section 4 deals with security analysis of the proposed protocol, and finally, section 5 deals with the conclusion and future work.

2. RELATED WORK

To maintain user convenience and high level of security, a highly unpredictable data must be available to the attacker so that they cannot get any information and prevent off-line verification or guess. A common form of guessing attack was examined and developed cryptographic protocols immune to attacks, and suggested a systematic way to examine protocols to detect vulnerabilities to such attacks (Gong et al., 1993). Several password authentication protocols were analyzed and found that public key cryptography provided resistance to offline password guessing attacks. They also incorporated public passwords as handy certificates that the user could carry without any requirement of computing devices (Halevi & Krawczyk, 1999). Further, the password-based authentication protocol model was proposed, and the model for this problem prevented threats like password guessing, forward secrecy, server compromise, and loss of session keys. Authentication Key Exchange (AKE) was used to secure the entity authentication protocol (Bellare et al., 2000). Encrypted Key Exchange (EKE) became the basis for many of the

subsequent research works on this area (Bellovin & Merritt, 1992; Bellovin & Merritt, 1993; Jablon, 1996; Steiner et al., 1995; Lucks, 1997; Patel, 1997; Wu, 1998). Challenge Handshake Authentication Protocol (CHAP) (Simpson, 1996) is also used to verify the identity of the claimant using a three-way handshake. Extension of CHAP namely Microsoft's Point to Point (P2P) CHAP protocol (MS-CHAP), which extends the user authentication functionality, provided on windows networks to remote workstations (Zorn & Cobb, 1998). The P2P Extensible Authentication Protocol (EAP) is a general protocol for P2P authentication and supports more than 40 authentication methods. A specific authentication mechanism is not selected by EAP at Link Control Phase but rather postpones this until the authentication phase (Aboba et al., 2004). KERBEROS is an authentication protocol designed to authenticate by using secret-key cryptography for client-server applications. It is used by many commercial products (Simpson & Willens, 1997; Neuman & Theodore, 1994). Remote Authentication Dial-In User Service (RADIUS) (Simpson & Willens, 1997) was developed for centralized AAA management of users for remote authentication. It is used when users want to connect to the server and use the network service. Later on, this protocol was brought into the Internet Engineering Task Force (IETF) standards. Further, DIAMETER protocol was developed to eliminate the limitations of RADIUS gateway. It serves similar purpose in Authentication, Authorization, and Accounting (AAA) applications however, advanced processes and operations were added to the protocol to make it reliable (Menezes et al., 2001).

Zero-knowledge authentication protocols based on zero knowledge were also developed (Fiat & Shamir, 1987; Fiege et al., 1988). In zero-knowledge proofs of knowledge, the prover demonstrates possession of knowledge without revealing any information (not even the one bit revealed in zero-knowledge proofs of assertions). A trusted third party chooses two large prime numbers p and q to ascertain the quality of $n = p \cdot q$. The quality of n is affirmed to general society; the values of p and q are kept secret. Alice the claimant picks a secret number s i.e. private key between 1 and $(n-1)$.

The Feige-Fiat-Shamir zero-knowledge protocol is like the Fiat-Shamir approach. It utilizes a vector of private keys s_1, s_2, \dots, s_k , a vector of open keys v_1, v_2, \dots, v_k and a vector of difficulties (c_1, c_2, \dots, c_k) (Fiat & Shamir, 1987). The private keys are picked arbitrarily, yet they must be relatively prime to n . The Guillou-Quisquater protocol is a growth of Fiat-Shamir protocol; in which fewer rounds could be utilized to demonstrate the identity of the claimant. A trusted outsider picks two prime numbers p and l to compute the worth of $n = p \cdot q$. The trusted gathering likewise declares the example e , which is co-prime with $\phi = (p-1)(q-1)$ (Fiege et al., 1988). Comparative analysis of existing authentication protocols based on security attacks were also investigated (Paul & Kumar, 2017).

A comprehensive authentication scheme (CIAS) was proposed for secured communication between Vehicle-to-Infrastructure (V2I) and inter Road Side Units (RSUs) in Vehicular Ad hoc Network (VANET) based on asymmetric encryption algorithm (Malik & Pandey, 2018). Another authentication protocol used Diffie-Hellman elliptic curve technique for authentication in Wireless Mesh Network (WMN) (Rathee & Saini, 2018). An authentication and key agreement (AKA) protocol was proposed which failed to meet security requirement related to the discovered authentication attack (Aiash et al., 2012). A secure and efficient AKA protocol SE-AKA uses Elliptic Curve Diffie-Hellman (ECDH) to realize key forward/backward secrecy (KFS/KBS), and it also adopts an asymmetric key cryptosystem to protect user's privacy (Lai et al., 2013). Secure user authentication and key agreement protocol were proposed by using a smart card to protect users' privacy (Amin & Biswas, 2016). Also, a secure mutual authentication scheme was proposed using elliptic curve cryptography for session initiation protocol for multimedia services (He et al., 2012).

Literature highlights that existing authentication protocols used cryptographic algorithms which are supposed to be mathematically unbreakable, but classical cryptography is directly affected by the breakthroughs in quantum cryptography because it relies solely on the hardness of the computing mathematical problem that cannot be solved by current computer in polynomial time, but theoretically can be solved on quantum computer (Chait & Mahdy, 2008). The effect of quantum computers attack on classical cryptography was highlighted (Pecen, 2014). In conventional cryptography, the one-time pad is an encryption technique that cannot be cracked, but requires the use of a one-time pre-shared key should be of same size or as long as the message size being sent.

Development of quantum computer is going with a rapid speed and by 2020, it may be available for general use and are very powerful that can easily break mathematical complexity-based authentication scheme (Chait & Mahdy, 2008). Till the advent of quantum computers, the challenge for the researcher is to devise quantum safe authentication scheme using basic channel. Hence, in this article, an attempt is made to devise the design of a quantum secure authentication protocol for securing the communication network from different types of attacks.

3. PROPOSED QUANTUM SECURE AUTHENTICATION PROTOCOL

Quantum secure authentication protocol is the demand for the coming decade for ensuring the security of the system. Development of such a secure authentication protocol is a challenge. All authentication mechanism based on standard mechanism is vulnerable and could be obsolete overnight when quantum computers would be available for general purpose. However, one-time pad (OTP) is the conventional cryptographic technique, which is considered to be quantum secure if it is implemented properly. In our proposed entity authentication protocol shown in Figure 1, the OTP key plays a key role to make the proposed authentication protocol quantum secure.

The following are the two different phases of the proposed quantum secure authentication protocol:

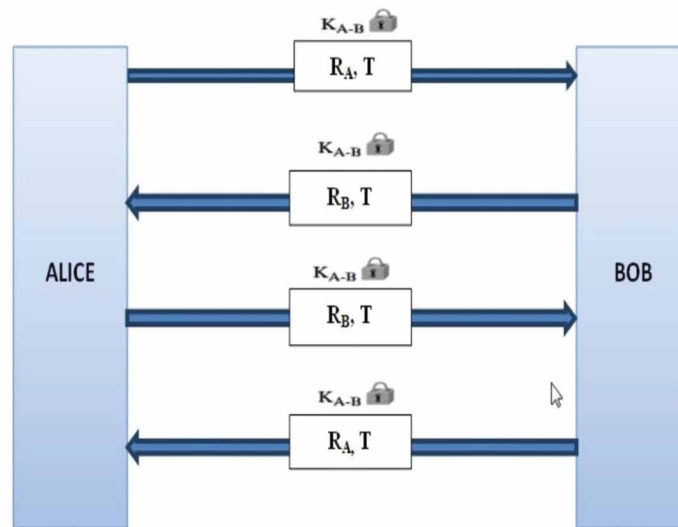
- 1. OTP Key Establishment Phase:** This is the first phase of the proposed authentication protocol, in which the following steps are carried in order to establish OTP Key between ALICE and BOB:
Step 1: To initiate OTP Key establishment, both entities send their userid, timestamp of the system through secured channel along with 50000 random upper case alphabet characters.
Step 2: The second entity verifies the user id and timestamp of the first entity and vice versa to start the OTP key establishment process.
Step 3: Both the parties use same matching algorithm to select 256 characters out of 50000 random characters. The process is continued till the same match is found at both ends to agree as partial OTP.
Step 4: If 256 characters out of 50000 random characters are not matched then a message will be sent as “Unable to establish OTP” key and go to step 1.
Step 5: The generated shared partial OTP key of 256 characters in step 3 are divided into equal size blocks based on some inherent logic. Finally, the blocks are mixed first and swapping of part to another part is done by both the parties in order to generate the final OTP key. The final key is shared between the parties.
- 2. Authentication Phase:** This phase is used to authenticate both the entities. The authentication steps are as follows:
Step 1: Initially, both entities retrieve the current time by using the internet address of the entities.

Step 2: Both the entities send random challenge to each other. Random challenge consists of a random string and current time information encrypted with the shared OTP key established during Key establishment phase along with the Internet Protocol (IP) addresses concatenated together.

Step 3: Each party receives the random challenge sent by them in both directions. Both the entities first decrypt the received encrypted random challenge using the shared OTP key and send the response as encrypted random challenge to either party in both the direction.

Step 4: Both parties compare the received random challenge with the sent random challenge and if match is found then authentication counter will be incremented by one and the process will be carried out further for another two times. If all the three times authentication process is successful, then both the entities are mutually authenticated and session is established between them.

Figure 1. Proposed authentication protocol



2048 bits shared key using OTP

R_A: Random string of Alice

R_B: Random string of Bob

T: Current time of the entity

3.1. Security Parameters

In the key establishment phase, pseudo number generator was devised to generate 50000 random characters. Also, dynamic user id was used which are periodically changed according to changes made by entities and are shared between them. Timestamp was employed to improve the security of OTP key establishment process. The value of the timestamp is unique because it changes every time. Moreover, to improve the security of key establishment process, 256 matched random characters are further divided into fixed size blocks and each block is interchanged with the other block in order to generate the final OTP key. It was used to prevent the proposed protocol from eavesdropping.

In the authentication phase, the current time of both entities was retrieved by using the internet protocol (IP) addresses of the entities. The reason behind this is that the IP address uniquely identifies each entity in the network. Moreover, the current time was used so that each entity should know the geographical location of each other. When either of the entity suspects that the other entity location is not trusted, then the authentication process can be terminated by either of the entity. The random challenge was used as authentication data. Due to randomness in authenticated data, it would be difficult to forge or guessed. It was employed to prevent the proposed protocol from password guessing, brute-force, dictionary attacks. The length of the final random challenge consists of 256 characters since generated shared OTP key was of 256 characters. Finally, the random challenge was encrypted using the shared OTP key before sending to each entity. Authentication counter was used as the checkpoint to ensure whether authentication process is successfully completed or not. It is incorporated to prevent the proposed protocol from reply attack. Also, authentication success and failure packets were used so that both entities should know the status of the authentication process.

The proposed pseudo number generator for selecting 256 random characters out of 50000 random characters formed from character A to Z is shown in Equation (1):

$$X_{i+1} = a*(X_i + b) \text{ mod } m \quad (1)$$

where, a, b and m are constant values used for the random number generator function.

After selection of 256 matched random characters, the matched characters are further divided into fixed size blocks and each block is interchanged with the other block in order to generate the final OTP key.

The OTP key made by random uppercase letters A-Z is designated as a number ranging from 0 to 25. Ciphertext of challenge is generated using Equation (2):

$$\text{Ciphertext} = \text{Plaintext} \oplus \text{OTP} \quad (2)$$

Plaintext from the encrypted challenge is generated using Equation (3):

$$\text{Plaintext} = \text{Ciphertext} \oplus \text{OTP} \quad (3)$$

where, \oplus is Exclusive OR operation.

3.2. Packets Format of the Proposed Entity Authentication Protocol

The proposed authentication protocol uses four types of packet exchange between claimant and verifier. They are:

1. Challenge Request Packet
2. Challenge Response Packet
3. Authentication Success Packet
4. Authentication Failure Packet

The types of packet exchange are explained below:

A Quantum Secure Entity Authentication Protocol Design for Network Security

1. **Challenge Request Packet:** The format of this packet consists of three fields namely random string, time and IP address. The random string consists of uppercase letters and time contains timestamp. The whole packet except the IP address is encrypted using the already established OTP key during key establishment phase. The format of the packet is as shown in Figure 2.

Table 1 shows the conversion table of TIME (T) into no. of characters used for calculation of random string in different proposed authentication packets.

Table 2 shows the conversion of IP addresses into no. of characters used by proposed entity authentication protocol.

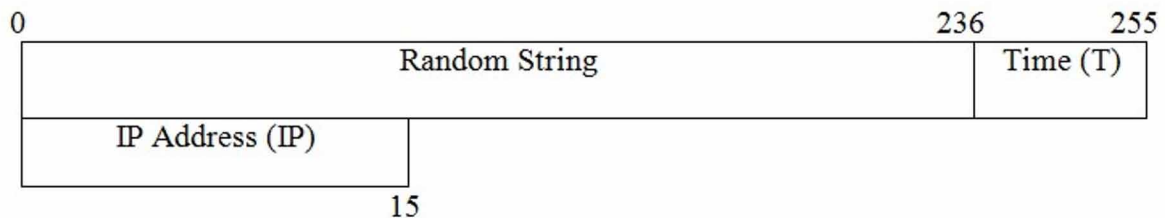
Table 1. Conversion of time to no. of characters

Time (T)	No. of Characters
00:00	16
07:37	19
17:38	18
:	:
23:59	16

Table 2. Conversion of IP addresses into no. of characters

IP Address	No. of Characters
10.255.126.254	14
192.168.25.128	14
138.168.129.229	15

Figure 2. Challenge request packet format



Calculation of Challenge:

$$\text{Challenge} = \text{Current Time} \mid \text{Random String} \mid \text{IP address} \tag{4}$$

where:

$$\text{Random String} = \text{Length of OTP Key} - \text{Length of Time (T)}$$

2. **Challenge Response Packet:** It consists of random string contains random uppercase letters and time in timestamp is encrypted using the shared OTP key shown in Figure 3;
3. **Authentication Success Packet:** It is sent when authentication is successfully done between entities. The authentication packet consists of the field shown in Figure 4;

4. **Authentication Failure Packet:** It is sent when authentication is not successfully done between entities. The authentication failure packet consists of the field shown in Figure 5.

Figure 3. Challenge response packet format

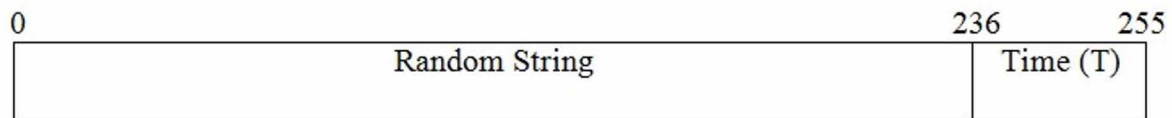


Figure 4. Authentication success packet format

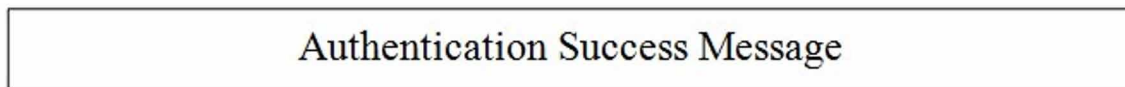


Figure 5. Authentication failure packet format



4. SECURITY ANALYSIS OF THE PROPOSED PROTOCOL

The Table 3 shows different existing Point-to-Point (P2P) authentication protocols, the year of their development, strength of these authentication scheme, and security attacks.

4.1. Security Analysis

Table 3 shows the different type of authentication protocol and its corresponding security attacks. The detailed evaluation of security attacks on the proposed authentication protocol is summarized as below:

1. **Eavesdropping:** In eavesdropping, the attacker tries to listen to the communication channel and to capture some useful information from the ongoing communication. In the proposed protocol, the plaintext is not sent in plaintext format whereas encrypted with 256 bytes OTP key. Since the beauty of OTP key is that it purely random and is not repeated for the next communication, hence it is difficult for the attacker to decrypt authentication request and response packets. Also, it is neither stored in a file nor reused for later communication; it makes the authentication protocol robust and prevents it from network-based eavesdropping attacks;

Table 3. Comparison among various existing P2P authentication protocols

Authentication Protocol	Year of Development	Authentication Scheme	Eavesdropping	Replay Attack	Man-in-the-Middle	Password-Guessing Attack	Dictionary Attacks	Brute-force Attacks	Reflection Attack	Impersonation
PAP	1992	Weak	✓	✓	✓	✓	✓	✓	✓	✓
CHAP	1994	Strong	✓	✗	✗	✗	✗	✓	✓	✗
EAP	2005	Strong	✓	✓	✓	✓	✗	✓	✓	✓
LEAP	2005	Weak	✓	✓	✓	✓	✓	✓	✓	✓
RADIUS	1991	Strong	✓	✓	✗	✓	✓	✓	✓	✓
KERBEROS	1980	Strong	✗	✗	✓	✓	✓	✓	✗	✓
PEAP	2005	Strong	✓	✓	✓	✓	✗	✓	✓	✓
Fiat-Shamir Protocol	1986	Zero Knowledge	✗	✓	✓	✓	✗	✓	✓	✓
Feige-Fiat-Shamir Protocol	1988	Zero Knowledge	✗	✓	✓	✓	✗	✓	✓	✓
Guillou-Quisquater Protocol	2004	Zero Knowledge	✗	✓	✓	✓	✗	✓	✓	✓

2. **Replay attack:** Due to the change in OTP as the secret key for each challenge request and response, it is difficult for the attackers to send the previously recorded messages of the past communications to be pretended as claimant and thereby the proposed authentication protocol prevents itself from reply attack. Also, during authentication phase, both the entities will verify that value of authentication counter must be three then only they are mutually authenticated and session is established between them;
3. **Man-in-the-middle (MitM) attack:** In the proposed authentication protocol, OTP key is used to encrypt challenge and decrypt the response. Hence, it is difficult for the adversary to decrypt the challenges and responses packets. Hence, the proposed protocol does not suffer from man-in-the-middle attack. Also, after successful authentication a session is established between the entities and is valid only for a single communication;
4. **Password-Guessing attack:** In the proposed protocol, the authentication is not based on a fixed password rather than random challenge; hence no password guessing attack could be launched. Also, there is no such challenge, or OTP key file exists on either side to guess it;
5. **Dictionary attacks:** To encrypt the challenge and response OTP key of 256 bytes is used. The formation of dictionary of 256 bytes OTP key is very difficult. It further complicates this issue when the 256 bytes is random for each challenge and response. So the chance of suffering from this attack is negligible;
6. **Brute-force attacks:** In this type of attack, attackers systematically check all possible passwords and password phrases until the correct one is found. Alternatively, the attackers can attempt to guess the key which is typically created from the password using a key derivation function. In the proposed protocol, brute force attack attempts are wasted because of randomness OTP key for each challenge and response no OTP key is later used for encrypting the challenge and response;
7. **Reflection attack:** The proposed protocol could not be affected by reflection attack due to following reasons:

- a. Only one TCP based connection is allowed at a time and claimant is not allowed to open the separate TCP connection to launch reflection attack;
 - b. Apart from TCP, no additional UDP based connection is allowed between claimant and verifier;
 - c. Claimant responds first to the challenge sent by the verifier before the verifier responds to the challenge sent by the claimant;
8. **Impersonation:** In the proposed authentication protocol, before the OTP key generation phase and authentication phase, claimant and verifier exchanged their socket address, user ID's and timestamps through the secure channel for connection establishment between them. These credentials changes for each initiation for connection establishment. Since it is very difficult for an attacker to know these credentials; it is difficult for him/her to launch an impersonation attack.

4.2. Proof for Quantum Secure

There are following reasons behind to say that the proposed authentication protocol is quantum secure:

1. In the proposed authentication protocol, the algorithms used for establishing the OTP key is random and found to be reasonably secured;
2. The stream of characters used in the OTP key establishment was random that constitute the ciphertext is genuinely random. Thus, there is very less chance to get any pattern or regularities for the cryptanalyst to attack the ciphertext;
3. The OTP key size is 256 bytes (2048 bits), and its corresponding search space is 2^{2048} , which is computationally very large and complicated to break by parallel computers as well as quantum computers;
4. The challenge and response issued by claimant and verifier are purely random strings and not meaningful sentences;
5. Shor's algorithm performs prime factoring in quantum computers and hence is useful against RSA or ECC encryption algorithm. In the proposed authentication protocol, such encryption algorithms are not used, rather 256 bytes (2048 bits) OTP key was used to encrypt the random challenge and response;
6. For quantum secure, the OTP key should be unique for all the communication.

5. CONCLUSION AND FUTURE WORK

Information security plays a pivotal role to secure systems from unauthorized access. Authentication protocols based on classical cryptographic technique suffers from different type of attacks as shown in the Table 3. Hence, there is an utmost requirement of proposing a novel P2P entity authentication protocol free from different attacks. In this paper, the design of proposed quantum secure authentication protocol is devised that is computationally quantum secure. Due to less availability and expensive quantum authentication technique, development of entity authentication protocol based on quantum cryptography is difficult to model, design, test, and implement in the current scenario. In future, implementation and testing of our proposed authentication protocol will be carried out.

REFERENCES

- Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., & Levkowitz, H. (2004). *Extensible authentication protocol (EAP)* (No. RFC 3748).
- Aiash, M., Mapp, G., & Lasebae, A. (2012). A survey on authentication and key agreement protocols in heterogeneous networks. *International Journal of Network Security & Its Applications*, 4(4), 199–214. doi:10.5121/ijnsa.2012.4413
- Amin, R., & Biswas, G. P. (2016). A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks. *Ad Hoc Networks*, 36, 58–80. doi:10.1016/j.adhoc.2015.05.020
- Bellare, M., Pointcheval, D., & Rogaway, P. (2000, May). Authenticated key exchange secure against dictionary attacks. In *Proceedings of the International conference on the theory and applications of cryptographic techniques* (pp. 139-155). Springer. 10.1007/3-540-45539-6_11
- Bellovin, S. M., & Merritt, M. (1992, May). Encrypted key exchange: Password-based protocols secure against dictionary attacks. In *Proceedings 1992 IEEE Computer Society Symposium on Research in Security and Privacy* (pp. 72-84). IEEE. 10.1109/RISP.1992.213269
- Bellovin, S. M., & Merritt, M. (1993, December). Augmented encrypted key exchange: a password-based protocol secure against dictionary attacks and password file compromise. In *Proceedings of the 1st ACM Conference on Computer and Communications Security* (pp. 244-250). ACM. 10.1145/168588.168618
- Calhoun, P., Loughney, J., Guttman, E., Zorn, G., & Arkko, J. (2003). *Diameter base protocol* (No. RFC 3588). The Quantum Computer. Retrieved from https://www.cs.rice.edu/~taha/teaching/05F/210/news/2005_09_16.htm
- Chait, D., & Mahdy, A. (2008). A Survey of Quantum and Classical Cryptography. *Student Paper E-Journal*. Retrieved from http://www.pro-technix.com/information/crypto/pages/vernam_base.html
- Fiat, A., & Shamir, A. (1986, August). How to prove yourself: Practical solutions to identification and signature problems. In *Proceedings of the Conference on the Theory and Application of Cryptographic Techniques* (pp. 186-194). Springer.
- Fiege, U., Fiat, A., & Shamir, A. (1988). Zero Knowledge Proofs of Identity. *Journal of Cryptology*, 1(2), 77–94. doi:10.1007/BF02351717
- Gong, L., Lomas, M., Needham, R., & Saltzer, J. (1993). Protecting Poorly Chosen Secrets from Guessing Attacks. *IEEE Journal on Selected Areas in Communications*, 11(5), 648–656. doi:10.1109/49.223865
- Halevi, S., & Krawczyk, H. (1999). Public-key cryptography and password protocols. *ACM Transactions on Information and System Security*, 2(3), 230–268. doi:10.1145/322510.322514

- He, D., Chen, J., & Chen, Y. (2012). A secure mutual authentication scheme for session initiation protocol using elliptic curve cryptography. *Security and Communication Networks*, 5(12), 1423–1429. doi:10.1002/ec.506
- Jablon, D. (1996). Strong Password-Only Authenticated Key Exchange. *Computer Communication Review ACM SIGCOMM*, 26(5), 5–26. doi:10.1145/242896.242897
- Kohl, J., & Neuman, C. (1993). *The Kerberos network authentication service (V5)* (No. RFC 1510).
- Lai, C., Li, H., Lu, R., & Shen, X. S. (2013). SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks. *Computer Networks*, 57(17), 3492–3510. doi:10.1016/j.comnet.2013.08.003
- Lucks, S. (1997, April). Open key exchange: How to defeat dictionary attacks without encrypting public keys. In *Proceedings of the International Workshop on Security Protocols* (pp. 79-90). Springer, Berlin, Heidelberg.
- Malik, A., & Pandey, B. (2018). CIAS: A Comprehensive Identity Authentication Scheme for Providing Security in VANET. *International Journal of Information Security and Privacy*, 12(1), 29–41. doi:10.4018/IJISP.2018010103
- Menezes, A. J., van Oorschot, P. C., & Scott, A. V. (2001). *Handbook of Applied Cryptography* (5th ed.). Boca Raton, FL: CRC Press.
- Neuman, B. C., & Theodore, T. (1994). Kerberos: An Authentication Service for Computer Networks. *IEEE Communications Magazine*, 32(9), 33–38. doi:10.1109/35.312841
- Patel, S. (1997, May). Number theoretic attacks on secure password schemes. In *Proceedings. 1997 IEEE Symposium on Security and Privacy* (pp. 236-247). IEEE. 10.1109/SECPRI.1997.601340
- Paul, S., & Kumar, S. (2017). Comparative Analysis of Various PPP Authentication Protocols. *International Journal of Innovative Research in Computer and Communication Engineering*, 5(2), 1399–1404.
- Pecen, M. (2014). Quantum Safe Cryptography and Security: An Introduction, Benefits, Enablers and Challenges, white paper. *European Telecommunications Standards Institute*.
- Rathee, G., & Saini, H. (2018). Authentication Through Elliptic Curve Cryptography (ECC) Technique in WMN. *International Journal of Information Security and Privacy*, 12(1), 42–52. doi:10.4018/IJISP.2018010104
- Rigney, C., Willens, S., Rubens, A., & Simpson, W. (2000). *Remote authentication dial in user service (RADIUS)* (No. RFC 2865).
- Simpson, W. (1996). *PPP challenge handshake authentication protocol (CHAP)* (No. RFC 1994).

A Quantum Secure Entity Authentication Protocol Design for Network Security

Simpson, W., & Willens, S. (1997). Remote Authentication Dial In User Service (RADIUS) (No. RFC2138).

Steiner, M., Tsudik, G., & Waidner, M. (1995). Refinement and Extension of Encrypted Key Exchange. *Operating Systems Review*, 29(3), 22–30. doi:10.1145/206826.206834

Wu, T. (1998, March). The Secure Remote Password Protocol. In *Proceedings of the 1998 Internet Society Network and Distributed System Security Symposium*, San Diego, CA (pp. 97-111).

Zorn, G., & Cobb, S. (1998). *Microsoft ppp chap extensions* (No. RFC 2433).

This research was previously published in the International Journal of Information Security and Privacy (IJISP), 13(4); pages 1-11, copyright year 2019 by IGI Publishing (an imprint of IGI Global).

Chapter 13

Medical Data Are Safe: An Encrypted Quantum Approach

Padmapriya Praveenkumar

Shanmugha Arts, Science, Technology, and Research Academy (Deemed), India

Santhiyadevi R.

Shanmugha Arts, Science, Technology, and Research Academy (Deemed), India

Amirtharajan R.

Shanmugha Arts, Science, Technology, and Research Academy (Deemed), India

ABSTRACT

In this internet era, transferring and preservation of medical diagnostic reports and images across the globe have become inevitable for the collaborative tele-diagnosis and tele-surgery. Consequently, it is of prime importance to protect it from unauthorized users and to confirm integrity and privacy of the user. Quantum image processing (QIP) paves a way by integrating security algorithms in protecting and safeguarding medical images. This chapter proposes a quantum-assisted encryption scheme by making use of quantum gates, chaotic maps, and hash function to provide reversibility, ergodicity, and integrity, respectively. The first step in any quantum-related image communication is the representation of the classical image into quantum. It has been carried out using novel enhanced quantum representation (NEQR) format, where it uses two entangled qubit sequences to hoard the location and its pixel values of an image. The second step is performing transformations like confusion, diffusion, and permutation to provide an uncorrelated encrypted image.

INTRODUCTION

The proliferation of telemedicine applications forces a massive requirement on the security and accuracy of the medical data transmission through communication channels. Health Insurance Portability and Accountability Act (HIPAA) states that over 17 crores of medical data have been breached (“Healthcare Data Breach Statistics”). IBM security and Ponemon Institute stated that the average cost of stolen record

DOI: 10.4018/978-1-7998-8593-1.ch013

Medical Data Are Safe

is increased to 4.8% (Global Overview, 2018). 20% of the victims received wrong diagnosis or delayed treatment due to the illegal use of healthcare information (“MIFA Shares Industry Wisdom on Medical Identity Theft and Fraud”). The medical report includes personal details, health insurance policy number and healthcare history. Using this vast information, forged insurance can be claimed. The challenges in any medical system are that the number of images handled by the unit is substantial; also the size of the images is bulky. In contrast to the normal images, medical images have more redundant data. As a result, it is essential to devise encryption methods to process these medical images, so as to reduce the computational complexity. To manage this situation in classical image processing; the concept of quantum-based computation has been integrated with image encryption algorithms to achieve high computation speed and to provide parallelism and minimal storage requirements.

BACKGROUND

A good encryption scheme should possess Confidentiality, Integrity and Authentication (CIA). The first one indicates that the data is kept private from unauthorised disclosure. Integrity is offered by constructing the data that has not been transformed or tampered. Finally, authentication is the method of data recognition by the sender and receiver.

Undeniably, a well-devised healthcare security system should fulfil two conditions: confusion and diffusion to accomplish CIA in any security system. The chaotic equations are induced for achieving the above-said conditions, due to its aperiodic nature and susceptible to the primary condition. The first chaotic system-based encryption was proposed by Fridrich J (Fridrich, 1998). Since then, a variety of chaotic system-based encryption algorithms were framed. Further to prevail over the weakness like small key space and to eliminate the discontinuous range of chaotic behaviour, Zhou *et al.* (Zhou, Bao, & Chen, 2014) proposed a new chaotic system, by integrating the existing chaotic maps.

For the bulky medical data, conventional encryption algorithms like Advanced Encryption Standard (AES), Data Encryption Standard (DES) and S-box permutation matrix are incapable of surviving against various brute force, statistical and differential attacks. Therefore, a number of encryption algorithms have been developed based on DeoxyriboNucleic Acid (DNA), watermarking and hash algorithms to provide privacy and to ensure the integrity of the medical images used across the globe. Transmitting the entire bulky medical data tends to overload the traffic across communication channels. To evade this scenario, partial encryption and integrity check algorithms were proposed recently by many researchers (Ravichandran *et al.*, 2017).

Classical image encryption algorithms are naturally extended to the quantum scenario due to the breakthrough of quantum information and quantum computation. Quantum computation has become an innovative tool for meeting with the real-time computational requirements. In an information storage and parallel computing, it has numerous exclusive computational qualities such as superposition of quantum state, quantum coherence and entanglement which makes quantum computing greater to its classical counterpart. In (Feynman, 1982), Feynman framed the initiative for the quantum computer, which comprises a physical machine which accepts input states as a superposition of many inputs (Deutsch, 1985).

In a quantum-enabled computer, the quantum image is an edition of the classical image. A variety of methods have been projected to signify the importance of quantum images and quantum image processing algorithms. Various quantum representation schemes were evolved to store the quantum image; few of them were Novel Enhanced Quantum Representation (NEQR), Entangled, Real ket, Multi-Channel

Representation of Quantum Image (MCRQI), Flexible Representation of Quantum Images (FRQI) and log-polar (Latorre, 2005; Sang, Wang, & Niu, 2016; S. E. Venegas-Andraca & Ball, 2010; Salvador E. Venegas-Andraca & Bose, 2003; Y. Zhang, Lu, Gao, & Xu, 2013). In NEQR format, two entangled qubit sequences are used for hoarding both the location and its pixel values of an image. The advantages of using NEQR are the time required for preparing the Quantum image representation is less, image retrieval is accurate, and a range of image operations can be done expediently as compared to other quantum image formats.

Most of the encryption algorithm uses quantum gates for encrypting the images due to its reversible properties (Tofoli, 1980). Heidari *et al.* (Heidari & Naseri, 2016), proposed a quantum m-bit embedding and watermarking procedures utilising NEQR format. Watermarking procedure by utilizing Quantum Wavelet Transform (QWT) is proposed by Song *et al.* (Song, Wang, Liu, Abd El-Latif, & Niu, 2013). However, the cover image cannot be retrieved in these quantum watermark algorithms. Image encryption algorithms assisted with quantum principle employing scrambling and diffusion operations is proposed by Beheri *et al.* (Beheri, Amin, Song, & El-latif, 2016). A novel quantum encryption algorithm is framed which utilises quantum gates and quantum gray code to provide uncorrelated cipher output (Abd El-Latif, Abd-El-Atty, & Talha, 2017). However, these proposed frameworks were unable to meet the optimum condition in terms of security analysis. Also researchers have validated their proposed algorithms using metrics like Number of Pixel Change Rate (NPCR), Unified Average Change in Intensity (UACI), (Wuet *al*, 2011), entropy, correlation and chi-square tests (Fu *et al.*, 2013; Fu, Zhang, Bian, Lei, & Ma, 2014; Helmy, El-Rabaie, Eldokany, & El-Samie, 2017; Li, Wang, Yan, & Liu, 2016; Praveenkumar *et al.*, 2015; Ravichandran *et al.*, 2016; X. Wang & Liu, 2017; S. Zhang, Gao, & Gao, 2014).

By examining numerous quantum encryption methodologies in the available literature, this chapter concentrates the following aspects in preserving and transferring the medical images:

- Proposes an image encryption algorithm employing quantum concepts, quantum gates and a hash function for integrity check and to protect the medical images.
- The proposed methodology utilizes Quantum SWAP, CNOT gates and Secure Hash Algorithm-512 (SHA-512).
- It can be implemented in both selective and complete image encryption applications.

PRELIMINARIES

Novel Enhanced Quantum Representation (NEQR)

By operating NEQR, the classical image can be represented in quantum representation. NEQR is preferred over FRQI because the time required to prepare NEQR quantum image reveals a rough quadratic drop and additional image operations can be carried out. NEQR uses two-qubit sequences for storing both the pixel and its position values. Therefore, it requires $q+2n$ qubits for storing the pixel value of an image. NEQR of the color Digital Imaging and Communication in Medicine (DICOM) image can be represented as,

Medical Data Are Safe

$$|I\rangle = \frac{1}{2^n} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} |C_{YX}\rangle |YX\rangle \tag{1}$$

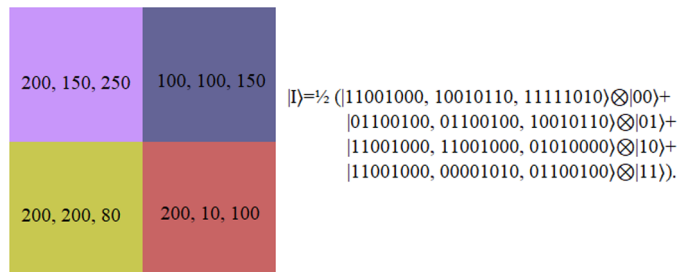
$$C_{YX} = C_{YX}^{0R} \dots C_{YX}^{7R} C_{YX}^{0G} \dots C_{YX}^{7G} C_{YX}^{0B} \dots C_{YX}^{7B} \\ = C_{YX}^0 \dots C_{YX}^7 C_{YX}^8 \dots C_{YX}^{15} C_{YX}^{16} \dots C_{YX}^{23}, C_{YX}^k \in \{0,1\}, C_{YX} \in [0, 2^q - 1] \tag{2}$$

Therefore, equation (1) can be rewritten as,

$$|I\rangle = \frac{1}{2^n} \sum_{YX=0}^{2^{2n}-1} \otimes_{i=0}^{23} |C_{YX}^i\rangle \otimes |YX\rangle \tag{3}$$

Figure 1 illustrates the NEQR paradigm for a 2x2 RGB (R-Red, G- Green, B-Blue) DICOM image, where $g(0,0) = (200, 150, 250)$ i.e. R=200, G=150, B=250. Then, the basis state can be denoted as $|11001000, 10010110, 11111010\rangle \otimes |00\rangle$.

Figure 1. NEQR representation for a 2x2 colour images



CONTROLLED-NOT (CNOT Gate)

CNOT is a type of two input quantum gate. Circuit diagram of CNOT gate and its wire diagram are shown in Figures. 2 and 3 respectively. It has the mapping of (a, b) to $(a'=a, b'=a \oplus b)$, where a and b represents control and the target qubits respectively. \oplus symbol in the mapping is used to represent the CNOT operation. If the control qubit is $|1\rangle$ then the target qubit is flipped else the target remains unaffected.

SWAP Gate

SWAP gate is yet another type of two-input quantum gate. The circuit diagram and its wire diagram are illustrated in Figures. 4 and 5 respectively. It maps (x,y) to $(x'=y, y'=x)$.

Figure 2. The CNOT gate

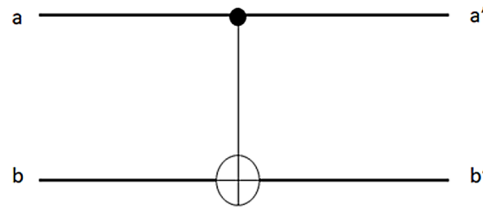


Figure 3. Wire diagram of CNOT gate

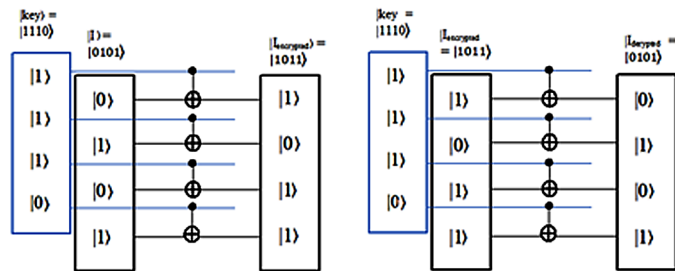


Figure 4. The SWAP gate

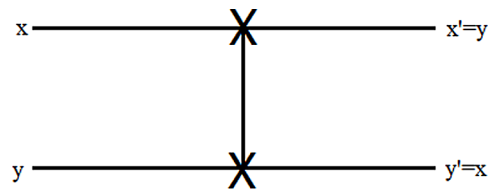
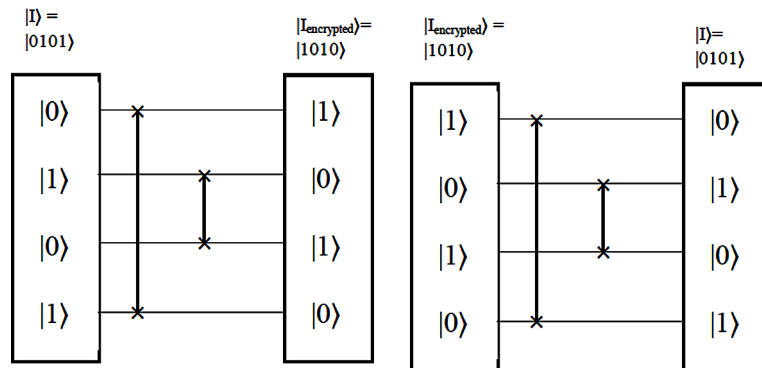


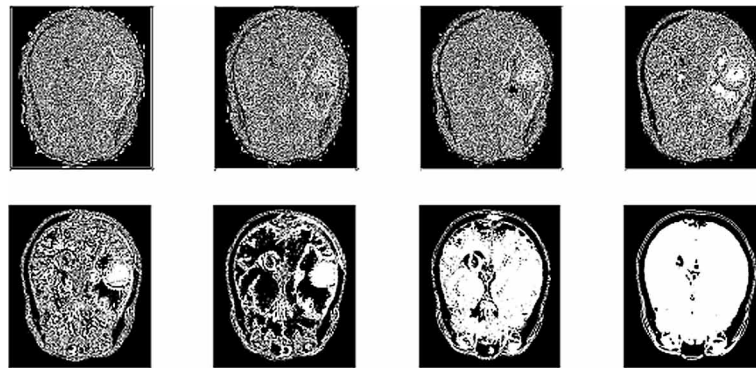
Figure 5. Wire diagram of SWAP gate



Bit Planes

A bit-plane comprises of a collection of bits mapping to the bit position of the given image. The RGB DICOM image will have the range from [0 - 255] for all the three (R, G and B) planes. The Least Significant Bit (LSB) is hoarded in the first-bit plane, and Most Significant Bit (MSB) of all pixel values will be kept in the eighth-bit plane and so on. Figure. 6 illustrates bit plane representation of the Red channel of the original image 1.

Figure 6. Bit planes of the R component of original image 1



Fingerprint and Hash

The fingerprint image is normally used for ensuring the integrity of the image. Both the sender and receiver will have the fingerprint image, which acts as a key input to the hash algorithm. It is a one-way function if x is given, then calculating $h(x)=y$ is trivial. But given y , it is difficult to compute $h^{-1}(y)=x$. Here, the SHA-512 algorithm is used which takes variable length image as input and produces 512-bit hash value output. Both the sender and the receiver estimate the hash value with the fingerprint image. These 512-bits are converted into an 8×8 matrix, and this hash value is incorporated in the image for verification, if there is any alteration in the cipher image during transit, then the original image cannot be retrieved at the receiver end.

QUANTUM ENCRYPTION AND INTEGRITY CHECK ALGORITHM

Medical image encryption algorithm utilising quantum concepts along with SHA-512, quantum bit planes and quantum gates are detailed in this section. Further, the proposed algorithm is integrated with fused Logistic, Tent and Sine maps. Figure 7 portrays the block diagram of the proposed methodology.

Initially, the hash value is produced from the fingerprint image by utilising the SHA-512 algorithm. Then the Region of Interest (ROI) and Region of Non-Interest (RONI) are separated from the original DICOM image. Further ROI and RONI image, chaotic map and the hash values are converted into quantum image format. The quantum ROI image is subjected to the 1st stage of encryption by utilising

the swap gate, between the quantum bit-planes and diffused by employing the CNOT gate. The 2nd stage of encryption is attained by exploiting the row and column shuffling. Additionally, it is diffused by applying the circular shift operation. Between the two encryption stages, the hash value is employed by operating the CNOT gate. At the end of two encryption stages, NPCR and UACI values are estimated and updated by the rounds of operation.

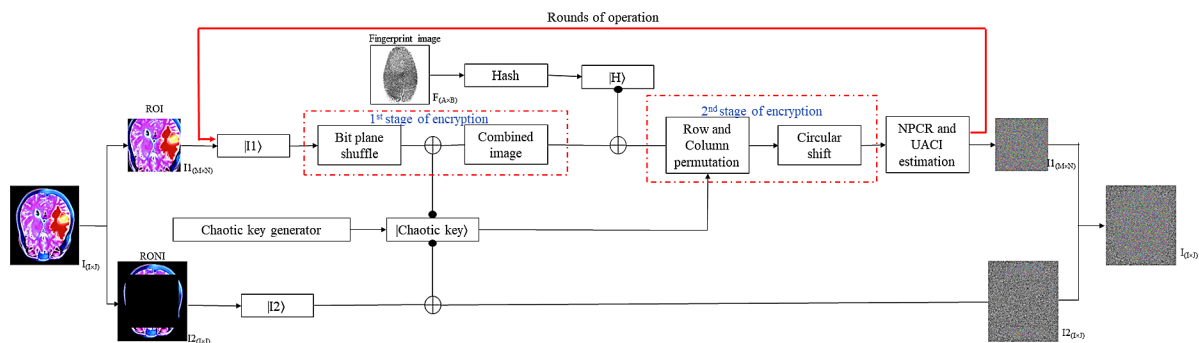
The Integrated Logistic-Tent (ILT) and Integrated Logistic-Sine (ILS) maps are specified in equations (4) and (5) respectively.

$$x_{n+1} = \begin{cases} \left[\mu x_n (1 - x_n) + \frac{(4 - \mu)x_n}{2} \right] \text{mod} 1; x_n < 0.5 \\ \left[\mu x_n (1 - x_n) + \frac{(4 - \mu)(1 - x_n)}{2} \right] \text{mod} 1; x_n \geq 0.5 \end{cases} \quad (4)$$

$$y_{n+1} = \left[r y_n (1 - y_n) + (4 - r) \sin(\pi y_n) / 4 \right] \text{mod} 1 \quad (5)$$

where (μ, r) are control parameters and $(\mu, r) \in (0, 4]$, (x_n, y_n) are initial parameters and $(x_n, y_n) \in [0, 1]$.

Figure 7. Block representation of the projected encryption scheme



Encryption Algorithm

Input: Original RGB DICOM image.

Output: RGB DICOM ROI image, RBG DICOM RONI image.

Step 1: Divide the DICOM image $(I_{(L \times L)})$ into ROI $(I_{(M \times N)})$ and RONI $(I_{(L \times L)})$. The initial point $(I_{(M_1, N_1)})$, height and width of ROI is taken as the key $(kc1, kc2, kc3, kc4)$ for separating ROI at the decryption stage. The procedure to separate ROI and RONI is given below:

ROI and RONI Separation Procedure

Crop ROI ($I_{1(M \times N)}$) from the DICOM image as ($I_{(I \times J)}$) and the left-over part is considered as RONI ($I_{2(I \times J)}$).

The initial point ($I_{1(M1, N1)}$), height and width of ROI is taken as keys (kc1 (M1), kc2 (N1), kc3, kc4) for separating ROI at the decryption stage.

ROI Encryption Process

Input: RGB DICOM ROI image.

Output: Interlinked image.

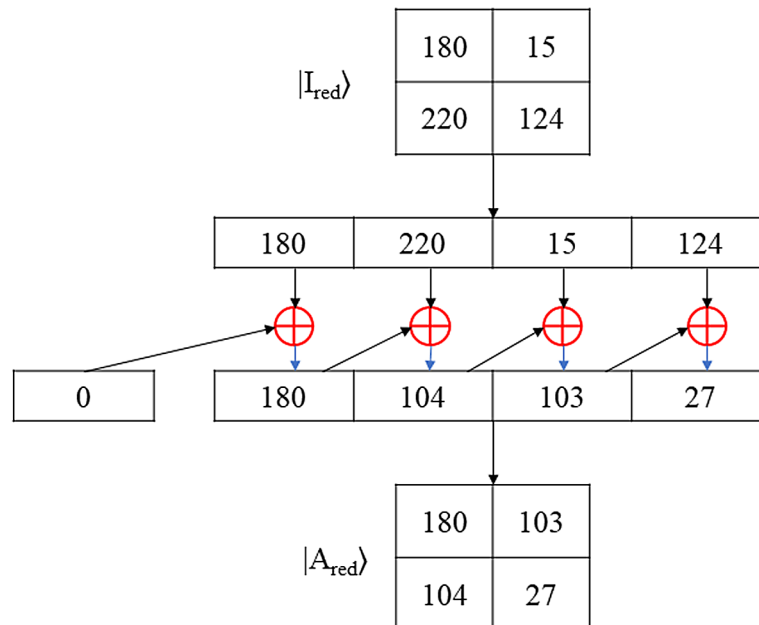
Step 2: Split the ROI DICOM image into red, green and blue planes.

Step 3: Transform the ROI red plane into NEQR quantum bit-plane representation (6) and convert the red plane into an array. Interlink the image pixels by operating equation (vii) on the array. Figure. 8 shows the pixel interlinking procedure using (7). Further, the obtained array is converted into the matrix, according to the size of ROI planes.

$$|I_{red}\rangle = \frac{1}{2^n} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} \otimes_{i=0}^8 |C_{YX}^i\rangle |YX\rangle \tag{6}$$

$$|A_{red}\rangle = CNOT(I_{red}(i, j-1), I_{red}(i, j)) \tag{7}$$

Figure 8. Example of pixel interlink



Step 4: Choose ‘ μ ’ and ‘ x_n ’ (K_1) and iterate ILS map for ‘s’ times and neglect first ‘t’ iterations for avoiding the transient effect. Choose the chaotic sequence $X = \{x_{t+1}, x_{t+2}, \dots, x_s\}$, where the size of X should be equal to $M \times N$ and operate equation (6) on ‘X’ and represent it as a quantum bit-plane image to get the sequence $|X\rangle$ and operate equation (viii) on $|X\rangle$ to get $|X'\rangle$.

$$|X'\rangle = \text{floor}\left(\text{mod}\left(|X\rangle \times 10^{17}, 256\right)\right) \tag{8}$$

Phase One: 1st Stage of Encryption

Input: Interlinked image, key- $|X'\rangle$.

Output: Diffused image.

Step 5: By operating the SWAP gate, bit-planes of $|A_{red}\rangle$ are shuffled to get $|A_{red}\rangle$.

Step 6: Operate CNOT gate on $|A_{red}\rangle$ and $|X'\rangle$ to get $|I_{CNOT}(i)\rangle$ where $i = 1$ to 8 (no. of bit planes), $|X'\rangle$ is the control bit, and $|A_{red}\rangle$ is the target bit. Finally, combine all the eight planes of $|I_{CNOT}\rangle$.

Figure 9 (a and b) shows the wire diagram of the proposed encryption and decryption modules.

Phase Two: Hash Value Implementation

Input : Diffused image, Hash values.

Output: Hash image.

Step 7: The fingerprint image of size $A \times B$ is given as input to the SHA-512 algorithm (Chai, Zheng, Gan, Han, & Chen, 2018), (M. Wang, Wang, Zhang, & Gao, 2018) and the output 512-bits are converted to decimal and reshaped into the 8×8 matrix. Transform the hash matrix into NEQR as

$$|H\rangle = \frac{1}{2^n} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} \otimes_{i=0}^8 |C_{YX}^i\rangle |YX\rangle \tag{9}$$

Step 8: Consider $|H\rangle$ as control bit and $|I_{CNOT}\rangle$ as target bit and execute CNOT operation to obtain the output $|H'\rangle$. The CNOT gate is applied to the first 8×8 matrix of $|I_{CNOT}\rangle$.

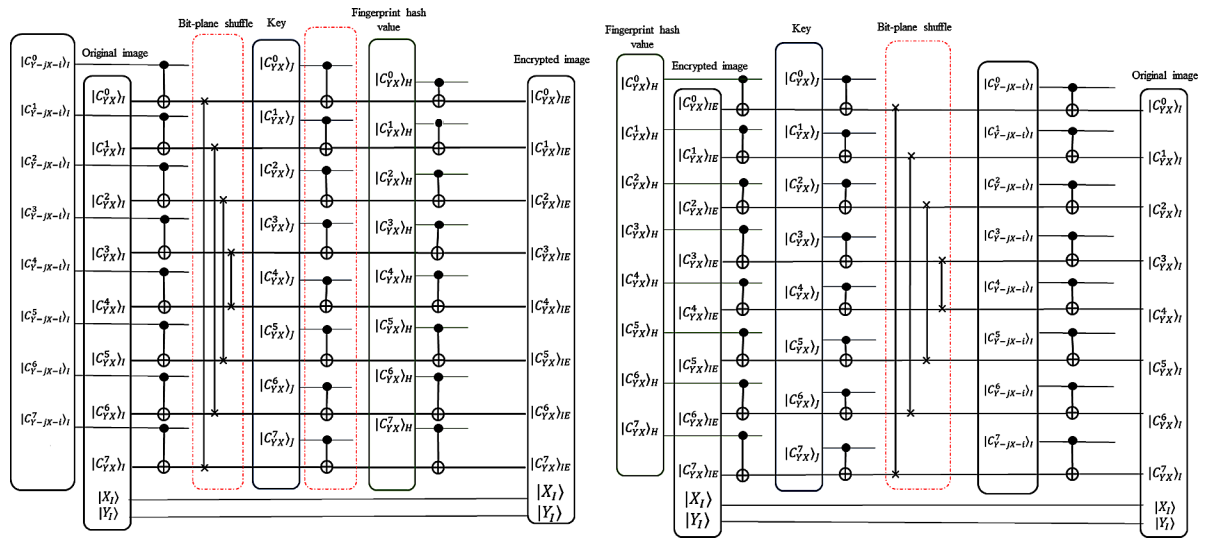
Phase Three: 2nd Stage of Encryption

Input: Hash image, Key- K_2, K_3 .

Output: Encrypted ROI DICOM image.

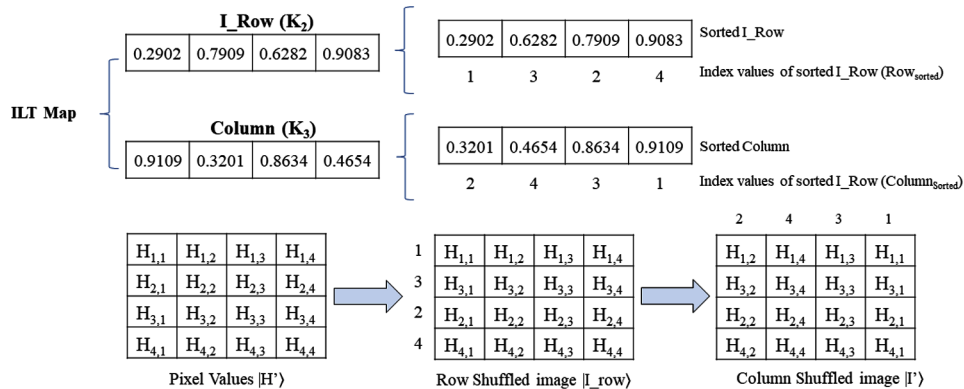
Step 9: Choose ‘r’ and ‘ y_n ’ (K_2) and iterate ILT map for ‘s’ times. To avoid transient effect, neglect the first 1000 iterations. Choose the chaotic sequence $I_Row = \{I_Row_{1001}, I_Row_{1002}, \dots, I_Row_s\}$ and sort I_Row to obtain the sorted index value as $Row_{sorted} = \{R_1, R_2, \dots, R_s\}$. Shuffle the rows of $|H'\rangle$ using Row_{sorted} to get $|I_row\rangle$.

Figure 9. (a and b) Wire diagram of proposed encryption (a) and decryption (b) algorithm



Step 10: Choose different ‘r’ and ‘y_n’ (K₃) values and iterate ILT map for ‘s’ times. To avoid transient effect, neglect the first 1000 iterations. Choose the chaotic sequence Column = {Column₁₀₀₁, Column₁₀₀₂, Column_s} and sort Column either in ascending or descending order to get the sorted index value as Column_{sorted} = {C₁, C₂, C_s}. Shuffle the columns of II_{row}) using Column_{sorted} to get II’). Figure.10 shows the example of row and column shuffle.

Figure 10. Row and Column Shuffled image



Step 11: Convert each row of II’ into its binary equivalent vector as,

$$|Row(i)\rangle = de2bi(|I’\rangle, 8) \tag{10}$$

where i =M (no. of rows in the image).

Step 12: Calculate the number of one's in $|Row\rangle$ and let it be $|N\rangle$.

Step 13: Compute $|D\rangle$ using equation (xi), if $|D\rangle=0$, then $|Row\rangle$ is right circular shifted by $|N\rangle$ times and if $|D\rangle=1$, then it is left circular shifted by $|N\rangle$ times and the resultant matrix be $|Row'\rangle$.

$$|D\rangle = \text{mod}(|N\rangle, 2) \quad (11)$$

Step 14: Convert each row of binary values into its decimal equivalent by using equation (xii), to get the encrypted image.

$$|I_{-1_{encrypt}}\rangle = \text{bi2de}(|Row'\rangle, 8) \quad (12)$$

Step 15: The final encrypted red plane ROI image is $|I_{-1_{encrypt}}\rangle$. The encrypted green and blue planes of ROI image are obtained by repeating steps 3 to 14 with the same key, and the final encrypted ROI is attained by concatenating the encrypted red, green and blue ROI planes.

RONI Encryption Process

Input: RGB DICOM RONI image.

Output: Encrypted RONI DICOM image.

Step 16: Split the RGB RONI DICOM image of the size $I \times J \times 3$ into red, green and blue planes.

Step 17: Transform the red plane of RONI image into NEQR quantum bit-plane representation as (13)

$$|RONI_{red}\rangle = \frac{1}{2^n} \sum_{Y=0}^{2^n-12^n-1} \sum_{X=0}^{2^n-12^n-1} \otimes_{i=0}^8 |C_{YX}^i\rangle |YX\rangle \quad (13)$$

Step 18: Repeat step 4 for ILT map (K_4) and transform it into NEQR quantum bit-plane representation. Operate CNOT gate by considering $|Key\rangle$ as control bit and $|RONI_{red}\rangle$ as target bit to get the encrypted RONI as $|RONI_{encrypt}\rangle$.

$$|Key\rangle = \frac{1}{2^n} \sum_{Y=0}^{2^n-12^n-1} \sum_{X=0}^{2^n-12^n-1} \otimes_{i=0}^8 |C_{YX}^i\rangle |YX\rangle \quad (14)$$

Step 19: Repeat steps 17 and 18 to get the encrypted green and blue RONI planes and the final encrypted RONI is attained by concatenating all the encrypted planes.

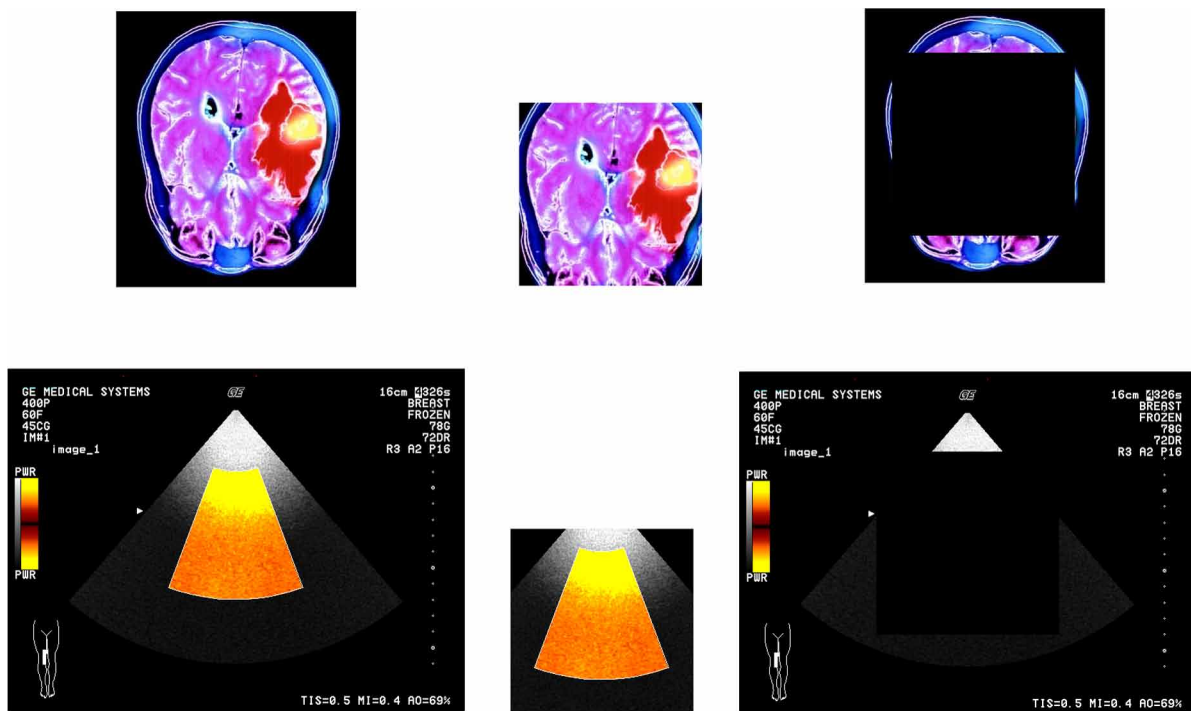
Step 20: Combine the encrypted ROI and RONI to get the encrypted image. The decryption procedure is the inverses of the encryption procedure as the qubits are invertible.

SIMULATION RESULTS AND ANALYSIS

The security of the projected scheme is demonstrated by using two 256×256 ROI RGB DICOM images as in Figure. 11 (a & d). The test images were taken from the web source (www.osirix-viewer.com) for various analysis. Owing to the deficiency of quantum computers, the proposed scheme is simulated in a personal laptop with Intel® Core™ i5 processor, 2.5GHz and 8GB RAM equipped with MATLAB R2016b. Further, the projected scheme is subjected to various attacks to prove that it is invulnerable to statistical, chosen plain text and differential attacks.

Figure 11 shows the different test images and their corresponding ROI and RONI images that are used in the proposed algorithm. Figure 12 (a-g) provides the various encryption stages output in ROI, Figure 13 (a-c) illustrates the output of RONI and Figure 14 (a-c) illustrates the output of the proposed algorithm.

Figure 11. Test images. (a) original image 1, (b) ROI 1, (c) RONI 1, (d) original image 2, (e) ROI 2, (f) RONI 2



EXHAUSTIVE ATTACK

Keyspace Analysis

Brute-force attack is also known as exhaustive attack. The hackers try to guess the key by checking all the possible keys. The proposed algorithm should have huge keyspace to counter-attack brute-force. In the proposed algorithm, for encrypting ROI, three sets of keys $Key_1 = \{K_1, K_2, K_3\}$ are used, and each

set contains two keys. Therefore, six secret keys are used for encrypting ROI. One set of keys ($Key_2 = \{K_4\}$) is used for encrypting RONI. So, the proposed algorithm uses four pairs of keys totalling eight secret keys. The keyspace of the proposed algorithm is 10^{112} , by setting the precision of each key to -14. Keyspace of 10^{112} is large enough to endure brute-force attack.

Key Sensitivity Analysis

The ILT and ILS maps are sensitive to the control parameters and the initial seed values. The sensitivity of ILT and ILS maps are tested by slightly differing one of the secret keys. Figure. 15 prove that even if a single bit is altered in the original key, the proposed algorithm cannot retrieve the original image. Figure. 15 (a and b) shows the ROI image 1 and encrypted ROI image 1 respectively. Figure 15 (c-e) shows the decrypted image from (b) with {Key set 1, Key set 2, Key set 3} respectively. Table 1 gives the precise and incorrect key sets.

Figure 12. Output of the ROI encryption scheme. (a) ROI 1, (b) Bit-plane shuffled 1, (c) CNOT 1, (d) Row and column shuffle 1, (e) encrypted ROI 1, (f) decrypted ROI 1

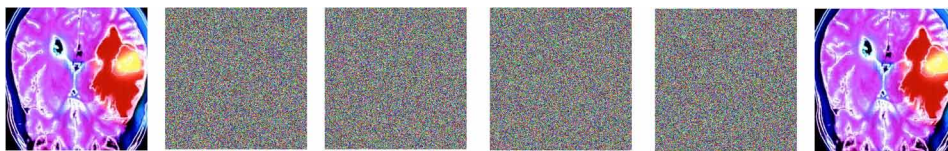


Figure 13. Output of RONI encryption scheme. (a) Original RONI 1, (b) encrypted RONI 1, (c) decrypted RONI 1

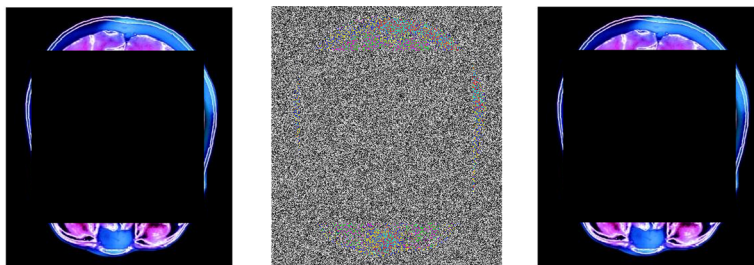


Figure 14. Output of the proposed encryption algorithm. (a) original image 1, (b) encrypted image 1, (c) decrypted image 1

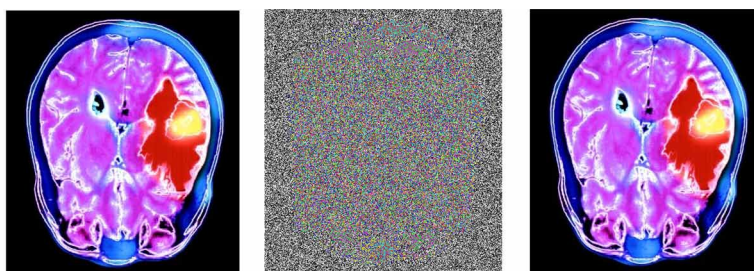


Figure 15. Key sensitivity test. (a) ROI 1, (b) encrypted image with Key, (c) decrypted image with Key set 1, (d) decrypted image with Key set 2, (e) decrypted image with Key set 3, (f) decrypted image with Key

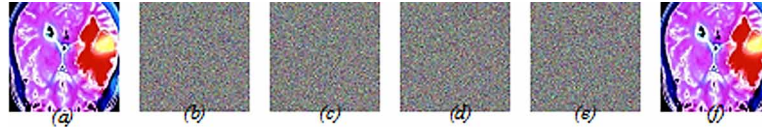


Table 1. Different keystets used for key sensitivity analysis

Values		Key	Key Set 1	Key Set 2	Key Set 3
K ₁	μ1	3.67676767676767	3.67676767676767	3.67676767676767	3.67676767676766
	x1	0.76767676767676	0.76767676767677	0.76767676767676	0.76767676767676
K ₂	r1	3.45645645645645	3.45645645645645	3.45645645645645	3.45645645645645
	y1	0.29029029029029	0.29029029029029	0.29029029029129	0.29029029029029
K ₃	r2	3.87687687687687	3.87687687687687	3.87687687687687	3.87687687687687
	y2	0.91091091091091	0.91091091091091	0.91091091091091	0.91091091091091
K ₄	r3	3.67676767676767	3.67676767676767	3.67676767676767	3.67676767676767
	y3	0.76767676767676	0.76767676767676	0.76767676767676	0.76767676767676

From this examination, it is clear that the proposed algorithm is susceptible to the key which means that the proposed algorithm can counterattack exhaustive attack.

Statistical Attack

By analysing the statistical nature of the cipher image hacker tries to gain knowledge about the key and the encryption algorithm. To examine the statistical nature and strength of the proposed algorithm against statistical attack, the proposed algorithm is subjected to various analysis like histogram analysis, correlation analysis, entropy and chi-square test. Table 2 provides the calculation of the percentage of 1's in all the bit planes. A suitable encryption algorithm should encrypt the image not only in pixel level but also in bit level. From Table 2, it is well-defined that the proposed algorithm encrypts the image perfectly even in bit-level.

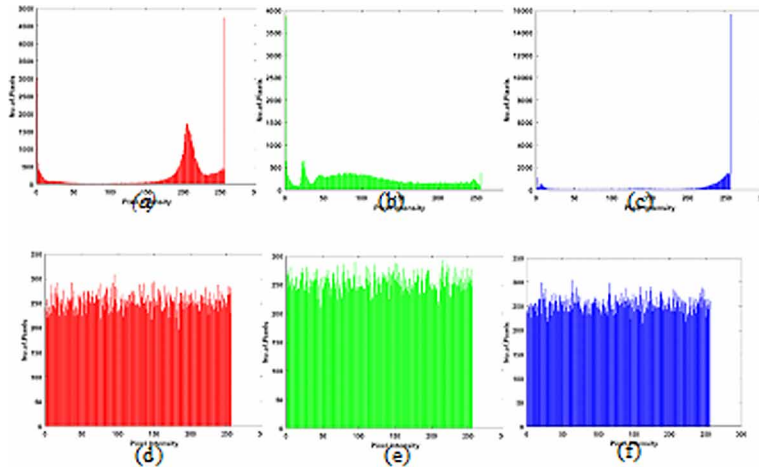
Histogram Analysis

The histogram is the graphical illustration of the Intensity level (x-axis) to the number of pixels (y-axis). Figure. 16 (a-c) gives the histogram of red, green and blue planes of ROI 1 images respectively. Figure. 16 (d-f) provides the histogram of red, green and blue planes of encrypted ROI 1 images respectively. From this, it is clear that the proposed algorithm produces a uniformly flat histogram for encrypted images even though the pixels are concentrated over the region in the original image.

Table 2. Percentage of 1's in ROI and encrypted ROI bit planes

Images/Planes		1	2	3	4	5	6	7	8	
ROI 1	Original	R	51.7608	51.0635	50.8987	52.7862	48.5504	35.6445	73.7258	82.7377
		G	47.5402	47.3007	47.6409	46.5667	48.5046	45.4849	49.4171	34.6069
		B	60.5636	61.2762	62.4496	63.6978	66.9693	74.3133	77.5726	78.9047
	Encrypted	R	49.8413	49.6505	50.2655	50.2090	50.1770	49.8992	50.2166	50.0152
		G	50.2105	49.9877	50.1678	49.9282	50.2258	49.6673	49.8962	50.1831
		B	50.2105	49.9877	50.1678	49.9282	50.2258	49.6673	49.8962	50.1831
ROI 2	Original	R	61.4196	60.4522	59.9868	60.9954	65.9027	45.4910	44.0948	42.5308
		G	47.6516	49.9435	47.7279	47.9599	51.9470	33.6517	32.3196	28.5736
		B	27.8640	26.7303	26.3168	27.2430	31.7077	11.1007	9.6984	8.1344
	Encrypted	R	49.8992	49.9893	50.0991	50.2517	49.9054	50.1754	49.8855	50.2029
		G	49.3164	49.9054	49.9420	49.9694	50.1052	49.8489	49.9847	49.6414
		B	50.0503	49.8825	49.6749	49.9969	50.2533	50.1403	49.9954	50.0915

Figure 16. Histogram analysis. (a) histogram of red plane in ROI 1, (b) histogram of green plane in ROI 1, (c) histogram of blue plane in ROI 1, (d) histogram of red plane in encrypted ROI 1, (e) histogram of green plane in encrypted ROI 1, (f) histogram of blue plane in encrypted ROI 1



Chi-Square (χ^2) Test

The uniform distribution of pixels in cipher image can be statistically understood with this test, and this is calculated by using (15),

$$\chi^2 = \sum_{m=i}^{256} \frac{(observed_i - expected_i)^2}{expected_i} \tag{15}$$

Medical Data Are Safe

where i is the level of intensity and the expected value is 256 for 256×256 image (Praveenkumar et al., 2015; Ravichandran et al., 2016.). Observed _{i} and expected _{i} in the equation are the original and expected values of the pixel from the histogram. For 255 degree of freedom, the significant levels for 5% and 1% are 293.2478 and 310.457 respectively. From Table 3 it is clear that the hypothesis is accepted for the 5% and 1% significant level which signifies the pixels are randomly distributed.

Table 3. Chi-Square analysis

Images	ROI 1			ROI 2		
	R	G	B	R	G	B
χ^2 Value	287.1484	227.8984	228.1875	252.8984	281.7734	248.5313
Decision	Accept	Accept	Accept	Accept	Accept	Accept

Correlation Analysis

Correlation gives the amount of relationship between a pair of adjacent pixels in the image, and this is estimated using equation (16). It is evident that in the plain image the pixels have a strong relationship with neighbouring pixels, but in the cipher image, the statistical relationship between the adjacent pixels should be reduced to withstand statistical attack. Figure 17 (a-c) shows the correlation of ROI 1 and (d-f) shows the correlation of encrypted ROI 1. Table 4 gives the correlation analysis of the proposed algorithm in all the three (X, Y and Z) directions. The value of correlation indicates that the suggested algorithm can withstand statistical attack.

$$Correlation_{mn} = \frac{cov(m, n)}{\sqrt{D(m)}\sqrt{D(n)}} \tag{16}$$

$$cov(m, n) = \frac{1}{N} \sum_{i=1}^N (m_i - E(m))(n_i - E(n)),$$

$$D(m) = \frac{1}{N} \sum_{i=1}^N (m_i - E(m))^2 \quad E(m) = \frac{1}{N} \sum_{i=1}^N m_i$$

Entropy Analysis

Global Shannon entropy is used for evaluating the randomness of the information, and this can be calculated by (17),

$$Entropy(\alpha) = -\sum_{i=0}^{2^N-1} p(\alpha_i) \log_2 p(\alpha_i) \tag{17}$$

$p(\alpha_i)$ is the probability of occurrence of symbol α . For a random image with 2^N symbols, the entropy should be close to N . For an RGB DICOM image, in each plane, the grayscale range will be 2^8 and if it is assumed that each level of gray is equiprobable and then the theoretical value of entropy will be 8. From the Table 5 and Table 6, it is evident that the calculated values are close to 1 and 8 in the bit planes and in the encrypted images respectively. The proposed algorithm can generate highly random cipher image and can withstand statistical attack.

Table 4. Correlation analysis of the proposed algorithm

Images			Horizontal	Vertical	Diagonal
ROI 1	Original	R	0.9399	0.9764	0.9262
		G	0.9264	0.9667	0.9029
		B	0.9595	0.9833	0.9472
	Diffused	R	0.0032	-0.0039	0.0048
		G	-0.0051	0.0035	0.0030
		B	-0.0087	0.0024	0.0050
ROI 2	Original	R	0.9868	0.9868	0.9808
		G	0.9683	0.9663	0.9543
		B	0.8939	0.8934	0.8574
	Diffused	R	0.0030	-0.0035	-0.0051
		G	-0.0045	-0.0015	-0.0016
		B	0.0048	0.0039	0.0042

Figure 17. Correlation analysis. (a) horizontal correlation of ROI 1, (b) vertical correlation of ROI 1, (c) diagonal correlation of ROI 1, (d) horizontal correlation of encrypted ROI 1, (e) vertical correlation of encrypted ROI 1, (f) diagonal correlation of encrypted ROI 1

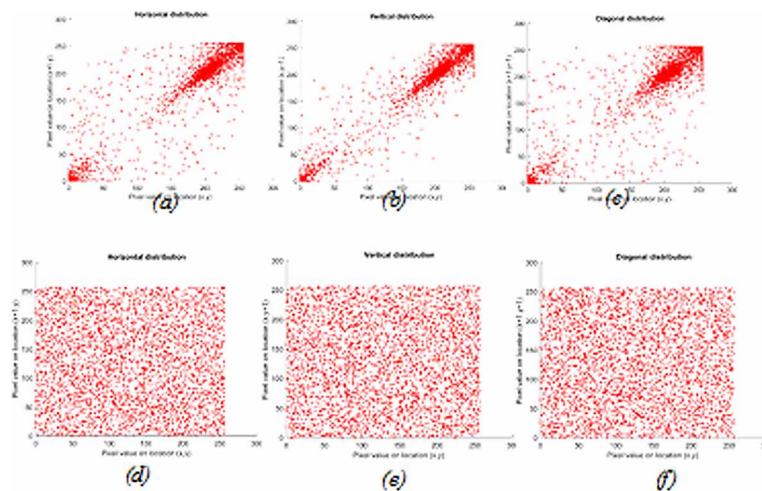


Table 5. Entropy analysis of ROI image and encrypted ROI image in bit planes

Images/Planes		1	2	3	4	5	6	7	8	
ROI 1	Original	R	0.9991	0.9996	0.9997	0.9977	0.9993	0.9396	0.8308	0.6636
		G	0.9982	0.9978	0.9983	0.9965	0.9993	0.9941	0.9999	0.9305
		B	0.9675	0.9629	0.9548	0.9451	0.9152	0.8219	0.7678	0.7433
	encrypted	R	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999	1.0000
		G	0.9999	1	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999
		B	1	0.9999	0.9999	0.9999	0.9999	1	0.9999	0.9999
ROI 2	Original	R	0.9620	0.9682	0.9710	0.9648	0.9257	0.9941	0.9899	0.9838
		G	0.9984	0.9999	0.9985	0.9987	0.9989	0.9214	0.9078	0.8631
		B	0.8535	0.8375	0.8314	0.8449	0.9011	0.5029	0.4593	0.4068
	encrypted	R	0.9999	1	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999
		G	0.9998	0.9999	0.9999	1	0.9999	0.9999	1	0.9999
		B	0.9999	0.9999	0.9999	1	0.9999	0.9999	1	0.9999

Table 6. Entropy analysis of original ROI and encrypted ROI images

Images/Directions	Original			Encrypted		
	R	G	B	R	G	B
ROI 1	6.7001	7.7369	6.1922	7.9968	7.9974	7.9974
ROI 2	4.8030	6.2290	4.4097	7.9972	7.9968	7.9972

Differential Attack

Number of pixel change rate (NPCR) and Unified Average Change in Intensity (UACI) gives the number of pixels transformed and the mean difference between two cipher images. A pair of cipher images is obtained from the original image after encryption and other one by changing a pixel value in the plain image. The proposed framework should produce different cipher images even if there is a single pixel change in the plain image. This is calculated by using (18) and (19),

$$NPCR = \frac{\sum_{mn} Image(m, n)}{H \times W} \times 100\% \tag{18}$$

$$UACI = \frac{1}{H \times W} \left(\frac{|Image_1(m, n) - Image_2(m, n)|}{255} \right) \times 100\% \tag{19}$$

$$Image(m, n) = \begin{cases} 0 & \text{if } Image_1(m, n) = Image_2(m, n) \\ 1 & \text{if } Image_1(m, n) \neq Image_2(m, n) \end{cases}$$

where H and W denote the column and row size of the image, Image₁ and Image₂ are the two cipher images before and after a pixel change in the plain image. The NPCR and UACI values are listed in Table 7 and 8 and from this table, it is evident that both the values are in the optimum range. The values are compared with critical value as in (Wu et al., 2011), and from this, it can be decided that the proposed algorithm can endure differential attacks.

Table 7. UACI values

Images		UACI (%)	UACI Critical Values		
			U ⁻ _{0.05} = 33.2824% U ⁺ _{0.05} = 33.6447%	U ⁻ _{0.01} = 33.2255% U ⁺ _{0.01} = 33.7016%	U ⁻ _{0.001} = 33.1594% U ⁺ _{0.001} = 33.7677%
ROI 1	R	33.4418	PASS	PASS	PASS
	G	33.4560	PASS	PASS	PASS
	B	33.4539	PASS	PASS	PASS
ROI 2	R	33.4393	PASS	PASS	PASS
	G	33.4669	PASS	PASS	PASS
	B	33.403	PASS	PASS	PASS

Table 8. NPCR values

Images		NPCR (%)	NPCR Critical Values		
			NPCR *0.05 = 99.5693%	NPCR *0.01 = 99.5527%	NPCR *0.001 = 99.5341%
ROI 1	R	99.5941	PASS	PASS	PASS
	G	99.5971	PASS	PASS	PASS
	B	99.5910	PASS	PASS	PASS
ROI 2	R	99.6093	PASS	PASS	PASS
	G	99.6017	PASS	PASS	PASS
	B	99.6048	PASS	PASS	PASS

Performance Comparison Analysis

Table 9 provides a comparison analysis of the proposed algorithm with recent studies available in Literature.

Entropy, correlation, NPCR and UACI values of the proposed algorithm are compared with the existing algorithms. (Abd El-Latif et al., 2017; Fu et al., 2013, 2014; Helmy et al., 2017; Li et al., 2016; Praveenkumar et al., 2015; Ravichandran et al., 2016, 2017; X.-Y. Wang et al., 2015; S. Zhang et al., 2014). The values are provided in Table 7 and from these values, it is obvious that the proposed algorithm can withstand different attacks. Table 10 provides the detailed description, advantages and disadvantages of the similar encryption schemes available in literature with the proposed methodology.

Table 9. Performance Comparison Analyses

	Correlation			Entropy	UACI	NPCR
	Horizontal	Vertical	Diagonal			
(Abd El-Latif et al., 2017)	-0.0027	-0.0119	-0.0053	7.98913	33.5018	99.63
(Praveenkumar et al., 2015)	-0.0033	0.0033	0.0117	7.9975	33.45	99.62
(Ravichandran et al., 2016)	-0.0519	-0.0385	0.00046	7.9992	33.37	99.996
(Ravichandran et al., 2017)	-0.0025	-0.0016	0.0116	7.9972	33.4399	99.5982
(Fu et al., 2014)	NA	NA	NA	7.9992	33.48	99.60
(S. Zhang et al., 2014)	-0.0154	0.0193	0.0032	NA	NA	NA
(Fu et al., 2013)	-0.0061	0.0122	-0.0197	7.9993	NA	NA
(Li et al., 2016)	0.0043	0.0046	0.00315	7.9954	NA	NA
(X. Wang & Liu, 2017)	-0.0011	-0.0016	0.0012	7.9974	33.44	99.61
(Helmy et al., 2017)	0.00183	NA	NA	NA	NA	NA
Proposed	-0.0012	0.00014	0.0017	7.9971	33.4435	99.5997

Table 10. Pros and Cons of the proposed scheme with the literature study

Title	Description	Advantages	Disadvantages
A Novel LSB Based Quantum Watermarking.(Heidari & Naseri, 2016)	Based on the m-bit embedding key, the watermark image is embedded in the LSB of the cover image.	No attacker can reach the watermarked secret image.	The cover image is not retrieved. In medical image watermarking, the cover image is required. Hence, this method is not applicable to medical images.
Adynamic watermarking scheme for quantum images using quantum wavelet transform.(Song et al., 2013)	The embedding capacity is controlled based on the dynamical diagonal vector which is based on the carrier and watermark images.	Max capacity is achieved.	The cover image is not retrieved. Therefore, this method cannot be utilised for medical systems.
Quantum image encryption based on Scrambling- Diffusion (SD) approach. (Beheri et al., 2016)	The image is confused by utilising the Arnold cat map and Fibonacci transformation and then diffused by gray-code.	Can be applied to all image formats.	The optimum values are not achieved.
Robust Encryption of Quantum Medical Images.(El-latif, Abd-el-atty, & Talha, 2017)	The medical image is confused by using the gray-code and then diffused by utilising the CNOT gate.	The proposed method is robust, and higher efficiency when compared to its classical counterpart.	The optimum values are not achieved.
Proposed methodology	Medical image encryption algorithm utilising quantum concepts together with SHA-512, quantum bit plane arrangements, gates and Integrated coupled Logistic maps using Tent and Sine maps.	<ul style="list-style-type: none"> • Can be used for all image formats • Can be implemented both in the selective and complete image regions 	Lack of quantum computers.

FUTURE RESEARCH DIRECTIONS

The proposed encryption scheme can be extended by adopting a unitary matrix to preserve entropy. Also, Hadamatrix can be integrated to achieve image compression.

CONCLUSION

This chapter proposes a quantum assisted image encryption scheme to safeguard DICOM images when transmitted over public networks. The proposed scheme uses NEQR procedure to convert the classical DICOM into quantum image format. Further, to reduce the channel overload the quantum converted DICOM is divided into ROI and RONI. Further by applying the chaotic key generated by the combined Logistic Sine and Tent maps, permutation was carried out in the ROI image. Additionally, the integrity of the proposed work is upheld by adopting the hash mechanism in the permuted ROI. Finally, CNOT gate operation was carried out between the RONI and the generated chaotic key. Encrypted ROI and RONI were combined to produce the uncorrelated cipher image output. Encryption metrics were evaluated to validate confusion, permutation and diffusion operations in the proposed encryption scheme.

ACKNOWLEDGMENT

The authors wish to acknowledge SASTRA Deemed University, Thanjavur, India for extending infra-structural support to carry out this work.

REFERENCES

- Abd El-Latif, A. A., Abd-El-Atty, B., & Talha, M. (2017). Robust Encryption of Quantum Medical Images. *IEEE Access: Practical Innovations, Open Solutions*, 6, 1073–1081. doi:10.1109/ACCESS.2017.2777869
- Beheri, M. H., Amin, M., Song, X., & El-latif, A. A. A. (2016). Quantum image encryption based on Scrambling- Diffusion (SD) approach. *Frontiers of Signal Processing (ICFSP)*, (2), 43–47.
- Chai, X., Zheng, X., Gan, Z., Han, D., & Chen, Y. (2018). An image encryption algorithm based on chaotic system and compressive sensing. *Signal Processing*, 148, 124–144. doi:10.1016/j.sigpro.2018.02.007
- Deutsch, D. (1985). Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 400(1818), 97–117. 10.1098/rspa.1985.0070
- El-latif, A. A. A., Abd-el-atty, B., & Talha, M. (2017). *Robust encryption of quantum medical images*. Academic Press.
- Feynman, R. P. (1982). Simulating Physics With Computers By R P Feynman.pdf. *International Journal of Theoretical Physics*, 21(6–7), 467.
- Fridrich, J. (1998). *Symmetric Ciphers Based on Two-Dimensional Chaotic Maps*. Academic Press.

Medical Data Are Safe

Fu, C., Meng, W., Zhan, Y., Zhu, Z., Lau, F. C. M., Tse, C. K., & Ma, H. (2013). An efficient and secure medical image protection scheme based on chaotic maps. *Computers in Biology and Medicine*, 43(8), 1000–1010. doi:10.1016/j.combiomed.2013.05.005 PMID:23816172

Fu, C., Zhang, G., Bian, O., Lei, W., & Ma, H. (2014). A Novel Medical Image Protection Scheme Using a 3-Dimensional Chaotic System. *PLoS One*, 9(12), e115773. doi:10.1371/journal.pone.0115773 PMID:25541941

Global Overview. (2018). Retrieved from https://public.dhe.ibm.com/common/ssi/ecm/55/en/55017055usen/2018-global-codb-report_06271811_55017055USEN.pdf

Healthcare Data Breach Statistics. (n.d.). Retrieved September 11, 2018, from <https://www.hipaajournal.com/healthcare-data-breach-statistics/>

Heidari, S., & Naseri, M. (2016). A Novel LSB Based Quantum Watermarking. *International Journal of Theoretical Physics*, 55(10), 4205–4218. doi:10.1007/10773-016-3046-3

Helmy, M., El-Rabaie, E.-S. M., Eldokany, I. M., & El-Samie, F. E. A. (2017). 3-D Image Encryption Based on Rubik's Cube and RC6 Algorithm. *3D Research*, 8(4), 38.

Latorre, J. I. (2005). *Image compression and entanglement*. Retrieved from <http://arxiv.org/abs/quant-ph/0510031>

Li, X., Wang, L., Yan, Y., & Liu, P. (2016). An improvement color image encryption algorithm based on DNA operations and real and complex chaotic systems. *Optik - International Journal for Light and Electron Optics*, 127(5), 2558–2565.

MIFA Shares Industry Wisdom on Medical Identity Theft and Fraud. (n.d.). Retrieved September 11, 2018, from <https://www.hipaajournal.com/mifa-shares-industry-wisdom-on-medical-identity-theft-and-fraud-3657/>

Osiri, X. DICOM Viewer | DICOM Image Library. (n.d.). Retrieved December 21, 2018, from <http://www.osirix-viewer.com/resources/dicom-image-library/>

Peres, A. (1985). Reversible logic and Quantum Computers. *Physical Review A*, 32(6), 3266–3276. doi:10.1103/PhysRevA.32.3266 PMID:9896493

Praveenkumar, P., Amirtharajan, R., Thenmozhi, K., & Balaguru Rayappan, J. B. (2015). Medical Data Sheet in Safe Havens - A Tri-layer Cryptic Solution. *Computers in Biology and Medicine*, 62(C), 264–276. doi:10.1016/j.combiomed.2015.04.031 PMID:25966921

Ravichandran, D., Praveenkumar, P., Balaguru Rayappan, J. B., & Amirtharajan, R. (2016). Chaos based crossover and mutation for securing DICOM image. *Computers in Biology and Medicine*, 72, 170–184. doi:10.1016/j.combiomed.2016.03.020 PMID:27046666

Ravichandran, D., Praveenkumar, P., Rayappan, J. B. B., & Amirtharajan, R. (2017). DNA Chaos Blend to Secure Medical Privacy. *IEEE Transactions on Nanobioscience*, 16(8), 850–858. doi:10.1109/TNB.2017.2780881 PMID:29364129

- Sang, J., Wang, S., & Niu, X. (2016). Quantum realization of the nearest-neighbor interpolation method for FRQI and NEQR. *Quantum Information Processing*, *15*(1), 37–64. doi:10.1007/11128-015-1135-5
- Song, X. H., Wang, S., Liu, S., Abd El-Latif, A. A., & Niu, X. M. (2013). A dynamic watermarking scheme for quantum images using quantum wavelet transform. *Quantum Information Processing*, *12*(12), 3689–3706. doi:10.1007/11128-013-0629-2
- Toffoli, T. (1980). *Reversible computing*. Berlin: Springer. doi:10.21236/ADA082021
- Venegas-Andraca, S. E., & Ball, J. L. (2010). Processing images in entangled quantum systems. *Quantum Information Processing*, *9*(1), 1–11. doi:10.1007/11128-009-0123-z
- Venegas-Andraca, S. E., & Bose, S. (2003). *Storing, processing, and retrieving an image using quantum mechanics*. Academic Press.
- Wang, M., Wang, X., Zhang, Y., & Gao, Z. (2018). A novel chaotic encryption scheme based on image segmentation and multiple diffusion models. *Optics & Laser Technology*, *108*, 558–573. doi:10.1016/j.optlastec.2018.07.052
- Wang, X., & Liu, C. (2017). A novel and effective image encryption algorithm based on chaos and DNA encoding. *Multimedia Tools and Applications*, *76*(5), 6229–6245. doi:10.1007/11042-016-3311-8
- Wang, X.-Y., Zhang, Y.-Q., & Bao, X.-M. (2015). A novel chaotic image encryption scheme using DNA sequence operations. *Optics and Lasers in Engineering*, *73*, 53–61. doi:10.1016/j.optlaseng.2015.03.022
- Wu, Y., Member, S., Noonan, J. P., & Member, L. (2011, April). NPCR and UACI Randomness Tests for Image Encryption. *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications*, 31–38.
- Zhang, S., Gao, T., & Gao, L. (2014). A Novel Encryption Frame for Medical Image with Watermark Based on Hyperchaotic System. *Mathematical Problems in Engineering*, *2014*, 1–11. doi:10.1155/2014/917147
- Zhang, Y., Lu, K., Gao, Y., & Xu, K. (2013). A novel quantum representation for log-polar images. *Quantum Information Processing*, *12*(9), 3103–3126. doi:10.1007/11128-013-0587-8
- Zhou, Y., Bao, L., & Chen, C. L. P. (2014). A new 1D chaotic system for image encryption. *Signal Processing*, *97*, 172–182. doi:10.1016/j.sigpro.2013.10.034


This research was previously published in Medical Data Security for Bioengineers; pages 142-165, copyright year 2019 by Medical Information Science Reference (an imprint of IGI Global).

Chapter 14

Quantum Cryptography

Key Distribution: Quantum Computing

Bhanu Chander

 <https://orcid.org/0000-0003-0057-7662>

Pondicherry University, India

ABSTRACT

Quantum cryptography is actions to protect transactions through executing the circumstance of quantum physics. Up-to-the-minute cryptography builds security over the primitive ability of fragmenting enormous numbers into relevant primes; however, it features inconvenience with ever-increasing machine computing power along with current mathematical evolution. Among all the disputes, key distribution is the most important trouble in classical cryptography. Quantum cryptography endows with clandestine communication by means of offering a definitive protection statement with the rule of the atmosphere. Exploit quantum mechanics to cryptography can be enlarging unrestricted, unfailing information transmission. This chapter describes the contemporary state of classical cryptography along with the fundamentals of quantum cryptography, quantum protocol key distribution, implementation criteria, quantum protocol suite, quantum resistant cryptography, and large-scale quantum key challenges.

INTRODUCTION

Cryptography is learning process for transfer secret information or intelligence by using mathematical operations, only applying secret or specific key the intended receipts can read or gets the original message. The message which is revolved around a masquerading structure process is called encryption. Converting masquerading text messages to plain text is called decryption. The key which makes plain text to cipher text is called the encryption key, coming to the receiver's end the key which makes cipher text to plain text is called the decryption key. Our standing statement will be that any time a person sends a message, that person has to send it over an unrestricted medium, so that anybody who wishes can pick it up. So,

DOI: 10.4018/978-1-7998-8593-1.ch014

the eavesdropper can take delivery of any message that A and B send to each other. The point, then, is to make it so that even though eavesdropper can see the message, it just looks like twaddle to her/him: she can't right to use the content of the message. Cryptography is the encounter among A and B on one track and eavesdropper on the other track. In a variety of times in the past, A and B have had the superior hand. At other times, the eavesdropper has been on top. At the current scenario, it seems that A and B are winning, but eavesdropper is inflexible at work trying to recapture her/his lead.

In cryptography, the procedures which are apply to shield information are achieved from mathematical theories and a set-of-rule based computations acknowledged as algorithms to translate messages in ways that create it tough to decode it. These algorithms are exploiting for cryptographic key generation, digital signing, and certification to protect data privacy, web browsing on internet and to shelter top secret dealings like credit and debit card dealings. The uncertainty law of quantum physics fabricates the most primitive fundamentals for quantum cryptography. Through quantum computers future being estimated to answer discrete logarithmic crisis as well as the commonly known cryptography schemes like AES, RSA, DES, quantum cryptography turn out to be the forecasted solution. In observation it is exploit to set-up a mutual, secret along with arbitrary sequence of bits to communicate among two arrangements, for instance take A and B. This set-up is acknowledged as Quantum Key Distribution. Subsequent to this key is shared among A and B, additional swapping of information can take place in the course of well-known cryptographic techniques.

In cryptography main role taken by keys, based on the chosen key cryptography split into two styles Symmetric or secret-key cryptography and Asymmetric key or public-key cryptography (Bennett and Brassard, 1987; Ekert 1991; Zhao and Qi, 2006; Padmavathi and Vishnu, 2016; NIST, 2016).

- **Secret Key Cryptosystem:** In secret-key cryptography, just a single key is shared within dispatcher as well as the recipient that key sustain for encryption as well as decryption which will keep as secret. That's the reason to call it a secret key or symmetric key cryptography. Security mainly established on problematical nonproven algorithms, most importantly it depends upon protected medium on behalf of key distribution.
- **Public Key Cryptosystem:** In asymmetric cryptography, two keys are used public and private keys, the private key is used to encrypt the messages and the public key is used to decrypt the encrypted message. Security is based on computational mathematical assumptions, most of the security algorithms found on non-proven mathematical assumptions.

CLASSICAL CRYPTOGRAPHY

Confidentiality is the topmost priority for cryptography. To accomplish this objective an innovation called cryptosystem is revealed. It used to join information along with some supplementary material or knowledge well-known as key and fabricate as a cryptogram. Sending secret messages is the principal application for cryptography. Most of the cryptosystems are depending on computational mathematical hypothesis; encryption and decryption are must equivalent by solving some computational difficult problems. The main problem is the distribution of keys or key distribution which can be solved by two methods one is mathematical assumptions known as classical cryptography and another method is Physics known as Quantum cryptography. Classical cryptography depends over computational difficulties

Quantum Cryptography Key Distribution

of factoring large integer numbers but quantum cryptography depends over universal laws of Quantum Mechanics (Bennett and Brassard, 1987; Peev, 2009; Vasileios and Kamer, 2018; Alfred and Pal, 2018; Guru and Raghu, 2016; Diff, 1976).

Suppose that Alice and Bob communicating over insecure transmission medium and encryption, decryption is done with the best of accepted cryptography algorithm which is most probably intractable by any accepted computing structure. At this time imagine here an Eve as an intruder who continuously listening over the communicational channel where Alice and Bob sending and receiving intelligence messages. Assume Alice and Bob use the factoring method then Eve also can make use of Factoring to break the key communication and steal the important data. The limitation of symmetric key cryptography is key sharing and it is the main reason since asymmetric cryptosystem gaining importance over symmetric one-time pad algorithm. Recent times Elliptic curve cryptography (ECC) acknowledged as state-of-the-art crypto and mostly handle for guaranteed financial transactions (Diff, 1976; Vasileios and Kamer, 2018; Alfred and Pal, 2018; Mateusz, 2018; Yin and Chen, 2016; Bennet and Brassard, 1982).

Because of computational complex calculations, public-key cryptography turns into as sluggish, mainly engaged toward swap keys. For instance, to distribute keys among two distant parties we may use most widely developed explanations such as RSA and Diffie-Hellman key formats. Nevertheless, asymmetric key is somewhat slower than symmetric key because of computation. Many people proposed hybrid models that combine the advantages of both cryptosystems to give better results in terms of security. These types of schemes exploit the speed of performance with speed of secret key design although power the adaptability of asymmetric cryptography. At the same time, existing asymmetric crypto methods are first-rate along with adequate on the way to provide confidentiality with integrity levels, but they may be exposed to a handful of risks. For example, the innovations in computer processing like quantum computing can proficient to decode the application like RSA, etc., in a timely manner so making public cryptosystems straight away out of fashion. Asymmetric cryptosystems like RSA plus Diffie-Hellman algorithms aren't more situated on mathematical testimonies. Above mentioned schemes reasonably measured as secured based on the elementary progression of factoring great integers into their primes. Thus the power of these algorithms is factoring of large prime numbers and till now there is no computer process that has the power of computing mathematical operation which can quickly compute the factoring of very large numbers. In a minute understanding take a look at DES symmetric key cryptography which was once considered as the first more secure algorithm, it contains 64-bit key length but mainly its key length is 56 bit remaining 8-bit keys are used to check error rate in data. But it is no longer secured as think; progression in machinery prepared it will inconsiderable to overthrow. But the reality is with the intention of modern mainframes can break the DES algorithm within a day or a few hours of time. After DES breakability Advanced Encryption Standard takes the position of Security. It has key lengths of 128,192,256 bits as we increase the key length security of algorithm increases but this public algorithm vulnerable to coming advancements in computing technologies. Another interesting fact is, breakable theorems might elaborate in upcoming or while back developed algorithms may modify to compute factors of enormous integers into respective primes in time comportment. Moreover, present no realizable witness is stated that it is impracticable to build up such a separating algorithm. From the above discussions asymmetric key crypto schemes are defenseless to insecurity concerning in future those type algorithms may be created (Johnson and Colin, 2002; Padmavati and Vishnu, 2016; Rosenberg and Harington, 2007; Shor, 1997; Vasileios and Kamer, 2018; Alfred and pal, 2018; Bennett and Brassard, 1982).

Modern Cryptography Key Distribution

Traditional cryptography key distribution is the main problem. In previous times people by sending through a physical medium (like a disk which contains the key) they believe that the problem is solved, but in the present digital world, this experiment is clearly impracticable. There is no possible way to check whether the medium is interrupted, whether its stuffing copied or not. To overcome this problem many researchers and scientists of the British invented a solution by using a padlock. For example, assume a scenario that two parties are communicating with each other before that communication the intended receiver sends one open padlock to the party which sends important information at the same time it keeps its own secret key. By using this open padlock sender will defend information, then the receiver is the solitary party who can undo information through the help of the key that he kept. Formally those padlocks are mathematical expressions known as “one-way function” because they can easily compute but hard to reverse (Brassard, 1998)

Many public-key algorithms are slow; the reason is complex computations. So the length of the key selection must be in a careful manner. In principle, the invaders who have indeed records of communication must have to wait for powerful computers enough to break communication. Classical cryptosystems are good for one to two years to keep valuable information keep secretly such as credit card numbers but when it comes the matter of information has to keep secret for a decade. Then three inventors came and propose RSA algorithm a new cryptography algorithm “which takes millions of years to break” and they are given the challenge to break the code for 100 dollars however this code is later broken by a group of scientists over the internet in 1994 (Bennett, 1982; Brassard, 1992). The second thing is public-key cryptography is vulnerable to progress against mathematical operations. There are many efforts are done on mathematics directed toward turnout that public crypto-system be secured. Till now notably no such algorithm is determined which can perform reversing one-way function for factors of primes. But the discovery of such algorithms can make difficult to public-key security to insecure. It has more interest and problematic to access the speed of a hypothetical process than that of scientific advances. Here is proof for this in the past of mathematics, where one person can capable to answer a dilemma, the same dilemma can be kept busy for years or decades. There are more possible chances for designing such an algorithm which can reverse the factor numbers one way function. Maybe the algorithm is already revealed but reserved in top secret. These all things basically mean that asymmetric cryptography is not more secure in future moreover can't guarantee future proof of key distribution (Omar and Shawkat, 2018; Alfred and pal, 2018; Guru and Raghupathy, 2016; Bennett and Brassard, 1982; Mullins and Justin, 2003).

One Time Pad Encryption Technique

Most of the symmetric and asymmetric cryptosystems are has combined the personality of the encryption algorithm (E) through plain text (P) is restored to cipher cryptosystem (C) which could openly well-known since such communications security mostly depends on Key (K). But which is secretly shared between sender and receiver and one more essential hypothesis of a cryptosystem is Kirchhoff's algorithm where privacy is necessity exist in key, not on the method. Alice produces cryptogram $C = E_k(P)$, throw it to Bob who decrypts it by $P = (E)^{-1}_k(C)$ to recovering the original plain text P. this entire process is run under the Eva eye surroundings. Numerous cryptography techniques are presented based on this simple principle some are secured and some can able to break depending on recent advancements in technology. But one algorithm invented in 1917 named “One-time pad” is provably unbreakable. In this both

Quantum Cryptography Key Distribution

Alice as well as Bob detachment a magnitude of top-secret key objects consists of arbitrary characters like letters, bits, digits which is as large as a transmitted message. Take a look on the principle $C_i = P_i + K_i \pmod{N}$ describe where Alice Sending message $P = (p_1, p_2, \dots, p_n)$ p will be in digits, bits, numbers and by using his own Key $K = (k_1, k_2, \dots, k_n)$ produce the cryptosystem $C = (c_1, c_2, \dots, c_n)$ by applying interchangeable mathematics with base N . when bob receives cryptosystem C , using interchangeable mathematics subtracts key from C to recover the original message P . In 1949 Shannon with information hypothesis proves that this cryptosystem is protected and key material is truthfully unsystematic moreover exploited for only once, advantages like speed, left to right encipherment.

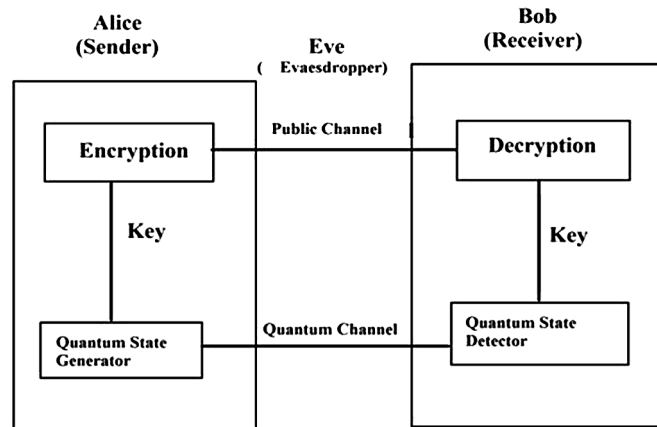
If the one-time pad is resistant then why it not at all utilizable why we are using factorial cryptosystems, reason is one-time pad involves key distribution, key management, and key management problems. At the beginning of crypto, Alice has to create accidental numbers that are not simple like appear. The system generated pseudo-random numbers will not give a secure secret key because it will generate the same sequence always. One key is generated by Alice to encrypt any message Alice should organize a replica for Bob to attain key, without giving any knowledge to Eve strictly a smooth fractional understanding of key. Possible chance is there if both Alice and Bob meet before communication and transfer key to each other, then key distribution is done securely but this does not happen every time. If they are not meet before and no secret key is shared and Alice can't simply send key substance to Bob since the foremost application in cryptosystems is broadcast which disposed to reactive eavesdroppers where Eve easily gets the key material. One easy way to avoid this one-time pad is, it requires encrypting with another one time pad. One time pad is indestructible, but in theory it is extremely tricky to utilize, through taking this motive public-key cryptosystems are complex but not impracticable to crack and simple to apply (Johnson and Colin, 2002; Omar and Shawkat, 2018; Mateusz, 2018; Peev, 2009; Vasileios and Kamer, 2018; Bennett and Brassard, 1982; Seema, 2017).

QUANTUM CRYPTOGRAPHY

Quantum cryptography idea first programmed in the late 1970s now it is the field handles for information security. Quantum crypto mainly used to develop crypto protocols that are used to defend quantum circumstances that have material goods that can't imitative. One of the most important advantages of quantum cryptography is which gives a piece of faultless sheltered information transmits. The first successful quantum cryptographic machine transmits top-secret key over 30 centimeters with polarized light (Bennett and Brassard, 1982; Seema, 2017). Besides other cryptosystems that perform computational complication of factoring huge integers, quantum crypto performs on the basic, fixed ideology of quantum technicalities. Mainly quantum crypto takes a Break on top of two supporter mechanics Heisenberg uncertainty principle as well as the principle of photon polarization. Without disturbing the system it cannot achievable to determine any quantum classification position accordingly polarization of photon in other words a light particle can only be identified at the point when it is measured. The above-indicated approach shows the main function at eavesdropper to uncomfortable in quantum cryptosystems. Second thing the photon polarization principle illustrates how the light particle can polarize in particular directions. While filtering a photon acceptable polarization filter will only discover a polarized photon or else shattered. In 1984 with the help of these most attractive principles as part of physics and information, two scientists named Charles H. Bennet along with Gilles Brassard promote the theory of quantum cryptosystem. Both of them believe corresponds to the fact that light can behave light waves

in addition to the characteristics of particles. Photons usually polarized in a variety of directions and these directions experience signify bits which corresponding to ones and zeros. These bits are utilized to generate secret keys for one time pad and some other public-key methods (Shor, 2000; Omar and Shawkat, 2018; Mateusz, 2018; Peev, 2009; Vasileios and Kamer, 2018; Bennett and Brassard, 1982; Seema, 2017; Bennett and Brassard, 1992).

Figure 1. Quantum cryptosystem model for solidly transmit arbitrary key



Light is generally applied to interchange information in telecommunication networks. Where each and every bit of information is taken as pulse, a pulse is released and sent over optical fiber to the receiver here is registered and transferred backward as electronic signals each pulse typically contains millions of particles of light which pronounced as Photons. The same thing is followed in quantum cryptography, a single photon contains an extremely small amount of light which came from laws of quantum physics moreover it cannot divide into fractions; it means eavesdroppers cannot measure the value of bit with the help of half photon. If the eavesdroppers want to know the bit value, he must observe the photon completely then only he can interrupt and disturb the communication. Another intelligent strategy for eavesdroppers can spot the photons, record the rate of that photon and set up a cloned photon, propel it to the intended beneficiary. But in quantum cryptography, two parties co-operate each other to prevent eavesdroppers from doing such types of actions (Bennett, 1992; Tang and Chen, 2014; Yin and Chen, 2016; Seema, 2017; Shor, 2002).

Difference Between Classical and Q-Bits

Classical knowledge represented in classical bits as 0 and 1. Mentioned classical bits are mostly used in classical or traditional cryptosystems. Q-bits: quantum cryptography mechanism works with quantum bits additionally known as Q-bits. Q-bits are different from classical bits mostly take superposition values between zero and one and they can't be copied.

In BB84 Alice send Bob an arbitrary sequence of Q-bits, which are uniformly expected to be in one of four feasible statuses [see Table]. When Bobs receives a Q-bit he measures that on Z basis or X basis in a random manner and saves records for future use. Then Alice makes an announcement to Bob on

Quantum Cryptography Key Distribution

which basis the state came from but didn't reveal what is the actual state was. Then Bob announces the results on what substructure or basis he calculated. If Bob calculated the same substructure as Alice measured, then prepare state to get the value as shown in the table. Both Alice and Bob keep the value which is measured on the same basis and discard the other values, measured bits are used as to generate the private key. But if Eva is clever he can implement all possible chances to bamboozle both Alice and Bob (Seema 2017).

Table 1.

State	Basis	Value
$ 0\rangle$	Z	0
$ 1\rangle$	Z	1
$ 0\rangle + 1\rangle$	X	0
$ 0\rangle - 1\rangle$	X	1

Polarization of Photons

Sender and receiver implement quantum protocol by exchanging photons, whose polarization states are used to encode bit values over fiber channel this fiber channel is called a Quantum channel. Here use four positions both concur for that. For suppose, a 1-bit assessment is able to encode whether vertical position or +45 degree diagonal, a 0-bit assessment be able to encode whether horizontal or -45 degree diagonal one. Basically, emission or polarization of luminous is the path of fluctuation of electromagnetic territory which is related to its field. Linear emission positions are definite in the direction of the fluctuation field. Linear polarization examples are Horizontal and vertical moreover diagonal states also considered as linear polarization. Photon can be able to polarize in whatever of the above-mentioned forms. Some filters subsist to discriminate horizontal states from vertical ones. When transient during similar filter, vertically polarized photon diverged to right, while horizontally polarized photon diverged to left. During this scenario rotate the filter to 45 degrees to organize differential among angular polarized photons. Suppose if a photon send in incorrect directed orientation like angular polarized photon through non-rotated filter, then it resolves accidentally diverged in one of the two indications so it's very difficult to recognize photon path prior to the filter (Poppe, 2004; Zhao and Qi, 2006; Peev, 2009; Pearson and David, 2004).

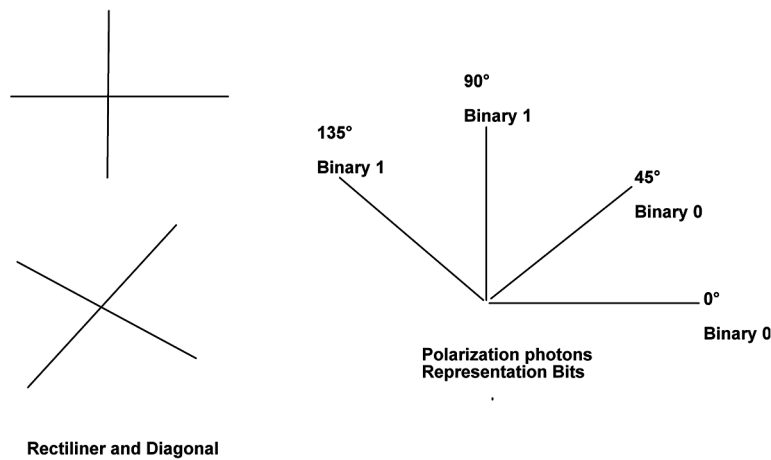
Quantum Key Distribution

Before concerning QKD we have to move forward over traditional key distribution, In cryptography where Alice/Bob send some quantity of key to Alice/Bob which have some negative aspects those we discuss above, to overcome those negative aspects we launch some supplementary practice where Alice/

Bob create individual keys, arbitrary sequence number sets, enclose with more numbers share to each one which is more than there key material. Finally correlate the above-mentioned set of numbers to distill or purified mutual subset, whichever remodeled the mutual key. In this direction they are not preferred entire number sets or precise numbers to key material, essential key material numbers should be secret, undercover furthermore random. Alice constructs successive of signs, one fluctuation for “1” and disparate fluctuation for “0” for each bit in his sets send a sign for Bob. Bob also transfer with his set bit by bit examine Alice sign with his bits, and constitute acknowledgment to Alice whether the sign is similar or not. Both Alice and Bob notify the bits accepted, reserve those bits in memory for shape final key, in addition, wipe out every other bit. Quantum cryptography proved experimentally in 1989 carry out by Bennett and Brassard where the key was transmitted/exchanged over 30 cm air. In 1990 at the University of Geneva key exchanged over optical fiber, key distribution takes cms to several kilometers. B92 QKD protocol expressed in provisions of measurement states in two structural Hilbert space equivalents to $\frac{1}{2}$ spin particles, spin operators $\alpha_1, \alpha_2, \alpha_3$ comply with algebra (Brandao & Oppenheim, 2012; Bennett and Brassard, 1998; Elliott and Chip, 2003; Rajani and Girma, 2007; Zhao and Qi, 2006; Yin and Chen, 2016; Padamavathi and Vishnu 2017; NIST, 2018; Richard and Alde, 2001).

$$[\alpha_i, \alpha_j] = 2i\epsilon_{ijk}\alpha_k; i, j, k= 1, 2, 3$$

Figure 2. Quantum cryptosystem – polarization of photons



The starting point of position with spin-up as well as spin-down on ahead the Z-axis

$$\alpha_3 \begin{Bmatrix} |\uparrow\rangle \\ |\downarrow\rangle \end{Bmatrix} = \begin{Bmatrix} +|\uparrow\rangle \\ -|\downarrow\rangle \end{Bmatrix}$$

Fulfilling the ortho-normality affairs

Quantum Cryptography Key Distribution

$$\langle \uparrow | \uparrow \rangle = \langle \downarrow | \downarrow \rangle = 1$$

$$\langle \uparrow | \downarrow \rangle = 0$$

Starting point states with spin up and spin down on ahead X-axis

$$\alpha_1 \begin{Bmatrix} | \rightarrow \rangle \\ | \leftarrow \rangle \end{Bmatrix} = \begin{Bmatrix} + | \rightarrow \rangle \\ - | \leftarrow \rangle \end{Bmatrix}$$

Substitute $| \rightarrow \rangle = 2^{1/2} (| \uparrow \rangle + | \downarrow \rangle)$ and $| \leftarrow \rangle = 2^{1/2} (| \uparrow \rangle - | \downarrow \rangle)$

An analysis with quantum theory is projection operator in Hilbert space, an analysis on behalf of spin-down

Onwards Z-axis is revealed as

$$P_{|\downarrow\rangle} = |\downarrow\rangle\langle\downarrow|$$

Similarly spin up along X-axis is revealed as

$$P_{|\leftarrow\rangle} = |\leftarrow\rangle\langle\leftarrow|$$

In B92 protocol Alice postures a pair of non-orthogonal measures; Bob also constructs a pair of non-orthogonal measurements. Various possible probabilities for the pass are given below (see table below).

Table 2.

$P_{ \downarrow\rangle}$	0	0.5
$P_{ \leftarrow\rangle}$	0.5	0

Alice, as well as Bob, set up a self-sufficient set of random numbers, thereafter planed bit by bit synchronization. Alice formulates photon polarization for each bit [see table (1)], plus dispatch it to Bob over a quantum channel. Bob arranges an analysis of each bit state he entangled as reported by his photon polarization [see table (3)]. Assemble record as “pass” or “fail”.

Table 3.

Bit	State
0	$ \uparrow\rangle$
1	$ \rightarrow\rangle$

Table 4.

bit	Measurement
0	$P_{ \leftarrow\rangle}$
1	$P_{ \downarrow\rangle}$

Bob will never record a “pass” if inherent bits are incomparable from Alice, moreover, Bob records a “pass” on at least 50% bits are familiar. In this direction we can’t anticipate which one is “pass”, nevertheless there are two achievable scopes one passes another one is fail there are no extra options. At last, Bob circulates entire bits over the public channel were the chance for eavesdroppers to plagiarize key material. Straightaway Alice, as well as Bob, considers just those bits in support of Bob’s result is “Pass” the above-mentioned particular bits used for key material (Yin and Chen, 2016; Padamavathi and Vishnu, 2017).

Simple BB84 Quantum Key Distribution Protocol

- Alice sends a random sequence of photons polarized horizontal, vertical, right circular and left circular.
- Bob measures the photons polarization in a random sequence of basis rectilinear, circular.
- Bobs measures his results
- Bob notify Alice which basis he uses for each photon on received ones.
- Alice tells Bob whos bases are correct.
- Alice and Bob keep the data that was correct and leaves the remainder data which was not useful.
- This data is interrupted as a binary sequence according to the coding sequence.

Table 5. Process of quantum key distribution – BB84 protocol

Alice’s bits	0 0 1 0 1 0 1 1 0 0 0 1
Alice’s Basis	+ x x + x + + x + x + +
Alice’s photon polarization	\nwarrow \swarrow \nearrow \searrow \swarrow \rightarrow \leftarrow \uparrow \uparrow \leftarrow \leftarrow \nearrow
Bob’s basis	+ + x + + x + x + x x +
Bob’s Photon polarization	\nwarrow \nearrow \leftarrow \searrow \uparrow \nwarrow \rightarrow \uparrow \rightarrow \leftarrow \searrow \nearrow
Alice’s Bob’s sequence polarization	\nwarrow \searrow \uparrow \leftarrow \nearrow
Alice’s and Bob’s bit sequences	0 0 1 0 1
Final key	0 1 0 1

Quantum Cryptography Key Distribution

- **B92 Protocol:** B92 considered as the customized protocol of BB84 by two states 0° and 45° . Photon polarization 0° in rectilinear basis symbolize binary value 0; polarization of photon 45° within diagonal basis symbolizes binary value 1.
- **Six State Protocols:** Six state protocols alike as BB84 protocol apart from it has three orthogonal bases to encode bits that intended to make broadcast among entities. As the name suggests it represents six states utilized to represent the bits.
- **SARGO04 Protocol:** The first phase which was introduced in the BB84 protocol is the same as the first phase of the SARGO04 protocol. Coming to the second phase initiator broadcasts pair of non-orthogonal states, where initiator utilizes one of them to predetermine his own bits unlike announcing bases directly. Both initiator and sender verify which bits they contain subsequent bases. If the receiver can able to measure accurate state if he used a suitable basis or else not able to achieve the bit.

QUANTUM CRYPTOGRAPHY IMPLEMENTATION

Quantum cryptography provides the best suitable secure communications nevertheless entire prototype systems have pointed to point links moderately than networks that distribute associations. BOSTON, HARVARD University along with BBN technology scientists combined to build six node quantum key cryptography system which provides continuous secure key exchanges between HARVARD and BBN which are 8-10 Km away from each other. Soon after scientists move the nodes across the network. This six node cryptography network is flexibility set up because the breakdown of connection or node doesn't indicate vanished of quantum cryptography some node be capable of taking steps to bond two extra nodes. Around the world research labs are under work to implement quantum repeaters (Elliot and Chip, 2002; Yin and Chin, 2006; Vasileios and Kamer, 2018; Brandao & Oppenheim, 2012).

DARPA

Quantum cryptography work through internet protocols to protect internet protocols, in addition, construct one type of VPN which endows with secure communication over unsecured networks similar to the internet at large. The DARPA security model is a cryptographic security model called Cryptographic virtual private network. Both public and symmetric key cryptography are used in traditional VPN networks to achieve authentication, integrity, and confidentiality. Where symmetric mechanisms provide traffic confidentiality and integrity and Public cryptography support authentication of endpoints, supports key exchanges. In consequence, the VPN system provides confidentiality and authentication without trusting the public network. Where in DARPA network existing VPN keys replaced by quantum cryptography and construction structure of VPN are unchanged.

MagiQ

MagiQ is New-York based start-up technology develop solutions for quantum cryptography. MagiQ technologies said that quantum cryptosystem is not the exact alternate for long-established cryptography techniques, but they add another comment for security that traditional crypto models can use to generate hybrid models that will provide more security. They made a bond with Cavium's networks, Cavium's

security chips are integrated within MagiQ servers as well as network boards. MagiQ claimed a quantum cryptographic box that compromises 40 pounds mountable in 9-inch rack that sells for 50000 dollars a unit. This box contains transmitter, receiver, electronics, and software's moreover it connects to remote parties via fiber optic cable links.

The SECOQC

Secure Communication based on Quantum Cryptography (SECOQC) is a collective research work designed and implemented by 41 industrial, research organizations under a European project. It suggests the system by QKD through importance on the prototype with the authenticated repeater. SECOQC introduced in the year 2003 and obtain popularity between 2004-2009. The SECOQC has a most important network-based agent named as SECOQC node module, which takes care of key distillation authentication for communications.

Hub and Spoke Network by Los Alamos National Laboratory

To route Quantum messages Los Alamos National Laboratory designed a focal pointed Hub as well as Spoke network in 2011. Basically, Hub used to receive quantum messages from respective nodes quantum transmitters. Here broadcast starts once every node points a one-time pad acknowledged via Hub, which was placed for protected broadcast over the conventional channel. As soon as the received message transmitted or routed to other nodes, the hub will initiate another one-time pad.

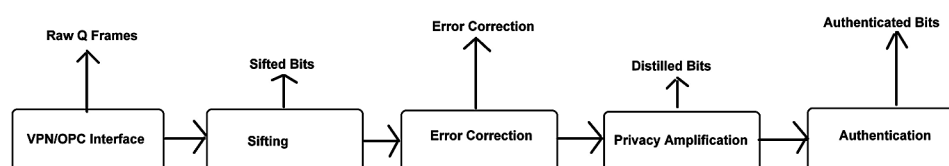
Tokyo QKD Network

Tokyo QKD initiated a conference held in Tokyo named Updating Quantum Cryptography and Communications (UQCC2010), it follows a star-based pattern connecting various centers. It has three phases namely the Quantum layer phase – generate keys with QKD functionality, Key management phase – gather and store QKD devices, Communication phase – allows secure allocation of keys.

QUANTUM CRYPTOGRAPHY PROTOCOL

Quantum cryptography entails a collection of dedicated protocols called Quantum protocols. New protocols are easy to implement or developed with help of these quantum protocols, this engine was premeditated by DARPA (Rivest, Shamir, and Adelman, 1978; Mullins and Justin, 2003; Tang and Chen, 2014; Yin and Chen, 2014; Shor, 2000; Zhao and Qi, 2006; Peev, 2009).

Figure 3. Protocol suite for quantum key distribution



Sifting

Sifting is a mechanism where Alice, as well as Bob fenestration, moved out from complete failure q bits from a suite of pulses. This failure q bit includes those Q-bits where Bob's spotters didn't endeavor to uncover photons vanished in transportation that Alice laser never transmitted. They also include the above-mentioned photon indications wherever Alice selects one base for transference however Bob selects another base for receiving. Near to the end of this procedure, Alice as well as Bob abandons the entire worthless patterns from individual enclosed storage, takes off simply those patterns that Bob expected moreover compared with Bob's basis.

Error Correction

Error bits 1's and 0's whereas Alice transmits as 1 however Bob captured as 0 or vice versa. Error bits allow both Alice plus Bob to resolve the entire error bits they shared, sifted moreover appropriate them so that Alice and Bob share alike error-corrected bits. Most of these error bits produce as a result of noise or through eavesdropping. Mostly fault detection in quantum cryptography includes unexpected things like indication confess assume to be Eavesdropper. So, there is a need for planed error discovery with adjustment codes which reveals miniature feasible in individual public control transportation enclosed by Alice and Bob.

Key Distillation

The BB84 procedure pretended that the only resource for inaccuracy in a series swap over through transmitter and receiver was the achievement of Eavesdroppers. Every part of other sensible quantum cryptography assumed errors caused by environmental perturbations of quantum channel or component imperfections. In order to avoid errors, a post-processing step acknowledged as key distillation executed behind the sifting of the key. Key distillation process expressed by two steps. In the first step allows us to estimate the actual error rate with the help of these error rates it is probable to compute the quantity of advice on key. The Second stair is called privacy amplification with the appropriate factor rate it will reduce or compress the key which helps to reduce the information of the eavesdropper. In order to prevent man in the middle attack, key distillation is accompaniment with authentication step where the eavesdroppers cut announcement carriers and make-believe to the emitter that he is the recipient. The pre-established secret key in receiver and emitter used for authentication in the standard channel. These initial undercover keys used to validate in primary quantum cryptography following that every conference or session a piece of key is formed is used to substitute prior validation key.

Privacy Amplification

This method called advantage distillation, where both Alice as well as Bob decline Eva's understanding of their mutual bits. The region which commences the privacy amplification decides on one linear hash function above the Galois Field (GF) where n is a number of bits as participation input, curved up to multiple of 32. Then transmit 4 bits to another end –the number of m bits of the shortened end result, primitive polynomial of the Galois Field, a multiplier, an m bit polynomial to add by commodity. Every surface then presents equivalent hash and abbreviates results into m bits presents privacy enlargement.

Authentication

Authentication permits both Alice as well as Bob defender adjacent toward “man in the middle attacks” who permits Alice to make sure as long as she exchanges a few words with Bob. Eavesdroppers may itself insert into the discussion among Alice and Bob at any phase in there contact. BB84 described the authentication problem using universal hash functions. The temperament of general hashing, every party that does not recognize top undisclosed key would have identified the exceptionally slighter possibility of being proficient to fabricate the communication but limitless computational power. Fortunately, a comprehensive authentic exchange can authorize a big number of fresh shared secret bits from QKD.

QKD CHARACTERISTICS

QKD suggests a technique as an agreement where collective unsystematic sequences of fragments between two types of machinery and awfully small probability those eavesdroppers capable to formulate successful interference of those fragments. Those random sequence fragments are used as secret keys between two distinct devices (Bennett and Brassard, 1982; Padmavathi and Vishnu, 2016; Vasileios and Kamer, 2018; NIST, 2018; Yin and Chen, 2016; Alfred and Menezes, 2018; Brassard and Bennett, 1996; Buttler, 2003).

Key Delivery

QKD is clearly a key distribution technique. Normally key distribution center task is to deliver keys speedily; it makes encipher equipment do not overwork their contribution of key bits. QKD systems achieve key material throughput of 1000 bits/second but in realistic achievements, this speed may be low, based on the uses of certain keys also speed comes to low. One time pad, high secure algorithms speed of traffic flow is high. Low is acceptable to speed for reliable low (compare to one-time pad) secure algorithms such as AES.

Authentication

Authentication certifies that information approaching from authentic source; moreover, it should be certified that no unlawful third-party stand-in like an authorized user. QKD not directly provides authentication process but the QKD system provides a recommendation of secret keys at paired machinery. Secret keys must distribute before QKD begins with the help of human courier or some other techniques, but it is a challenging task.

Robustness

In the QKD key object, fundamental is safe communication; moreover, it is tremendously vital that the flow of key objects is not interrupted which may happen through adversary or else accidentally. Here QKD techniques employed with a point to point, if the point link is disrupted by any event instead via active probing otherwise any fiber cut the entire flowing key material would stop.

Confidentiality

Data confidentiality protects the data so any unauthorized user can't understand and examine it. Invaders should not know the regularity facts and content of facts broadcasted. Classical undisclosed key structures deteriorate from insider hazard or a logical load of keying objects distribution. Public key systems suffer from encryption and decryption is mathematically intractable, Diffie-Hellman may break at some point in the future. Privacy is the foremost justification for getting a concentration in QKD, it contributes to mechanical circulation of keys to provide safekeeping higher to its participants.

Traffic Analysis

In key distribution, traffic analysis such as the heavy flow of keying material between two parties which make eavesdroppers estimate that a large amount of useful information flows between them. In QKD most steps assumed dedicated, point to point links between communicating entities that clearly underlay key distribution techniques.

EAVESDROPPING

Eavesdropping is the process of someone who secretly listens, read messages and conversations by unintended recipients. Eavesdropping done in phone calls, email, instant messages and any other communications which considered private. Providing security services to these messages when data transmission over public channels. This security service is habitually executed by Encryption. Eve has unlimited power resources and has access to future technologies. In quantum cryptography, Eve can hide in noise, replace quantum channels with better instruments with lower-level noise, which makes the identification of Eve difficult. Eve also possesses all possible traditional attacking methods like attacking RING, spoofing, flooding, at a time attach one probe to Q-bit and accessing local storage of Alice or Bob, but measure several probes coherently. Individual attack attaches one q-bit at a time and measures one time. In a joint attack, Eve possesses several q-bits collectively (Richard and Alde, 2002).

LARGE SCALE QUANTUM KEY CHALLENGES

Quantum key distribution (QKD) along with a one-time pad produces a secure transportation base on quantum principles. Here the ultimate goal is to establish global Quantum key distribution for all over world appliances. Various researchers, scientists come up with dissimilar methods but still, it has faced some critical issues (Qiang, Feihu and Yu, 2018; Mateusz, 2018)

1. There is a huge breach among theory and practical approaches of QKD, QKD secure only when it deployed with ultimate devices like faultless distinct photon but that type devices are not more available.
2. Large scale key distribution which shows huge channel failure and no-stability. At present 440 km distance in fiber tunnel is recorded. But the problem in fiber tunnel is as the distance increases the

key velocity significantly reduces. Quantum repeaters, satellite-based quantum transportation are some solution to avoiding these concerns.

(Y. Zhao and Qi, 2006) executed QKD through a 15 km fiber spool, (Rosenberg and Harrington, 2007) apply decoy-state QKD from end to end 100 km fiber, (Y, Zhao, Lo and Qiet, 2009) complete 144 km decoy-state QKD in free space, (Tang and Yin, 2014) attain MDI-QKE over 200 km fiber through enlarge the system clock rate from 1 – 75 MHz with help of solitary photon detectors. (Yin and Chen, 2016) complete the MDI-QKD space to 404 km low loss fiber via optimizing the limitation along with a low-loss fiber.

OUTLINE OF QUANTUM-RESISTANT CRYPTOGRAPHY

From past decades Public key cryptography (PKC) turns to be inseparable from our digital communications. Security concepts of these cryptosystems lean on the complexity of theoretic mathematical problems like discrete log problems and Factorization etc. the invention of quantum computers resolves the issues quicker than convolution computers. The foremost utilization of PKC in these days is digital signatures and the key establishment and the formation of a large-scale quantum computer would be rendering many of these PKCs insecure.

There is a huge requirement for strong cryptography computing levels in both classical and quantum cryptography techniques. To avoid security attacks in classical crypto techniques, NIST (National Institute of Standards and Technology) instructs to maintain algorithm key sizes from 80 bits to 112-128 bits. It is still undecided when scalable quantum computers accessible for everyone. Research groups seriously working on a quantum computer that can break or crack the security code of the RSA technique in a few hours of time. This is a super-serious threat to current cryptography systems. Earlier evolutions from weaker to stronger cryptography security determined based on the time-complexity of attacking through a classical computer. Unluckily bit-of-security methods not able to consider into account the security of algorithms against quantum cryptanalysis, hence it was insufficient to show evolution to quantum-resistant cryptography. Moreover, there is no conformity view on what key lengths endow with satisfactory levels of security next to quantum molests.

The progress for post-quantum cryptography needs major resources to analyze quantum-resistant schemes. In recent times importance in the areas of quantum computing and quantum-resistant cryptography enlarged because of various adversaries in the improvement of quantum computing hardware. NIST is working on the above-mentioned standardization endeavors in quantum cryptography. Moreover, it also draws strategies to specify a preliminary evolution criterion that contains security and performance requirements for quantum-resistant public-key cryptography standards.

Modern Quantum Resistant Cryptography Techniques

The imminent consciousness of adaptable quantum computers makes a tremendous shake on present security transportation. Powerful expansion of quantum computers, public key infrastructure based cryptographic methods turn vulnerable to the quantum algorithm. Quantum resistant cryptography is an energetic research area, that makes an effort to design innovative fresh quantum-resistant public cryptography protocol. Lattice-based cryptography is promising as one of the majority possible options.

Quantum Cryptography Key Distribution

Because of its efficient execution on software, hardware that has previously shown to calculate and even outshines the presentation of existing conventional protection public key proposals

Lattice-based cryptography: Lattice based key organization crypto techniques reasonably simple, parallelizable and well-organized. Moreover, the security of these techniques verified secure under a worst-case fighting hypothesis, moderately than on the adequate case. Code-based Cryptography: Early 1978, a well-known researcher proposed the McEliece crypto algorithm, it has not broken since. But it suffers from huge key sizes, with the addition of some pre-arranged structures algorithms key sizes able to reduce. Code-based digital signatures, Code-based-crypto techniques more useful in modern systems. Hash-based signature: Hash-based digital signatures produce tremendous security against all attacks, even against quantum attacks also. However, the negative aspect is that the signer must keep a record of the exact number of previous messages, and additionally, it produces a limited number of signatures. Multivariate polynomial cryptography: Numerous multivariate crypto techniques presented base on the complexity of explaining multivariate polynomials in excess of finite fields. A few of them mostly unbeaten as an advance to signatures.

CONCLUSION

Assigning Quantum physics to cryptography opens a door for research in security and enhancement of modern cryptosystem troubles. Quantum cryptography modifies the security way of all modern cryptosystems using Q-bits. QKD in concern with one time pad encoding can produce intellectual-theoretical security for communication. At this time QKD has been extensively employed in numerous fiber networks, however, its employment in large scale remains experimentally exigent. Chapter provides QKD characteristics, key challenges and Modern Quantum resistance cryptography techniques are described briefly. Many researchers around the world find out innovative mechanisms for making quantum cryptography indestructible. We can glance forward to the electrifying the outlook of quantum cryptography with countless potential hypothetical and investigational.

REFERENCES

- Abood, O. G., & Guirguis, S. K. (2018). A Survey on Cryptography Algorithms. [IJSRP]. *International Journal of Scientific and Research Publications*, 8(7).
- Bennett, C., & Brassard, G. (1984). Quantum cryptography Public key distribution and coin tossing. In *Proceedings of the International conference on computers, systems and signal processing*. Academic Press.
- Bennett, C.H. (1985). Quantum public key distribution system. *IBM systems*.
- Bennett, C.H. & Brassard. (1987). Quantum Public key distribution. *Seget news*, 18(4), 51-53.
- Bennett, C. H. (1992). Quantum cryptography using two non orthogonal states. *Physical Review Letters*, 68(21), 3121–3124. doi:10.1103/PhysRevLett.68.3121 PMID:10045619
- Bennett, C. H. (1992). Quantum cryptography using two non orthogonal states. *Physical Review Letters*, 68(21), 3121–3124. doi:10.1103/PhysRevLett.68.3121 PMID:10045619

- Bennett, C. H., Brassard, G., Breidbart, S., & Wiesner, S. (1982). Quantum Cryptography, or Unforgeable Subway Tokens, Advances in Cryptology. In *Proceedings of Crypto '82*. Plenum Press.
- Bennett, C. H., Brassard, G., Breidbart, S., & Wiesner, S. (1982). Quantum Cryptography, or Unforgeable Subway Tokens, Advances in Cryptology. In *Proceedings of Crypto '82*. Plenum Press.
- Bennett, C. H., Brassard, G., & Mermin, N. D. (1992). Quantum cryptograph. *Physical Review Letters*, 68(5), 557–559. doi:10.1103/PhysRevLett.68.557
- Bennett, C. H., Brassard, G., & Mermin, N. D. (1992). Quantum cryptography without Bell's theorem. *Physical Review Letters*, 68(5), 557.
- Bennett, C.H. & Shor, P.W. (1998). Quantum information theory. *IEEE Information theory*, 44(6), 2724-2742.
- Brandao, F. G., & Oppenheim, J. (2012). Quantum one-time pad in the presence of an eavesdropper. *Physical Review Letters*, 108(4).
- Brassard, G. (1988). *Modern Cryptology*. New York: Springer.
- Brassard, G. (1996). Cryptography columns- 25 years of Quantum cryptography. *Sigactnews*, 27(3), 13-24.
- Buttler, W. T. (2003). Fast and Efficient error reconciliation for quantum cryptography. *Physical Review*, 76, 5.
- Curcic, T. (2004). Quantum networks: From Quantum cryptography to quantum architecture. *Computer Communication Review*, 34(5), 3–8.
- Elliott, C. (2002). Building the quantum network. *New Journal of Physics*, 4(1), 46.
- Elliott, C., Pearson, D., & Troxel, G. (2003). Quantum cryptography in practice. In *Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communications*. ACM.
- Goel, R., Garuba, M., & Girma, A. (2007, April). Research directions in quantum cryptography. In *Proceedings of the Fourth International Conference on Information Technology (ITNG'07)* (pp. 779-784). IEEE.
- Hellman, D. (1976). New Directions in Cryptography. *IEEE Transactions Theory*, 22(6), 644–654. doi:10.1109/TIT.1976.1055638
- Hughes, R. J., Alde, D. M., Dyer, P., Luther, G. G., Morgan, G. L., & Schauer, M. (1995). Quantum cryptography. *Contemporary Physics*, 36(3), 149–163.
- Johnson, R. C. (2002). *MagiQ employs quantum technology for secure encryption*. EE Times.
- Kumar, M. G. V., & Ragupathy, U. S. (2016, March). A Survey on current key issues and status in cryptography. In *Proceedings of the 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)* (pp. 205-210). IEEE.
- Kute, S. S., & Desai, C. G. (2017). Quantum Cryptography: A Review. *Indian Journal of Science and Technology*, 10(3).

Quantum Cryptography Key Distribution

MagiQ Technologies. (2003). [Press Release].

Martinez-Mateo, J., Elkouss, D., & Martin, V. (2013). Key Reconciliation for High Performance Quantum Key Distribution. *Scientific Reports*, 3(1), 1576. doi:10.1038rep01576 PMID:23546440

Mavroeidis, V., Vishi, K., Zych, M. D., & Jøssang, A. (2018). The impact of quantum computing on present cryptography. *International Journal of Advanced Computer science and Applications*, 9(3).

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (2016). *A Handbook of Applied cryptography*. CRC press.

Mullins, J. (2003). *Quantum Cryptography's Reach Extended*. IEEE Spectrum Online.

NIST. (2016). Recommendation for Key Management Special Publication (SP) 800-57 Part 1 Revision 4. doi:10.6028/NIST.SP.800-57pt1r4

Padamvathi, V., Vardhan, B. V., & Krishna, A. V. N. (2016, February). Quantum Cryptography and Quantum Key Distribution Protocols: A Survey. In *Proceedings of the 2016 IEEE 6th International Conference on Advanced Computing (IACC)* (pp. 556-562). IEEE.

Pearson, D. (2004, November). High-speed QKD Reconciliation using Forward Error Correction. *AIP Conference Proceedings*, 734(1), 299–302.

Peev, M., Pacher, C., Alléaume, R., Barreiro, C., Bouda, J., Boxleitner, W., ... Zeilinger, A. (2009). The SECOQC quantum key distribution network in Vienna. *New Journal of Physics*, 11(7), 075001. doi:10.1088/1367-2630/11/7/075001

Poppe, A., Fedrizzi, A., Ursin, R., Böhm, H. R., Lorünser, T., Maurhardt, O., ... Jennewein, T. (2004). Practical quantum key distribution with polarization entangled photons. *Optics Express*, 12(16), 3865–3871.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120–126.

Rosenberg, D., Harrington, J. W., Rice, P. R., Hiskett, P. A., Peterson, C. G., Hughes, R. J., ... Nordholt, J. E. (2007). Long-distance decoy-state quantum key distribution in optical fiber. *Physical Review Letters*, 98(1), 010503. doi:10.1103/PhysRevLett.98.010503 PMID:17358462

Scarani, A., Acin, A., Ribordy, G., & Gisin, N. (2004). Quantum cryptography protocols robust against photon number splitting attacks. *Physical Review Letters*, 92(5), 057901. doi:10.1103/PhysRevLett.92.057901 PMID:14995344

Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review*, 41(2), 303–332. doi:10.1137/S0097539795293172

Shor, P. W., & Preskill, J. (2002). Simple proof of security of the BB84 Quantum key distribution protocol. *Physical Review Letters*, 85(2), 441–449.

Tang, Y.-L., Yin, H.-L., Chen, S.-J., Liu, Y., Zhang, W.-J., Jiang, X., ... Pan, J. W. (2014). Measurement device-independent quantum key distribution over 200 km. *Physical Review Letters*, 113(19), 190501. doi:10.1103/PhysRevLett.113.190501 PMID:25415890

Yin, H.-L., Chen, T.-Y., Yu, Z.-W., Liu, H., You, L.-X., Zhou, Y.-H., ... Pan, J.-W. (2016). Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Physical Review Letters*, 117(19), 190501. doi:10.1103/PhysRevLett.117.190501 PMID:27858431

Zhang, Q., Xu, F., Chen, Y. A., Peng, C. Z., & Pan, J. W. (2018). Large scale quantum key distribution: Challenges and solutions. *Optics Express*, 26(18), 24260–24273.

Zhao, Y., Qi, B., Ma, X., Lo, H.-K., & Qian, L. (2006). Experimental quantum key distribution with decoy states. *Physical Review Letters*, 96(7), 070502. doi:10.1103/PhysRevLett.96.070502 PMID:16606067

Zych, M. (2018). Quantum Safe Cryptography Based on Hash Functions: A Survey [Master's Thesis]. University of Oslo.

This research was previously published in Quantum Cryptography and the Future of Cyber Security; pages 84-108, copyright year 2020 by Information Science Reference (an imprint of IGI Global).

Chapter 15

Vulnerability of the Synchronization Process in the Quantum Key Distribution System

A. P. Pljonkin

Southern Federal University, Taganrog, Russia

ABSTRACT

A typical structure of an auto-compensation system for quantum key distribution is given. The principle of operation of a fiber-optic system for the distribution of quantum keys with phase coding of photon states is described. The operation of the system in the synchronization mode and the formation of quantum keys was investigated. The process of detecting a time interval with an optical synchronization pulse is analyzed. The structural scheme of the experimental stand of the quantum-cryptographic network is given. Data are obtained that attest to the presence of a multiphoton signal during the transmission of sync pulses from the transceiver station to the coding and backward direction. The results of experimental studies are presented, which prove the existence of a vulnerability in the process of synchronization of the quantum key distribution system. It is shown that the use of a multiphoton optical pulse as a sync signal makes it possible for an attacker to unauthorized access to a quantum communication channel. The experimental results show that tapping a portion of the optical power from the quantum communication channel during the synchronization process allows an attacker to remain unnoticed while the quantum protocol is operating. Experimentally proved the possibility of introducing malfunctions into the operation of the quantum communication system at the stage of key formation, while remaining invisible for control means.

DOI: 10.4018/978-1-7998-8593-1.ch015

1. INTRODUCTION

Modern cryptographic protocols that ensure the security of transmitted messages have a high resistance to burglary. The stability of ciphers is based on mathematical formulations and the limited computing resources of the attacker. It is believed that until now the most reliable security in the transmission of messages provides the use of one-time pads. The development of symmetric methods of encryption is limited to the main problem in the transmission of confidential information, which is formulated as the problem of distributing a secret key between legitimate users.

The well-known Shannon rule, which interprets the use of a secret key for a secure transmission, is updated with the development of new technologies for the formation of secret keys. Thus, the achievement of absolute secrecy in the transmission of messages is possible only by solving the problem of key distribution.

The development of methods of quantum cryptography to ensure security in telecommunications systems of information transmission theoretically allows to achieve absolute secrecy of ciphers (Gisin et al., 2002). Quantum cryptography is based on the laws of quantum physics and is based on the coding of the quantum state of a single particle. The essence of quantum cryptography lies in the reliable distribution of the secret key between legitimate users. Another component in the quantum distribution is the creation of a random secret key (Bennet et al., 1992; Stucki et al., 2002; Broadbent & Schaffner, 2007).

Practical implementation of quantum cryptography is based on quantum key distribution systems (QKDS). If the existing encryption algorithms can be distorted by mathematical improvements, then quantum cryptography is the only way to solve the problem of key distribution. Recall that the basis of quantum cryptography lies in the following statements: it is impossible to clone an unknown quantum state and it is impossible to obtain information on non-orthogonal quantum states without perturbation. Consequently, any unauthorized measurement will lead to a change in the quantum state.

In quantum cryptography, symmetric cryptosystems are common (Makarov, 2007). In such systems, one key is used for both encryption and decryption. Messages sent along the lines of quantum communication, theoretically can't be intercepted or copied. Quantum key distribution is a technology based on the laws of quantum physics to create a sequence of random bits in two remote users. This sequence is used as a cryptographic key, and the key array itself is called a "one-time pad."

2. QUANTUM KEY DISTRIBUTION SYSTEMS

In 2007, the methods of quantum cryptography were first applied in a large-scale project. Quantum security system, developed by the Swiss company idQuantique, was used to transmit voting data at the parliamentary elections in Geneva. To date, really functioning quantum communication systems have been created. The efforts of developers are now aimed at increasing the communication range, increasing the speed of forming a quantum key, improving the characteristics of fiber-optic components.

As noted earlier, a symmetric cryptosystem generates a shared secret key and distributes it among legitimate users to encrypt and decrypt messages (Rumyantsev & Pijokin, 2015). An attacker attempting to investigate transmitted data can't measure photons without distorting the original message. The system on the open channel compares and discusses signals transmitted on the quantum channel, thereby verifying them for the possibility of interception. If the system does not contain errors, then the transmit-

ted information can be considered securely distributed and secret, despite all the technical capabilities that a cryptanalyst can use.

Quantum key distribution systems operate under the control of quantum protocols. There are several protocols of quantum cryptography based on the coding of single photon states, for example: BB84, B92, Koashi-Imoto, SARG04 and their modifications (Kurochkin et al., 2012). Under the signal in quantum communication systems is meant the transmitted quantum state of a photon. The first protocol that was implemented in the QKD systems is called BB84. The basis of the BB84 protocol is the principles of particle phase coding and auto-compensation of polarization distortions. This protocol is also called bi-directional because of the propagation of the optical signal along a single fiber-optic path in two directions. Note that today the BB84 protocol has more efficient modifications. In the known BB84 protocol, the receiver analyzes the photons and randomly selects the polarization measurement method. On an unprotected channel, the receiver informs the sender of the method of choosing the basis for each photon, without revealing the measurement results themselves. After that, the sender on an unprotected channel tells you whether the type of measurement for each photon is correctly selected. As a result, an unrefined (raw) key is generated.

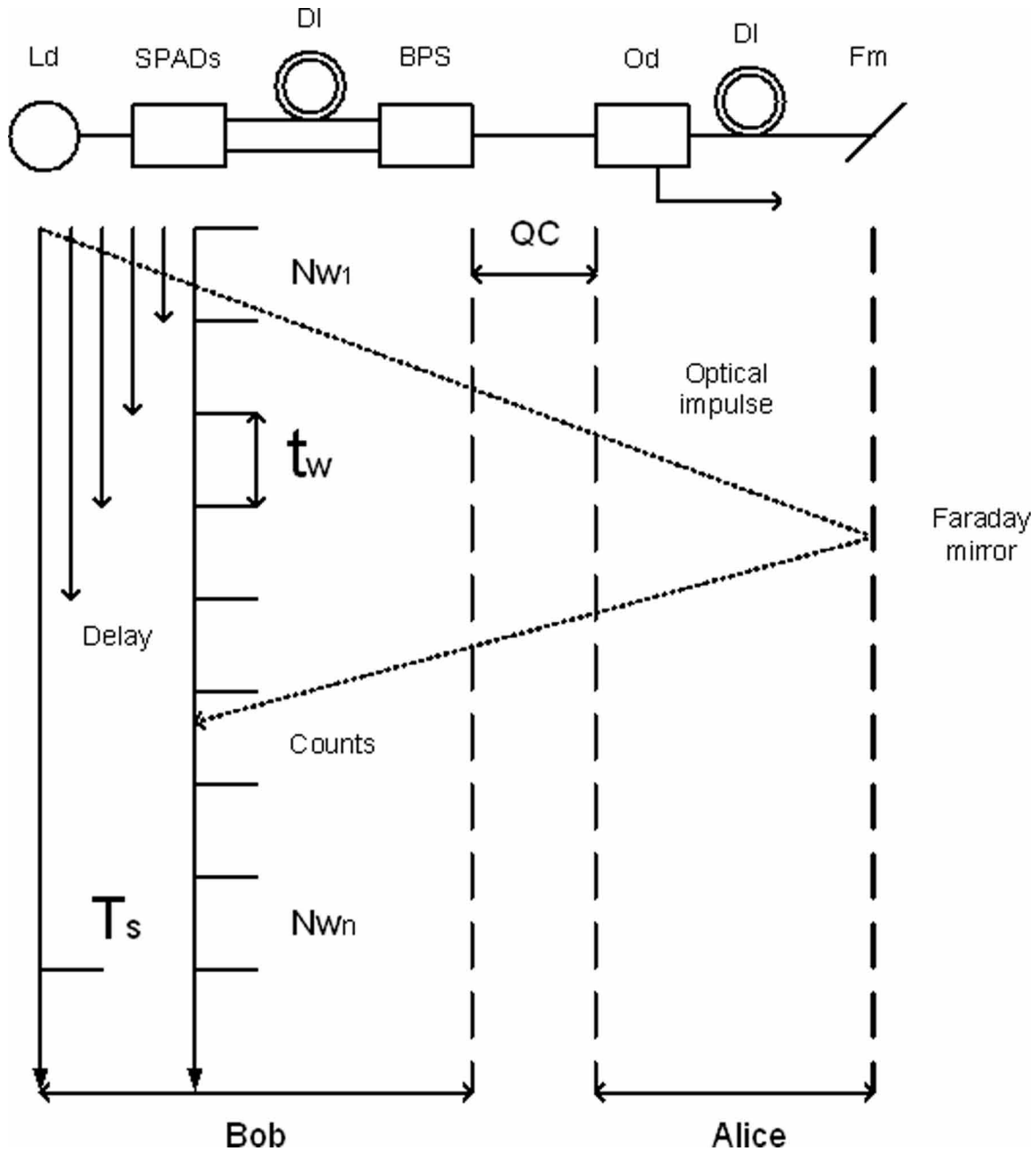
3. SYNCHRONIZATION IN QKD SYSTEM

The QKD system can't operate without synchronization (Lydersen et al., 2010). During the synchronization process, optical pulses propagate from the transceiver station to the encoding and vice versa. The synchronization task is the detection of the signal time interval with maximum accuracy. We will explain that under the signal time interval is meant a time window containing an optical sync pulse. The pulses are recorded by one-photon avalanche photodetectors of the transceiver station. Let us consider in more detail the synchronization process using the example of an active quantum key distribution system with phase coding of photon states. The process consists of three stages, each of which is a continuation of the previous one and consists in determining the moment of detection of the optical pulse by single-photon photodetectors. The problem of detecting the signal time interval is solved by measuring the propagation path length of the optical pulse from the transceiver station to the encoding and vice versa. The structural scheme of the synchronization process of the auto-compensation QKD system is shown in Figure 1.

A laser diode generates optical pulses at a wavelength of 1550 nm and a duration of about 1 ns. The period and duration of the optical pulse are absolutely stable. The repetition period T_g is determined by the length of the quantum communication channel between the stations of the QKD system. The time frame equal to the optical pulse repetition period T_g is divided into N_w of time windows with a duration t_w so that $T_g = N_w \cdot t_w$. Photodetectors are put into working mode and a sequential polling of all temporary windows begins. Each window is analyzed N times. Thus, the value of N is formulated as the sample size in the time window. When analyzing each time window, the number of registered photoelectrons (PEs) and / or pulses of dark current (PDC) is fixed. After polling all N_w time windows, an array of values of registered PE and / or PDC is formed. The conditions for detecting the optical pulse by the detection equipment during synchronization are described in [9]. The time window with the maximum number of registered FEs is recognized as a signal window. At each next stage of synchronization, the duration of the time window is reduced. So, in the first stage $t_w = 300\text{ps}$, on the second $t_w = 60\text{ps}$, at the third stage $t_w = 10\text{ps}$.

Vulnerability of the Synchronization Process in the Quantum Key Distribution System

Figure 1. Sync pulse detection. *Ld* – laser diode; *SPADs* – single-photon avalanche photodiodes; *DI* – delay line of optical radiation; *BPS* – beam polarizing splitter; *Od* – optical divisor; *Fm* is a Faraday mirror; *QC* – quantum channel; *Delay* - time delay of gating; *Nw1* (*Nwn*) – the number of time windows; *Counts* – the moment when photodetectors are triggered; *tw* – duration of the time window.

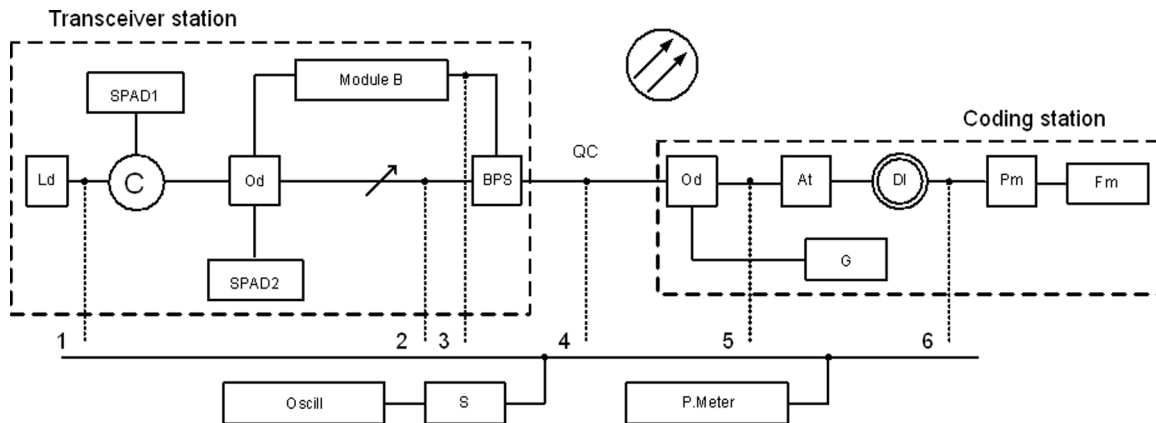


Vulnerability of the Synchronization Process in the Quantum Key Distribution System

Note that the accuracy of the time window in 10ps makes it impossible to change the physical length of the quantum communication channel after the synchronization process. The latter requires periodic initialization of the synchronization process under real conditions of operation of quantum distribution systems, since even a slight atmospheric effect on the quantum channel causes deformation of the optical fiber.

To study the process of entering synchronism, the experimental stand is assembled (Figure 2). Two stations of the QKD system are interconnected by a fiber-optic communication line. Each station is controlled by software. To construct an energy model of the quantum key distribution system, six optical control points measure the power level of the optical radiation. The connections were made using plug-in connections. The measurements were carried out using the Yokogawa optical modular system and the LeCroy digital oscilloscope.

Figure 2. Structural scheme of the optical part of the QKD system. *Ld* – laser diode; *C* – optical circulator; *Od* – directional coupler; *SPAD* – photodetectors; *Module B* – small radiation delay line, phase modulator, filter; *BPS* – beam polarizing splitter; *QC* – quantum channel; *At* – attenuator; *G* – circuit with clock generators; *DI* – radiation delay line with a length of 24 km; *Pm* – phase modulator; *Fm* – Faraday mirror; *S* – medium converter; *P.Meter* – optical power meter.



The energy model of the system made it possible to calculate the power loss of optical pulse on all sections of the fiber-optic signal propagation path (Pijokin & Rumyantsev, 2016). The latter shows that during the synchronization (detection of a time interval with an optical pulse), the signal optical pulse contains more than 10^3 photons in back propagation from the coding station to the transceiver. Note that the transmission of synchronizing signals from the transceiver station to the coding one is always performed in multiphoton mode. In addition, it is established that avalanche photodiodes function in the linear mode during synchronization, and the procedures for error correction and power control (as in the operation of the quantum protocol) are completely absent.

Thus, it can be concluded that the synchronization process in quantum key distribution systems with automatic compensation of polarization distortions takes place in a multiphoton mode and does not have means of protection against unauthorized access.

4. ATTACK ON THE QUANTUM CHANNEL EXPERIMENTS

Note that back in 2007, a group of scientists successfully carried out an attack on the quantum key distribution system with phase coding (Rumyantsev & Pijokin, 2016). The attack was based on imperfection of the system and was aimed at destabilizing the quantum protocol. During the implementation of the attack, it was assumed that the system was already synchronized.

Let us prove that the vulnerability of the synchronization process can be used to further interfere with the operation of the quantum key distribution system at the stage of functioning of the quantum protocol.

Multiphoton mode potentially allows an attacker to organize unauthorized access to a fiber-optic communication channel (to a quantum channel). The purpose of unauthorized access can be not only the interception and reading of information, but also the synchronization of the equipment of the attacker with the aim of interfering with the operation of the QKD system. Attack “Trojan horse” is an example of the closest to practical implementation, when it is possible to replace the original messages with an attacker’s messages. The attacker connects to the quantum communication channel and generates copies of optical pulses intercepted from the transceiver station and then sent to the encoding station. Thus, legitimate users can not recognize the presence of an attacker in a quantum communication channel. Realized auto-compensation systems with phase coding of photon states function according to a two-pass scheme, i.e. optical signals propagate along a single fiber in both directions. Such a realization complicates the problem of unauthorized access to a quantum communication channel but does not completely exclude it. The moment of interception of the optical pulse during direct propagation of the signal does not give complete information to the attacker about the operation of the system. The decisive moment is the appearance of an optical pulse in the backward propagation of a reflected signal in a quantum channel. Having information about the time of re-reflection, the attacker is able to simulate the work of the encoding station and at the right time send imitation signals to the photodetectors of the transceiver station.

Figure 3 (a) shows the scheme of the experiment with an optical power coupler integrated into the quantum communication channel. Coefficients of division 90/10 (%). 10% of the power of optical radiation is diverted to the measuring equipment with a direct signal passing (from the transceiver station to the coding one). 90% are sent to the coding station. At backward propagation the signal without losses arrives at the transceiver station. With this modification, not only the synchronization process, but also the process of quantum key distribution (quantum protocol) function in the regular mode. The theoretical error, which is calculated by the software of the QKD system, was 2.85%. The actual error was 0.65%. Note that the values obtained are not critical; the system does not detect the removal of part of the optical power from the quantum communication channel.

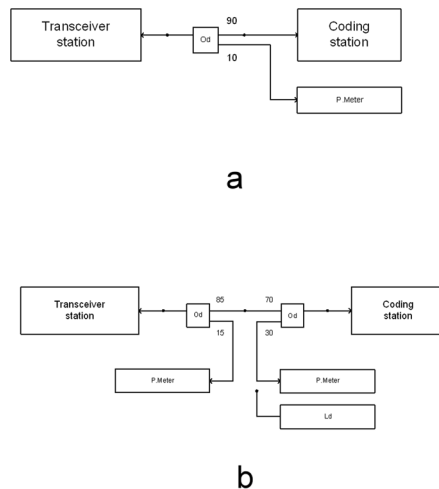
Let us realize the problem of removing part of the optical power at two points of the quantum communication channel. For this purpose, a circuit was constructed using two directional fiber-optic couplers with division coefficients of 85/15 (%) and 70/30 (%). The couplers are integrated in the quantum communication channel as shown in Figure 3 (b).

To prove the thesis that the optical fiber elements of the coding station are inactive during the synchronization process, we will conduct the following experiment: during the detection of the length of the fiber-optic communication line, we detach the transceiver station from the quantum channel and give the optical pulse 0dBm to the input of the 85/15 coupler in the direction of the coding station. At the same time, we capture the values at the outputs of the couplers 15% and 30% – -9.6 dBm and -57.7 dBm, respectively. We repeat the measurements, but the coding station is de-energized this time. The

Vulnerability of the Synchronization Process in the Quantum Key Distribution System

values at the outputs of the couplers of 15% and 30% are -9.6 dBm and -57.7 dBm, respectively. Thus, the experimental results show that the active fiber-optic elements of the coding station are not involved in the synchronization process and do not affect the optical signal.

Figure 3. (a) use of a directional coupler in a quantum communication channel; (b) extraction of optical power at two points



As noted earlier, the attacker's task may be not only to intercept and decrypt information transmitted via the quantum communication channel, but also to introduce interference to destabilize the system. We will experimentally prove the possibility of introducing interference into the operation of the quantum protocol, without detecting the presence of an attacker in the quantum communication channel.

In accordance with the scheme presented in Figure 3 (b), we will integrate fiber-optic couplers into a fiber-optic communication line between two stations of the QKD system. The first stage of the experiment is organized using a quantum communication channel with a length of 1000 m. The operation of the quantum key distribution system is started in the regular mode. According to the algorithm of work, the system subsequently tests the laser diode and photodetectors, analyzes the value of losses in the fiber-optic communication line. After the system analysis, the process of detecting the length of the quantum communication channel (synchronization) is started. The system synchronized without detecting the presence of two couplers in the quantum communication channel. Then the key distribution process is initiated. In fact, the measured error was 2.97%. The operation of the quantum protocol also did not detect the presence of couplers. The circuit with two integrated couplers operated continuously for 36 hours. The key distribution and synchronization process worked in a cyclic mode, the keys were accumulated in the buffer. At the second stage of the experiment, during the distribution of the quantum keys, a source of radiation with a wavelength of 1550 nm with a power of about 1 mW and a repetition rate of 270 Hz was connected to the output of the divider 15%. The level of the measured error increased from 2.97 to 3.35%, but the process of forming the quantum keys was not violated and continued normal operation. Next, we connected a radiation source with the same parameters to the output of 30%, while the pulses were sent to the coding station. With such a scheme, the source of radiation in the key formation mode

was briefly switched on. Note that in the presence of two couplers with respect to signal parameters, you can determine the mode in which QKD systems work without difficulty. Because of the impact on the coding station on the assembled circuit, the process of forming the quantum key ceased to function. The system entered the tuning mode without detecting the presence of couplers (the error level in the system did not change). Violation of the process of key formation is perceived by the system not as an attacker in the communication channel, but as a mismatch of the frame structure of the sync pulse frames. After turning off the source of interference, the system is adjusted and continues to operate the quantum protocol. The experiment was repeated for a length of a quantum communication channel of 2, 4, and 6 km according to a similar scheme. The results of the experiment remained unchanged, for all fiber-optic communication lines the system did not detect the presence of two couplers in the optical communication channel.

We note that similar studies in related fields are also relevant (Rumyantsev & Pijokin, 2015; Pijokin, 2017; Pijokin et al., 2017; Yuen, 2016; Pijokin et al., 2016; Distribution, 2010; Chan et al., 2011; Advanced in Security and Privacy..., 2018; Botnet-based distributed denial of service..., 2012; AIZain et al., 2015; Gupta et al., 2016; Gupta et al., 2017; Bushan et al., 2017; Gupta et al., 2017; Aakanksha et al., 2017; Shashank et al., 2017).

5. CONCLUSION

Thus, it is proved that if an intruder enters the quantum communication channel at the stage of configuring a QKD system, the attacker may remain unnoticed during synchronization and during the formation of the quantum key. The latter makes it possible to interfere with the operation of the QKD system without revealing its presence. The results of the experiment show that it is not necessary for an attacker to have expensive equipment for intercepting and decrypting quantum keys. The presence of standard optical power couplers and access to the fiber-optic communication lines between the stations of the QKD system allows to interfere with the system operation at the required time, while remaining unnoticed.

The results of experimental studies allow us to formulate concrete conclusions about the vulnerability of the synchronization process of the QKD system: during the synchronization, the active nodes of the coding station are inactive and, therefore, the algorithms for ensuring the protection and control of the optical sync pulse are not functioning; the transmission of optical signals is carried out in multiphoton mode, which allows an attacker to remove a part of the optical power from the quantum communication channel, remaining undetected; an attacker has enough typical fiber optic equipment to interfere with the operation of the system at the stage of quantum key distribution, while remaining unnoticed for control.

ACKNOWLEDGEMENT

Work is performed within the grant of President of Russian Federation for state support of young Russian scientists MK-2338.2018.9 “Creation of an automated algorithm for integrating quantum keys into the data network while providing enhanced security against unauthorized access to the quantum communication channel”.

REFERENCES

- Alomari, E., Manickam, S., Gupta, B. B., Karuppayah, S., & Alfaris, R. (2012). Botnet-based distributed denial of service (DDoS) attacks on web servers: classification and art. arXiv:1208.0403
- AlZain, M. A., Li, A. S., Soh, B., & Pardede, E. (2015). Multi-cloud data management using Shamir's secret sharing and quantum byzantine agreement schemes. *International Journal of Cloud Applications and Computing*, 5(3), 35–52. doi:10.4018/IJCAC.2015070103
- Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., & Smolin, J. (1992). Experimental quantum cryptography. *Journal of Cryptology*, 5(1), 3–28.
- Bhushan, K., & Gupta, B. B. (2018). A novel approach to defend multimedia flash crowd in cloud environment. *Multimedia Tools and Applications*, 77(4), 4609–4639.
- Broadbent, A., & Schaffner, C. (2016). Quantum cryptography beyond quantum key distribution. *Designs, Codes and Cryptography*, 78 (1), 351–382.
- Chan, P., Lucio-Martínez, I., Mo, X., & Tittel, W. (2011). Quantum Key Distribution. *Distribution*, 20. doi:10.1007/978-3-642-04831-9
- Gupta, S., & Gupta, B. B. (2017). Detection, avoidance, and attack pattern mechanisms in modern web application vulnerabilities: present and future challenges. *International Journal of Cloud Applications and Computing*, 7(3), 1–43. doi:10.4018/IJCAC.2017070101
- Distribution, Q. K., & Cases, U. (2010). GS QKD 002 - V1.1.1 - Quantum Key Distribution; Use Cases. *Innovation*, 1, 1–32.
- Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Reviews of Modern Physics*, 74(1), 145–195. doi:10.1103/RevModPhys.74.145
- Gupta, B., Agrawal, D. P., & Yamaguchi, S. (Eds.). (2016). *Handbook of research on modern cryptographic solutions for computer and cyber security*. Hershey, PA: IGI Global.
- Gupta, S., & Gupta, B. B. (2018). XSS-secure as a service for the platforms of online social network-based multimedia web applications in cloud. *Multimedia Tools and Applications*, 77(4), 4829–4861.
- Gupta, S., Gupta, S., & Chaudhary, P. (2017). Enhancing the browser-side context-aware sanitization of suspicious HTML5 Code for halting the DOM-Based XSS vulnerabilities in cloud. *International Journal of Cloud Applications and Computing*, 7(1), 1–31. doi:10.4018/IJCAC.2017010101
- Kurochkin, V., Zverev, A., Kurochkin, J., Riabtzhev, I., & Neizvestnyi, I. (2012). Quantum Cryptography Experimental Investigations. *Photonics*, 5, 54–66.
- Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J., & Makarov, V. (2010). Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics*, 4(10), 686–689. doi:10.1038/nphoton.2010.214
- Makarov, V. (2007). Quantum cryptography and quantum cryptanalysis [doctoral thesis]. Norwegian University of Science and Technology.

- Pljonkin, A., & Rumyantsev, K. (2016, March). Single-photon synchronization mode of quantum key distribution system. In *2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT)* (pp. 531-534). IEEE. doi:10.1109/ICCTICT.2016.7514637
- Pljonkin, A., & Rumyantsev, K. (2016, October). Quantum-cryptographic network. In *2016 IEEE East-West Design & Test Symposium (EWDTS)* (pp. 1-4). IEEE. doi:10.1109/EWDTS.2016.7807623
- Pljonkin, A., Rumyantsev, K., & Singh, P. K. (2017). Synchronization in Quantum Key Distribution Systems. *Cryptography*, *1*(3), 18. doi:10.3390/cryptography1030018
- Pljonkin, A. P. (2017, March). Features of the Photon Pulse Detection Algorithm in the Quantum Key Distribution System. In *Proceedings of the 2017 International Conference on Cryptography, Security and Privacy* (pp. 81-84). ACM. doi:10.1145/3058060.3058078
- Rumyantsev, K. E., & Pljonkin, A. P. (2015, December). Synchronization algorithm of quantum key distribution system with protection from unauthorized access. In *2015 Workshop on Recent Advances in Photonics (WRAP)* (pp. 1-4). IEEE. doi:10.1109/WRAP.2015.7805988
- Rumyantsev, K. E., & Pljonkin, A. P. (2016, January). Preliminary stage synchronization algorithm of auto-compensation quantum key distribution system with an unauthorized access security. In *2016 International Conference on Electronics, Information, and Communications (ICEIC)* (pp. 1-4). IEEE. doi:10.1109/ELINFOCOM.2016.7562955
- Rumyantsev, K. Y., & Pljonkin, A. P. (2015). Security of synchronization mode of quantum keys distribution system. *Izvestiya SFedU. Engineering and Science*, *5*(166), 135–153.
- Sajeed, S., Huang, A., Sun, S., Xu, F., Makarov, V., & Curty, M. (2016). Insecurity of detector-device-independent quantum key distribution. *Physical Review Letters*, *117*(25), 250505. doi:10.1103/PhysRevLett.117.250505 PMID:28036200
- Stucki, D., Gisin, N., Guinnard, O., Ribordy, G., & Zbinden, H. (2002). Quantum key distribution over 67 km with a plug&play system. *New Journal of Physics*, *4*(1), 41.
- Tewari, A., & Gupta, B. B. (2017). Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags. *The Journal of Supercomputing*, *73*(3), 1085–1102. doi:10.1007/11227-016-1849-x
- Yuen, H. P. (2016). Security of Quantum Key Distribution. *IEEE Access*, *4*, 724–749. doi:10.1109/ACCESS.2016.2528227

This research was previously published in the International Journal of Cloud Applications and Computing (IJCAC), 9(1); pages 50-58, copyright year 2019 by IGI Publishing (an imprint of IGI Global).

Chapter 16

Optimal Parameter Prediction for Secure Quantum Key Distribution Using Quantum Machine Learning Models

Sathish Babu B.

RV College of Engineering, Bangalore, India

K. Bhargavi

Siddaganga Institute of Technology, India

K. N. Subramanya

RV College of Engineering, Bangalore, India

ABSTRACT

The advent of quantum computing is bringing threats to successful operations of classical cryptographic techniques. To conduct quantum key distribution (QKD) in a finite time interval, there is a need to estimate photon states and analyze the fluctuations statistically. The use of brute force and local search methods for parameter optimization are computationally intensive and becomes an infeasible solution even for smaller connections. Therefore, the use of quantum machine learning models with self-learning ability is useful in predicting the optimal parameters for quantum key distribution. This chapter discusses some of the quantum machine learning models with their architecture, advantages, and disadvantages. The performance of quantum convoluted neural network (QCNN) and Quantum Particle Swarm Optimization (QPSO) towards QKD is found to be good compared to all the other quantum machine learning models discussed.

DOI: 10.4018/978-1-7998-8593-1.ch016

INTRODUCTION

Today's e-manufacturing, digital world provides a variety of services for the benefit of mankind, which includes e-Health, e-Bank, e-Hotel, e-Government and e-Commerce. For successful operation of these services several factors, like privacy, security, confidentiality, cost, trust, compatibility, and standardization, need to be taken into account. Among all the factors security is given paramount importance as the data being exchanged need to be protected from third party attacks. Traditional cryptography is one of the methods that allow us to store and send the data via encryption and reverse decryption process and established secure communication between two parties by protecting the data from attackers using public and private key distribution strategies (Van & Thijssen, 2015).

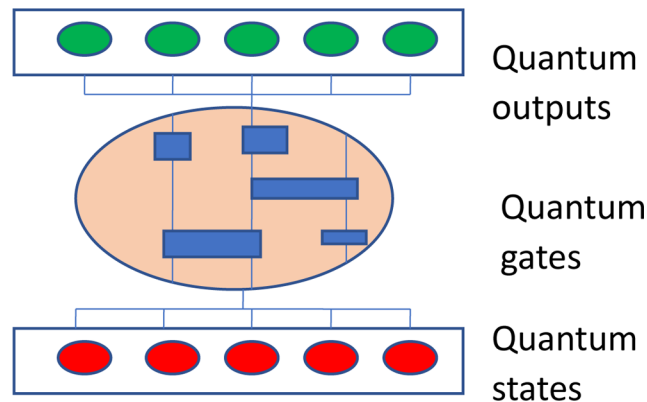
Some of the consequences of traditional cryptography are listed below.

- The message which is strongly authenticated using cryptographic mechanism sometimes makes it difficult to take legitimate decisions at crucial time.
- The speed of execution slows down due to complex mathematical operations.
- Providing selective access to the data is difficult using crypto system.
- The design of the crypto system is poor in terms of architecture, protocol, and procedures used for encoding and decoding.
- Cost of setup and operation of public key cryptosystem is high as it demands separate public key infrastructure.

QUANTUM COMPUTING: AN OVERVIEW

Quantum computing is a revolutionary technology which leverages the characteristics of quantum mechanics such as superposition and entanglement to perform computation extremely faster than classical computing technologies (Feynman, 1982).

Figure 1. Quantum computing process

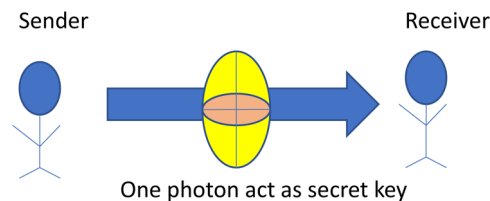


Many forms of quantum technologies are already in use, out of which quantum key distribution has been pioneered by using commercially available quantum computers. Quantum sensors and actuators are allowing scientists to work at nano-scale levels with remarkably higher precision and sensitivity. Development of quantum processors is another main stream activity which is seriously taken up by some of the top-notch technology companies. A generic representation of quantum computing process is given in figure 1, consists of quantum states whose output is processed by quantum gates to yield quantum outputs.

The advent of quantum computers is bringing in the following threats to successful operations of classical cryptographic techniques.

- Classical cryptographic algorithms rely on the complexity of the mathematical function used for encryption and decryption, which can be easily tackled by quantum computers using photon properties.
- Shors quantum computer algorithm is an attack on asymmetric cryptographic algorithms as it can easily find prime factors for the given integer (Yimsiriwattana & Lomonaco, 2004).
- Grover's quantum computing algorithm weakens symmetric cryptographic algorithms as it can determine the unique input to a black box output generating function using $O\sqrt{N}$ function evaluation, where N represent the size of the evaluation function (Zalka, 1999).
- Quantum hacking affects the security and privacy of key agreement-based protocols like Diffie–Hellman (DH), and Menezes–Qu–Vanstone (MQV) through photon polarization.
- Encryption algorithms like Rivest-Shamir-Adleman (RSA), Digital Signature Algorithm (DSA), and elliptic curve cryptography (ECC) are breakable as a quantum computer can easily factor the large keys.

Figure 2. High level view of quantum cryptography



QUANTUM CRYPTOGRAPHY: AN OVERVIEW

The consequence of classical cryptography led to the innovation of quantum cryptography which was developed by Stephen Weisner in the year 1970 (Brassard & Crepeau 1996). In quantum cryptography the cryptographic operations are performed and the data is stored in qubits i.e., each bit can be on, off, or both which is obtained by superposition of the multiple quantum states whereas in traditional cryptography the cryptographic operations are carried out by storing the data in binary format i.e., either on or off. As a result the quantum cryptography allows quantum computation to be performed in order of magnitude which is super faster than the conventional processors in the system (Goyal, Aggarwal, &

Jain,, 2011),(Lakshmi & Murali, 2017). A high level view of quantum cryptography is shown in figure 2. The major differences between classical cryptography and quantum cryptography are given in Table 1.

Table 1. Classical cryptography versus quantum cryptography

Classical Cryptography	Quantum Cryptography
Relies on mathematical formulas.	Relies on the law of quantum physics.
It is vulnerable to the improvement in technologies.	It is not vulnerable to the improvement in the technologies.
Extent of security achieved is dependent on the complexity of factoring the large integer number.	Extent of security is dependent on the quantum superposition and photon polarization rate.
Classical cryptography protocols are usually device dependent and rarely device independent.	Quantum cryptography protocols are device independent.
The bit rate is limited by the limitation of the computational resources.	The bit rate supported extends up to 1Mbits/second.
The communication range supported is millions of miles.	The communication range supported is limited to few 10's of miles.
Register storage is up to 2^n bit strings.	Register storage is up to one n bit strings.
The life expectancy of the classical cryptographic algorithms keeps changing due to the changes in mathematical computation.	The life expectancy of the quantum cryptographic algorithms does not change as the laws of physics remain constant.
Stand alone systems with portable software are enough to perform classical cryptographic computations.	Dedicated quantum computers are required to perform quantum operations.
It is independent of the transmission medium used for data exchange.	It is dependent of the transmission medium used for data exchange.
It is appropriate for long distance communication.	It is inappropriate for long distance communication.
It is not costly as the mathematical computations can be performed on resource constrained devices.	It is costly as for transmission of every photon a separate quantum channel is required.
Supports sequential execution of computational tasks.	Supports parallel execution of computational tasks.

APPLICATIONS OF QUANTUM CRYPTOGRAPHY

The quantum cryptography is being used in variety of applications where the traditional cryptography fails to provide required amount of security (Ellie, 2018), (Lee, Barnum, Bernstein, & Swamy, 1999). Few of the important applications of quantum cryptography are given below.

- Developing an ultra-secure voting system which supports safe transfer of votes from one counting station to another counting station and prevents fraudulent elections from being conducted.
- Transition from traditional internet to quantum internet which prevents hacking of confidential data.
- Establishing secure communication between national and international bank for safe exchange of financial data and the transmission channels used are not susceptible to security threats.
- Maintaining and transferring the defense documents over the internet by preventing the threats of copying the data from eavesdropper.

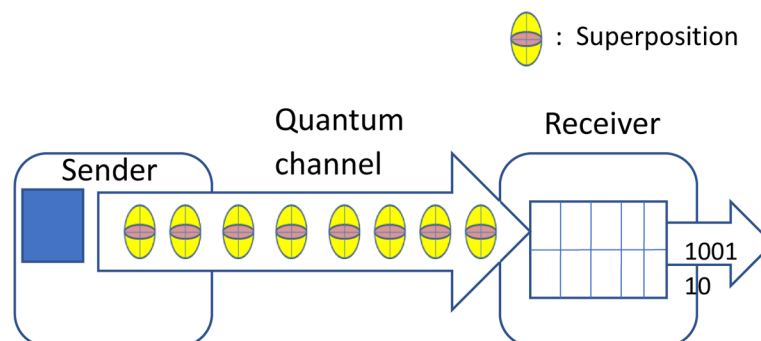
Optimal Parameter Prediction for Secure Quantum Key Distribution Using Quantum ML Models

- Establishing secure communication over open space environment between the satellites and astronomers by preventing the attacks from adversaries.
- Facilitating fast search mechanisms over the database in which every record is visited individually using quantum computer enabled with qubit superposition principle.
- Optimal solutions to NP-hard and unpredictable problems like travelling salesman, rice's theorem, halting problem, and so on are given quickly using quantum algorithms.
- Performing predictive analytics over the business database to forecast the future trends by mining the hidden patterns in the data collected.
- Analysis of complex structure of human brain in which billions of neurons are interconnected in microscopic manner.
- Understanding chemical and physical properties of DNA structure and even to predict the future dynamics of the molecular structures of DNA.
- Exploring the power of genetic programming using quantum computing to simulate the mechanism of selection, crossover, and mutation.
- Real time processing and exact analysis of drug discovery process using quantum computers.
- Controlling of air traffic by streamlining the traffic and maintaining the confidentiality of the operational data.
- Securing the IoT-based smart grids using quantum cryptography and secure transmission of power data.

QUANTUM-BASED KEY DISTRIBUTION (QKD)

There is a tremendous pressure in the industry to make the classical cryptographic techniques quantum safe, which has given rise to intense research in the domain of quantum-based key distribution (QKD) which makes use of properties of photons to securely exchange the keys or key related information between the communication entities. Quantum key distribution is considered as replacement for traditional key distribution strategies due to the several reasons like ease detection of eavesdropper, suitable for long-term security, capacity to deliver unrestricted security, uses minimum resources for key exchange, exhibits continuously improving features, cannot be virtually hacked, relies on physics laws instead of

Figure 3. QKD process



mathematical functions, and so on (Gottesman, Lo, Lutkenhaus, & Preskill, 2004). A sample depiction of the QKD process is given in figure 3.

To conduct QKD in a finite time interval there is a need to estimate photon states and analyze the fluctuations statistically. The choice of the intensity and the probability of sending the message, are difficult to estimate in quantum cryptography and is directly related to the optimal performance of the system. Many of the existing QKD protocols over symmetric and asymmetric security channels, uses coordinate descent algorithm to determine the intensity and probability of sending the message were suffered from delay and the increased requirements of quantum computing resources (Bennett & Brassard, 2014). As there are many efforts to carry out QKD on mobile devices like the drone, mobile phones, satellites which demands the performance over large scale networks. Some of the practical challenges for QKD are listed below.

- Parameter optimization during key distribution is computationally intensive for both smaller and larger connections.
- Compared to classical key distribution quantum key distribution is complex as it just extends the existing secret key model.
- The use of quantum key does not prevent hypothetical hacking i.e. the hacker tries to insert large amount of data during decryption.
- QKD strategy works at lower rate as some of the existing optical fibers are incompatible with the developed QKD.
- The success rate of QKD is limited to individual system but they don't span towards global large-scale networks.
- The certification of security of QKD pertaining to market and laws are not completely defined.
- The QKD strategy is vulnerable to some of the attacks like man-in-the-middle, side channel, device imperfections, and errors in calibration.
- The scalability factor of QKD chip is still less as it incorporates single photon detectors with amplitude modulator and homodyne detectors.
- The cost of integration of light weight QKD models in the mobile devices is high due to high level of miniaturization.

Among all the challenges listed, parameter optimization for secure QKD is addressed in the chapter using quantum machine learning models with a self-learning ability. These models are useful in predicting the optimal parameters for quantum key distribution as they offer several prospects in terms of speed, storage capacity, accuracy, and efficiency.

QUANTUM MACHINE LEARNING (QML)

QML is an interdisciplinary research which combines quantum physics with machine learning. It is a study to build the suit of machine learning techniques as quantum algorithms to run on quantum computers. Learning basically deals with how energy evolution takes place in the quantum circuits (Biamonte, Wittek, Pancotti, Rebentrost, Wiebe, & Lloyd, 2017), a diagrammatic representation of the QML process is given in Figure 4. The driving force for QML process is the dataset, which gets encoded and are passed to the quantum circuit via gate parameters then the results obtained are verified against the objectives

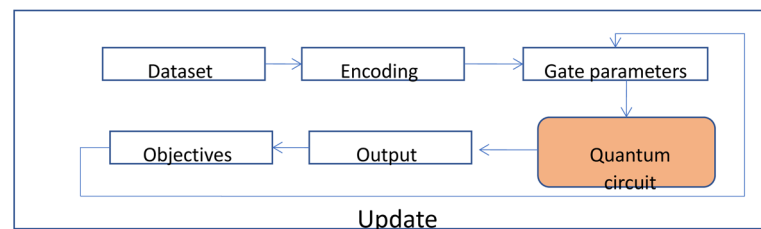
Optimal Parameter Prediction for Secure Quantum Key Distribution Using Quantum ML Models

set. The process of reading the input from the gate parameters and passing through quantum circuit for verification of the output is repeated until desired level of accuracy is obtained.

QML can also be employed over the data generated by quantum experiments and there are also efforts to propose quantum learning theory. Some of the applications of QML are listed below.

- Simulation of movements of the molecules and establishing interaction between the molecules.
- Discovery of advancement in the field of medical science and discovery of drug materials.
- Topological analysis of the big data with accelerated speed.
- Used to train classical Boltzmann machines to perform scientific computations.
- Preserving the cryptographic data from hackers.
- Establishing the quantum awareness in brain cognition.
- Used to generate music which leads to creative productions.
- Generation of TV scripts by mimicking the realistic set of dialogues.
- Generation of text using high level quantum enabled machine learning APIs.
- Detection and classification of objects from complex image scenario.
- Scenario based classification of lanes for automated driving.
- Safety critical classification of car and cyclist scenarios using trajectory data.
- Automatic generation of dramatic and piano music using popular projects like Magenta, DeepJazz, BatchBot, FlowMachines, WaveNet, and GRUV.
- Voice recognition and classification with quadratic speedup.
- Anomaly and fraud detection using elastic quantum search APIs.
- Segmentation and analysis of market using quantum machine learning classification models.
- Automatic translation of scripts written in one language into another language.
- Identification of abnormalities in the financial contracts and development of precise credit lending applications for banking sectors.
- Quick information retrieval based on the images and texts in popular search engines and shopping sites.

Figure 4. QML process



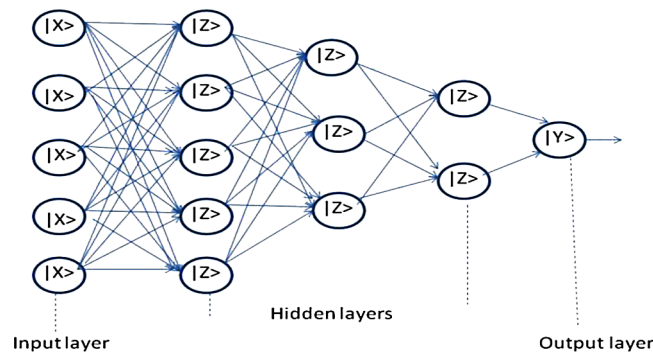
Some of the potential quantum machines learning models used for parameter optimization are: Quantum Feed Forward Neural Network (QFFNN), Quantum Recurrent neural network (QRNN), Quantum Backpropagation Neural Network (QBNN), Quantum Convolved Neural Network (QCNN), Quantum Reinforcement Learning (QRL), Quantum Q learning (QQL), Quantum Particle Swarm Optimization

(QPSO), Quantum Annealing (QA), and Quantum Differential Evolution (QDE). We provide the detailed discussion on these models in the following subsections.

QUANTUM FEED FORWARD NEURAL NETWORK (QFFNN)

The QFFNN includes the generalization of the classical neural network model with coherent quantum inputs. The individual neurons are made revisable, and they are generalized to become quantum reversible. The networks of neurons are trained using the global gradient descent algorithm, which generalizes the cost function. The performance of QFFNN is found to be excellent over the conventional feed forward neural network models for training dense, large-scale, fully connected networks (Wan, Dahlsten, Kristjansson, Gardner, & Kim, 2017).

Figure 5. $|X\rangle * |Z\rangle * |Y\rangle$ QFFNN architecture



The simple architecture of QFFNN is given in figure 5. It mainly consists of three layers i.e., quantum enabled input layer, several hidden layers, and an output layer. The QFFNN is used for classification jobs and the quantum enabled neurons are referred as qurons, and qurons are predefined in input layer, hidden layers, and the output layer. The qurons offer several prospects over the classical neurons in terms of integration, dissipative dynamics and unitary quantum theory. The input is processed sequentially from the input layer through several hidden layers and aggregated at the output layer. The summary of the QFFNN machine learning model are given in Table 2.

The optimality in parameter prediction for secure key distribution using QFFNN is dependent on the type of the algorithm used for training of the QFFNN model. The model is able learn the complex, nonlinear relationship among the input data samples easily in which the connection between the data samples do not form a cycle. The convergence rate is also high due to the deployment of multi level neurons in the output layer and its training is easy compared to the training of the single level neurons in the output layer. In parameter prediction continuous input is fed into the neural network to generate continuous parameter prediction as output. The flow of data from the input layer of the network to the output layer is strictly pre-calculated which makes the model to work in a more efficient manner compared to traditional systems.

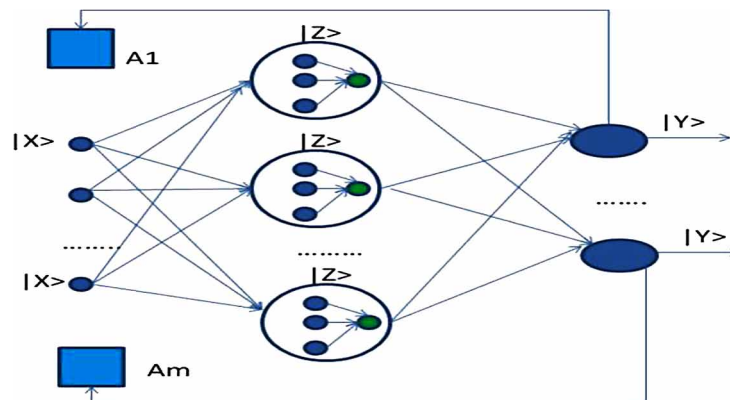
Table 2. Summary of QFFNN

<p>Prospects:</p> <ol style="list-style-type: none"> 1. Exponential storage capacity to process huge amount of information. 2. Accelerated speed of processing. 3. Ability to learn easily from large neural networks through empirical observations. 4. Easily captures non-linear relationship between input and output variables. 5. Prediction accuracy is high and is also towards the actual value. 6. Errors are assessed very easily and are prevented from propagating to other stages of the network. 7. Ability to process unseen relationships in the input data is high which helps in generalization of the input model and even predict from unseen data. 8. Self-associative nature of qurons in QFFNN leads to efficient implementation of multi modular recognition schemes. 9. Quantum associative memory leads to store complicated patterns and even recall it within the specified time interval.
<p>Consequences:</p> <ol style="list-style-type: none"> 1. There might be chances of deviation in the QFFNN output achieved due to sub-quantum level fluctuation. 2. The randomness in sub quantum level causes problems during quantum experiments. 3. Treating individual qubits as neuron in the QFFNN becomes complex during initial iterations. 4. The architecture of QFFNN is difficult to understand due to non-evolutionary behavior of qurons in feedforward network.
<p>Training methods:</p> <p>Trainlm, gradient descent, content based filtering, delta rule, and genetic algorithms,</p>
<p>Precision:</p> <ol style="list-style-type: none"> 1. For uniform datasets after sufficient training iterations the QFFNN model achieved an accuracy of 60%. 2. For non-uniform datasets the accuracy of prediction is below 50% as even with several iterations of training the exact number of hidden layers and number of hidden nodes in every layer could not be determined easily.
<p>Activation functions: Sigmoid, TanH, and ReLU.</p>

QUANTUM RECURRENT NEURAL NETWORK (QRNN)

The QRNN includes quantum algorithms among the connections between the nodes to form a directed graph using the temporal sequence. The performance of QRNN is excellent over large scale data as it operates at exponentially high speed compared to classical recurrent neural network models. Hence QRNN is extensively applied to a variety of applications including pattern recognition, pattern mining, pattern reconstruction, and optimization (Luitel, & Venayagamoorthy, 2010), (Kutvonen, Sagawa, & Fujii, 2018).

Figure 6. $|X\rangle * |Z\rangle * |Y\rangle$ architecture of QRNN with contextual units



Most popular QRNN is Hopfield network which is used in applications like pattern recognition and optimization. The architecture of QRNN is given in figure 6. Which mainly consists of quantum enabled input layer, hidden layer, output layer, and contextual units. The connection from output layer is given to contextual units, at every time interval the input sample is forwarded from one layer to another and the learning rule gets updated. The qurons in QRNN stores the previous values in the hidden states which are used in generating highly precise output even in the presence of the uncertainty. The summary of the QRNN machine learning model is given in Table 3.

The optimality in parameter prediction for secure key distribution using QRNN model dependent on the type of the data labels used for labeling the data samples. The data samples can be labeled either sequentially or non-sequentially, after feeding the data samples the training of QRNN model is easy as it is composed of very few training parameters. The QRNN model is able to model the sequence of inputs in which every current input is dependent on the previous input. The capability of the QRNN model to remember each and every interaction throughout the process of learning makes it suitable for parameter prediction applications. It allows for the formation of the loops within the QRNN model as a result the information will stay inside the network for long duration of time. Compared to other traditional neural networks the recurrent neural network can learn long sequences of the input with long time gaps between the input samples easily and efficiently in parallel.

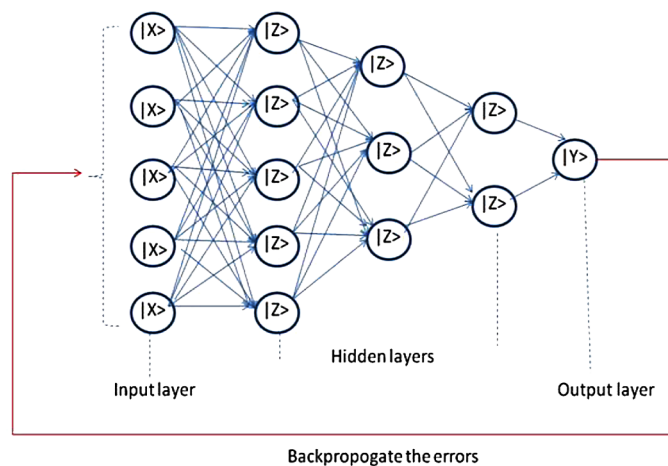
Table 3. Summary of QRNN

<p>Prospects:</p> <ol style="list-style-type: none"> 1. Exponentially sized polynomial numbers can be easily stored in QRNN qubits. 2. The computational complexity of QRNN is very low i.e., logarithmic value. 3. Achieves exponential speedup compared to classical RNN. 4. QRNN uses quantum algorithm to perform large matrix multiplication. 5. Easy to extract the hidden pattern in the input sample which reduces the runtime of the QRNN model. 6. The training of the QRNN is done using Hebbian model approach which helps in solving complex linear equations in quadratic time interval. 7. The transfer of data in quantum states to quantum devices is easy due to the availability of the pure state data in the hidden layers of the QRNN model. 8. The QRNN model is data-driven and generalized approach can be easily applied to any of the new fields without prior knowledge about the field.
<p>Consequences:</p> <ol style="list-style-type: none"> 1. The QRNN model still suffers from inherent stability problem as several architectures of RNN into a single QRNN. 2. If gradient descent optimization method is used while training the QRNN the chances of network getting exploded is more. 3. The QRNN model demands frequent updating of the architecture elements along with the coefficient parameters which causes problems during practical implementation of the model. 4. Embedding the QRNN model inside the deep learning model is difficult using tanh and ReLu activation function.
<p>Training methods:</p> <p>Stochastic gradient descent, recursive filter, correlation rule, Bayes filter, and convolution filter</p>
<p>Precision:</p> <ol style="list-style-type: none"> 1. For uniform data samples with sequential labeling the performance of the QRNN model falls in the range of 70% as it efficiently handles the problems like gradient vanishing, and exploding tendency in the network. 2. For non-uniform data samples with non-sequential labeling the performance of the QRNN model is in average range i.e., 50% as it fails to process the long sequence of non-sequential data samples and it gets stuck in recurring gradient vanishing problem.
<p>Activation functions:</p> <p>Softmax, kernel activation function, and linear.</p>

QUANTUM BACKPROPAGATION NEURAL NETWORK (QBNN)

The QBNN is used exhaustively in pattern recognition by back-propagating the errors using various kinds of activation functions. The backpropagation of the errors through a neural network makes the network self-programmable, self-organizable, interactive, and are capable enough for solving computation intensive problems (Gonçalves, 2016). The performance of QBNN is faster and more accurate compared to conventional BPNN models in prediction problems.

Figure 7. $|X\rangle * |Z\rangle * |Y\rangle$ QBNN architecture



The simple architecture of QBNN model is given in figure 7. It mainly consists of two stages: the first stage is the learning stage and the second stage is the Backpropogation stage. During the learning stage the network learns from the input samples through several layers of feed forward neural network and in the backpropogation stage the neurons in output layer back propagates the error and make the network to get self-stabilized. The summary of QBNN machine learning model is given in Table 4. The optimality in parameter prediction for secure key distribution using QBNN model is dependent on number of qurons considered in every layer of the network. The poor performance is due to several factors like extremely sensitive to noise and outliers, the use of matrix based approach for Backpropogation leads to lot of errors, requires smaller learning rate to stabilize the learning process, too few qurons in the layers causes underfitting problem, finding accurate weights for Backpropogation of the errors takes too long time, and so on.

QUANTUM CONVOLUTED NEURAL NETWORK (QCNN)

The quantum inspired CNN deep learning models uses a variable sized small set of parameters for training and implementation of the quantum neural networks for image analysis. The QCNN is capable of performing both encoding and decoding tasks in parallel which outperforms the conventional CNN

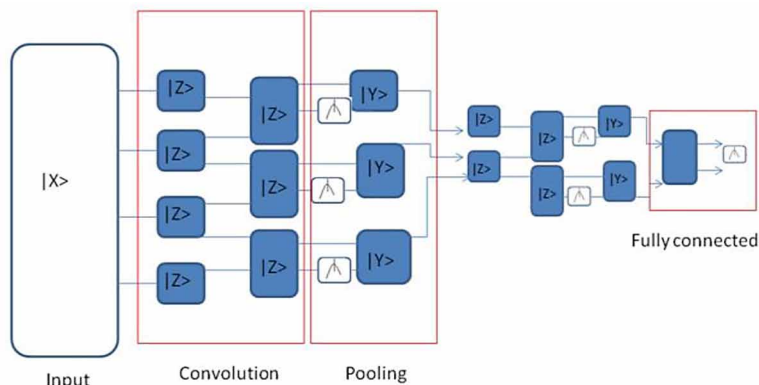
by removing the problem of exploding gradients in image recognition and classification tasks (Cong, Choi, & Lukin, 2019).

Table 4. Summary of QBNN

<p>Prospects:</p> <ol style="list-style-type: none"> 1. It is more efficient in terms of energy as the quantum states are embodied easily inside the multi-layer backpropagation network. 2. Exhibits exponential speed due to parallel computation of quantum states. 3. The QBNN model is easily adaptable in nature due to the back propagation of errors. 4. The use of NOT gates with lowered decoherence level along with the qurons makes the topology of the QBNN model more generic. 5. The ability to solve complex non-linear problem is high as qurons in QBNN model are self-adaptable and can easily understand the dynamic stochasticity and periodic variation in the learning environment. 6. The learning rate of the qurons decreases from larger value to smaller value and adjusts the weights between the qurons automatically which leads to rapid learning.
<p>Consequences:</p> <ol style="list-style-type: none"> 1. Convergence speed of the QBNN model is very slow as the gradient descent method is used for error back propagation. 2. Validating the learning ability of the QBNN model is difficult to the reoccurrence of the XOR problems in the hidden and output layers of the QBNN model. 3. The error propagation rate during training phase of the QBNN model is high due to inappropriate updating of the weights associated with the learning phase of the QBNN model. 4. The random superposition of qurons during training and testing period of the QBNN model leads to weak connection between the qurons among various layers of the QBNN model.
<p>Training methods:</p> <p>Genetic algorithms, evolutionary theory, and chain rule</p>
<p>Precision:</p> <p>With respect to both uniform and non-uniform data samples the QBNN model suffers from poor performance in terms of parameter prediction for key distribution.</p>
<p>Activation functions:</p> <p>Logistic, gradient backpropagation, and threshold.</p>

The architecture QCNN is given in figure 8, which mainly consists of three layers i.e., convolution layer, pooling layer, and fully connected layer. The parameters unitaries in the three layers of the QCNN will be initialized and training happens through gradient descent learning. The convolution layer is composed of several unitaries and processes images of varying dimensions. The pooling layer is mainly

Figure 8. Architecture of QCNN



Optimal Parameter Prediction for Secure Quantum Key Distribution Using Quantum ML Models

used to reduce the size of the QCNN model by computing final mean unitary over several the initial unitaries. The fully connected layer consists of non-local measurements used to do classification jobs. The summary of the QBNN machine learning model are given in Table 5.

The use of QCNN in predicting the optimal parameters for quantum key distribution is beneficial in terms of learning rate, convergence speed, and accuracy. The QCNN model can quickly capture the patterns in the both uniform and non-uniform data samples and they involve less complexity and even save lot of memory compared to conventional CNN model. The QCNN model consists of only $O(\log(N))$ variational input parameters for any input of size N qubits. As a result it is very easy to train and test the realistic quantum key distribution applications and achieves near optimal accuracy. It can also recognize any infinitesimal quantum states during key distribution using a single dimensional topological analysis mechanism. It also has inbuilt error correction model which prevents the propagation of errors from one phase to another phase during key distribution. The performance of the QCNN model is found to be good due to the reasons like use of local spatial coherence in the input data samples, parameter sharing using convolutional and pooling layers, ability to easily locate the features in the input data samples, easily adaptable model due to the use of data augmentation and regularization, and so on.

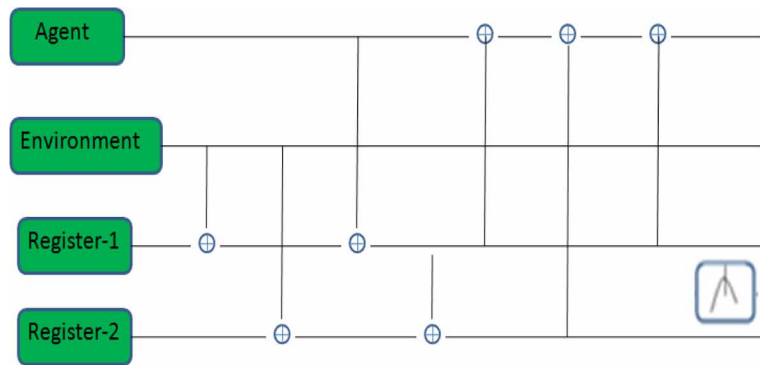
Table 5. Summary of QCNN

<p>Prospects:</p> <ol style="list-style-type: none"> 1. The speed of operation increases exponentially using qHob and qHeb training algorithms. 2. The accuracy achieved in classification jobs is high due to quantum enabled error correction mechanism. 3. The addition of quantum convolution layer into the conventional CNN architecture increases the power of computation. 4. The hypothesis generated by the QCNN is correct due to the use of quantum-convolutional circuits. 5. The QCNN model is highly scalable as quantum-convolutional layers are free from error and can operate with a smaller number of quantum circuits. 6. Able to model complex non-linear relationship in cellular automata as flexibility is provided to keep layer specific configuration attributes. 7. Polynomial sized image classification problems can be solved easily as the QCNN model allows several quantum-convolutional layers to be stacked one after the other.
<p>Consequences:</p> <ol style="list-style-type: none"> 1. In order to achieve higher accuracy, the QCNN model demands large data samples. 2. The chance of converging to local optimal solutions is high as the QCNN model exhibits higher dependency on the initial parameter tuning. 3. The QCNN model fails to handle the invariance caused during translation i.e., when the images with slight variation is fed during training the qurons in the quantum-convolutional layers won't get triggered as they cannot encode the position and orientation of the images. 4. The use of qurons in pooling layer leads to loss of information.
<p>Training methods: Backprop, RMSProp, and Adadelata</p>
<p>Precision: The performance of the QCNN model goes above 85% for all forms of data i.e., uniform and no uniform samples considered for training and testing.</p>
<p>Activation functions: tanh, ReLu, and LeakyReLu</p>

QUANTUM REINFORCEMENT LEARNING (QRL)

The QRL model combines the quantum theory with a reinforcement learning agent, which works based on state superposition principle and also exploits the quantum parallelism for updating over time. The QRL model decides the probability of Eigen value based on the amplitude which gets updated by collecting the rewards which increase the convergence rate of the learning model and increases the learning ability of the agent by achieving the proper balance between exploration and exploitation (Dong, Chen, Li, & Tarn, 2008).

Figure 9. Architecture of QRL



The architecture of QRL is given in figure 9 which mainly consists of four main components i.e., agent, environment, register-1, and register-2. The interaction happens in several forms like agent to environment, agent to register-1, agent to register-2, register-1 to register-2, environment to register-1, and environment to register-2. To facilitate accelerated learning logical quantum gates and XOR gates are embedded inside the reinforcement learning protocol. The representation of QRL can be extended easily for multiple qubits systems which are useful for demonstration of applications like harmonic oscillators, superconductors, movement of atoms, and so on. The agent in QRL model easily learns about the environment and meanwhile environment also gains knowledge about the agent and more number of registers can be updated simultaneously which increases the learning speed by receiving maximum possible rewards. The summary of the QRL machine learning model are given in Table 6.

QUANTUM Q LEARNING (QQL)

The QQL model appears in several forms like single valued Q learning, double valued Q learning, multiple agents-based Q learning, these algorithms are combined with the quantum states and action space for parameter optimization in the high-performance computing environment. The application of quantum mechanics in Q learning resolves the contextual bandit problem by preventing the long-delayed reward signals generation (Dunjko, Taylor, & Briegel, 2017).

Table 6. Summary of QRL

<p>Prospects:</p> <ol style="list-style-type: none"> 1. The quantum reinforcement learning is useful for epoch type environment in which the state of the environment keeps changing rapidly. 2. Achieves accelerated speed in object classification by receiving maximum possible rewards over iterations using multi qubits enabled quantum states. 3. The chances of quantum agent failing to perform any desired action is exponentially small due to quadratic improvement in forming high quality learning policies. 4. The quantum agents are adaptable to complex environment as it always takes valuable steps towards the reward in incremental manner. 5. The quantum agent is equipped with hyper parameters or meta parameters which help in fixing any undeterministic problems. 6. The convergent speed rate of the quantum agent is optimal as it perfectly balances between exploration and exploitation.
<p>Consequences:</p> <ol style="list-style-type: none"> 1. It is difficult to realize the fully quantum-controlled environment exactly using quantum agents. 2. The use of progressive wavelet decoders in QRL is infeasible due to the uncertainty involved during decoding. 3. The accuracy achieved in classification jobs is low due to piecewise representation of trajectories in the environment. 4. While dealing with high dimensional environment the use of XOR, NOT, and CNOT causes problems during generalization. 5. Too much reinforcement of the quantum agents can lead to overloading of the quantum states and may produce wrong results.
<p>Training methods:</p> <p>Trial and error approach, cut and try, reward based, and session backpropogation.</p>
<p>Precision:</p> <ol style="list-style-type: none"> 1. The performance of QRL towards parameter prediction for quantum key distribution is satisfactory and lies in the range of 50% for the data samples which are having continuous states. 2. The QRL is a probability-based model with dynamic programming ability which exhibits high accuracy in terms of recall precision, true positive and true negative classification. But when the QRL model is exposed to data samples with discontinuous high dimensional states the model becomes infeasible and significantly slower.
<p>Activation functions:</p> <p>Rectified linear function, softmax, sigmoid, and tanh.</p>

The architecture of quantum Q learning is given in figure 10 which stores the quantum reinforcement learning policies by super-positioning it in the qubits. The value function of the conventional Q learning algorithm is replaced by the quantum enabled action-value function. The quantum agent performs action to get highest possible reward and the learning process is controlled by the discount factor. In QQL the quantum states are based on Markov property that output of each state depends on previous state. By storing the previous experience in every quantum states memory, the actions are taken to maximize the throughput of QQL network and the loss function is also minimized. The summary of the QQL machine learning model are given in Table 7.

Figure 10. Architecture of QQL

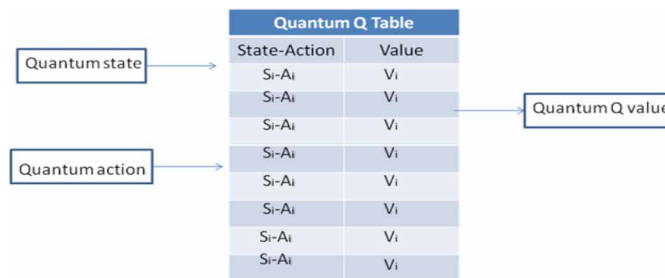


Table 7. Summary of QQL

<p>Prospects:</p> <ol style="list-style-type: none"> 1. The accuracy of the result obtained is high as it consistently updates the policy of learning at regular period of intervals. 2. The convergence rate of the QQL is high as it replaces the value function with the quantum action-value function. 3. Achieves perfect balance between the exploration and exploitation due to the use of quantum states while deriving the action policies. 4. The speed of learning is good as the quantum state-action pair holds most accurate information compared to the ordinary state-action pair of Q learning. 5. The amount of time required to traverse every state of the quantum table decreases due to the use of quantum reinforcement policies. 6. Even when the target function is unstable the training phase of the QQL model remains in steady state.
<p>Consequences:</p> <ol style="list-style-type: none"> 1. The quantum agents give equal weightage to optimal and sub-optimal paths which reduces the quality of Q learning policies formed over high dimensional environment. 2. The chance of trapping in local minimal solution is high when the policies formed are similar to each other. 3. Even the quantum reinforcement learning agents express the inability to deal with the long horizons. 4. The samples required to train the quantum agent's increases with the increase in the number of the quantum states and action pairs.
<p>Training methods:</p> <p>Backpropagation, random batch transition, experience replay, and neural fitted Q iteration.</p>
<p>Precision:</p> <ol style="list-style-type: none"> 1. The performance of QQL model in parameter prediction for quantum key distribution is satisfactory and lies in the range of 50%. 2. For uniform data samples the QQL model quickly learns the pattern by calculating fixed rewards, the use of policy gradient method always leads to perform an action which has highest expected target value. 3. But for non-uniform data samples the performance of the QQL model gets affected as too much of reinforcement leads to overloading of the quon states and which in turn diminishes the quality of results.
<p>Activation functions:</p> <p>Policy gradient, Piece-wise, and min-max.</p>

QUANTUM PARTICLE SWARM OPTIMIZATION (QPSO)

The QPSO model applies quantum laws of mechanics to improve the behavior of conventional PSO to achieve guaranteed global convergence. With the introduction of interpolation operator in QPSO, it is possible to find new globally best solutions in the search space. The QPSO is applied to solve multi-modal complex and constrained problems containing too many varying parameters (Liu, Chen, Chen, & Xie, 2019).

The architecture of quantum Q learning is given in figure 11 which mainly consists of particles with global and local positions. The small particles tend to move towards the larger particles by following the bigger arrow which exhibits highest probability path i.e., the path which moves the small particles towards larger particles. In conventional PSO there might be some smaller particles which are misleading in nature if more number of particles gets attracted towards the misleading smaller particles the chances of getting trapped in local optimal solution is more. This problem is prevented by using Gaussian distribution strategy which determines the misleading local particles easily in the wider search space and prevents the situation of falling into local optima solutions. The summary of the QPSO machine learning model are given in Table 8.

QPSO guarantees to produce global optimal key distribution policies using probabilistic approach for searching better solution within the limited time interval. In QPSO the state of the particles are represented in wave form instead of choosing position and velocity of the particle which makes the technique to be suitable for cryptographic applications. Here the probability of a particle to be present a quantum state is determined using quantum density function which prevents the explosion rate during key distribution. The walking mechanism of QPSO is in isotropic direction which helps in searching global optimal pa-

Optimal Parameter Prediction for Secure Quantum Key Distribution Using Quantum ML Models

rameters among the wide range of highly dense parameter set for training the quantum neural network. The QPSO model exhibits high optimality in parameter prediction due to several features like ability to search global optimal solution using levy flight mechanism, successful quantum logic gate operations over the noisy data samples, computation overhead is less due to the involvement of fewer tuning and control parameters, adaptive quantum states update mechanism which avoids the particles from falling into local optimum solutions, and so on.

Figure 11. Architecture of QPSO

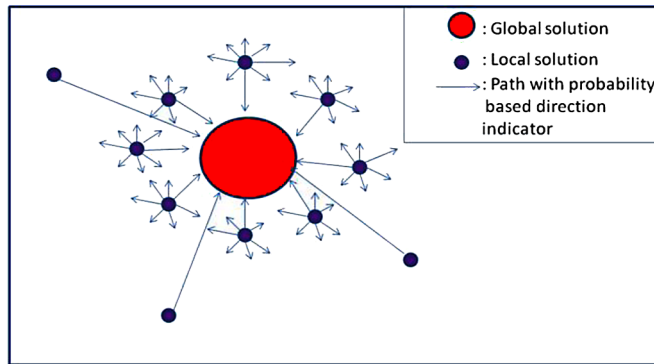


Table 8. Summary of QPSO

<p>Prospects:</p> <ol style="list-style-type: none"> 1. The chances of falling into local optimal solution are prevented by detecting misleading particles early. 2. The speed of computation is high as a smaller number of control parameters are involved in the QPSO and overhead caused by them is also less. 3. The QPSO can easily explore larger search space and consists of very little assumption during computation. 4. By using the uncertainty principle of quantum mechanics, the particles are made capable enough to appear in the search space. 5. The QPSO convergence to globally optimal solution easily compared to classical PSO as it reaches the stopping criteria in very little iteration. 6. The error propagation is also less in the QPSO architecture as it consists of only a smaller number of local optimal solutions. 7. The use of quantum mechanics in PSO algorithms is able to solve any real-world problems in logarithmic time interval. 8. The QPSO follows probabilistic approach in finding the solution in discrete manner which makes it suitable to solve large scale multiple valued real time problems.
<p>Consequences:</p> <ol style="list-style-type: none"> 1. It is difficult to estimate the quantum particles values during beginning interval of learning in QPSO. 2. If the local and global solutions are highly scattered in the wide search space the accuracy of the solution drops. 3. The approach is not suitable for system which is non-coordinated in nature due to its randomness in computation. 4. It demands frequent updating of quantum velocity in the memory which might slow down the convergence rate.
<p>Training methods:</p> <p>Gradient descent, error backpropogation, and wrapper method.</p>
<p>Precision:</p> <p>The optimality in parameter prediction for quantum key distribution using QPSO model is very good and is in the range of above 80% for both uniform and non-uniform data samples.</p>
<p>Activation functions:</p> <p>Hyperbolic tangent, radial basis, and log sigmoid.</p>

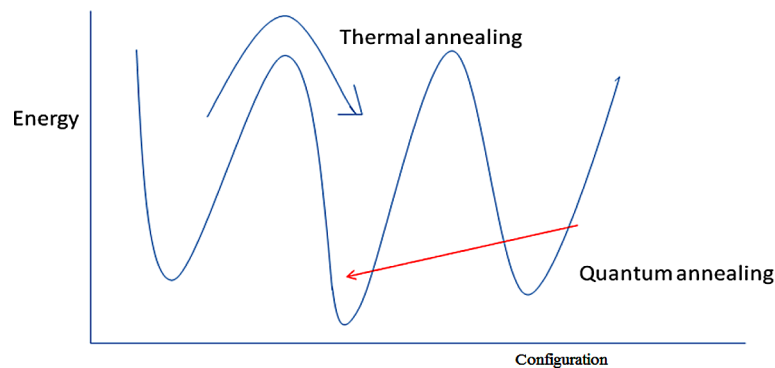
QUANTUM ANNEALING (QA)

The QA is one of the metaheuristic models used to find the global solution among the available set of candidate solutions based on quantum fluctuations. The model finds the global best solution in the existence of several local minima solutions as it applies the quantum mechanical superposition on all possible states with equal weights. Its speed is 100 times faster than conventional simulated annealing and is not sensitive to the missing information during prediction. The quantum annealing is used in variety of complex applications like artificial intelligence, aerospace, rocket launching, and so on (Chancellor, 2017).

Sample architecture of quantum annealing is given in figure 12 the energy applied to the quantum annealing changes with respect to time and it take the shape of D-shaped curve. The amplitude of all the states of quantum annealing is found to vary in parallel whereas in simulated annealing it is totally dependent on energy of the states. The states of the system keep changing continuously by using more number of quantum cost factors which helps in doing the quantum operations in parallel. The use of quantum fluctuation in annealing make sure that that it will never produce a solution which gets trapped in local minima. To perform the tunneling operation quantum computers are preferred than the traditional computers and even the propagation of errors is prevented by using the methodology of quantum entanglement. The summary of the QA machine learning model are given in Table 9.

Some of the characteristics of the quantum annealing which contributes to good performance are reduction in error propagation rate due to qubits computation, ability to solve the problems quickly due to the availability of D-wave processors, arriving at global optimal solution is easy as it the candidate solution can be searched easily by mimicking tunneling with semi-classical energy landscape.

Figure 12. Architecture of quantum annealing



Quantum Differential Evolution (QDE)

The QDE model applies the operators like mutation, crossover, and vector selection over the input sample to select optimal global parameter among the existing several local optimal parameters. The use of quantum-based differential evolution is excellent in terms of speed of operation and rate of convergence (Fu, Ding, Zhou, & Hu, 2013). Sample architecture of quantum differential evolution is given in figure 13. After setting the initial parameters in quantum states the individual trails of candidate solutions are

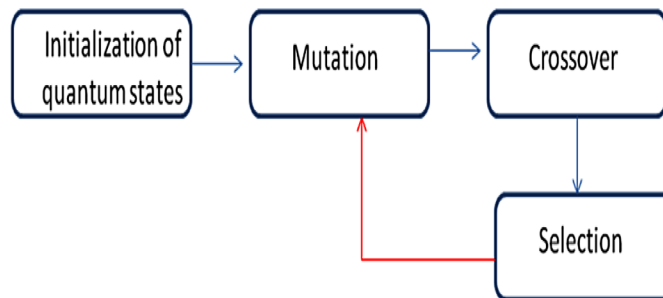
Optimal Parameter Prediction for Secure Quantum Key Distribution Using Quantum ML Models

generated by using crossover operation and the highly fit solutions is selected using selection operator. The quantum states are embedded inside the class states of the candidate solution by using the Monte Carlo method. The position of the individual candidate solutions are updated using the position iteration policy until the stopping criteria is reached. The summary of the QDE machine learning model are given in Table 10.

Table 9. Summary of QA

<p>Prospects:</p> <ol style="list-style-type: none"> 1. The quantum fluctuations methodology of quantum annealing is helping in performing prime number factorization with high speed. 2. The speed of operation is 10^8 times faster than the traditional annealing. 3. Quantum annealing is preferred over the simulated annealing to solve optimization problems as it provides runtime polymorphism. 4. With the increase in the size of the problem the annealing time takes the shape of D formed curve and it is exponentially very lower. 5. The energy required to solve high dimensional problems is very less due to annealing of quantum states.
<p>Consequences:</p> <ol style="list-style-type: none"> 1. If the quantum states are annealed repeatedly over the iteration then it might slow down the quantum annealing process. 2. Often the behavior of quantum annealing is application specific which limits its generality in terms of operation. 3. While solving complex problem with uncertainty the time taken to find global optimal solution is high.
<p>Training methods:</p> <p>Ensemble learning, stochastic gradient descent, and Monte Carlo</p>
<p>Precision:</p> <p>The performance of the QA model with respect to parameter prediction for quantum key distribution is satisfactory in the range of 60% for both uniform and non-uniform data samples.</p>
<p>Activation functions:</p> <p>Periodic function, Boltzmann distribution function, and radial activation function.</p>

Figure 13. Architecture of quantum differential evolution



The performance comparison of all quantum machine learning models is summarized in the Table 11. This shows the performance of various quantum machine learning algorithms with respect to parameters like convergence rate, accuracy, speed of execution, and scalability on a scale of low, medium, or high.

Table 10. Summary of QDE

<p>Prospects:</p> <ol style="list-style-type: none"> 1. Due to the use of quantum search mechanism in differential evolution the tendency of premature convergence gets prevented. 2. It also achieves perfect balance between exploration and exploitation phases which results high optimal solutions. 3. The accuracy in determining the potential candidate solution is high due to the use of quantum states. 4. Ability to process the input data without explicit segmentation and separation is high. 5. The representation of the input data in quantum states is in terms of Q-bit strings which makes the processing stage easier. 6. It guarantees global optimal solution with least concern about the initial parameters setting. 7. The time taken to convergence to global optimal solution is very less due to the involvement of fewer control parameters and use of differential evolution operators. 8. The potential to balance between exploration and exploitation is high as the tendency to converge to sub-optimal solutions is very less.
<p>Consequences:</p> <ol style="list-style-type: none"> 1. The efficiency of the quantum differential evolution algorithms are depended on the initial parameter setting for control parameters and is difficult to select appropriate values for the control parameters which in turn affects efficiency. 2. The efficiency of the quantum differential evolution fails when it is applied over the epistatic problems as it cannot capture the valid expressions in phenotypes with uncertainty. 3. The time taken to find global optimal values for control parameters of quantum differential evolution is high as it requires more number of quantum iterations.
<p>Training methods:</p> <p>Ensemble averaging, error backpropagation, and affinity propagation.</p>
<p>Precision:</p> <ol style="list-style-type: none"> 1. The performance of the QDE model towards parameter prediction for quantum key distribution is not satisfactory as it falls in the range 30% to 50% for uniform and non-uniform data samples. 2. The poor performance of QDE model is due to the reasons like inability to capture exact pattern in the input data sample due to influence of noise, high tendency to fall into local optimal solution due to improper choice of genetic operators, and so on.
<p>Activation functions:</p> <p>Radial basis function, penalty function, and nondifferential neuron function.</p>

Table 11. Comparison of quantum machine learning models

Technique	Convergence Rate	Accuracy	Speed	Scalability
QFFNN	Low	Medium	Low	Low
QRNN	Low	Medium	Medium	Medium
QBNN	Low	Low	High	Low
QCNN	High	High	Medium	High
QRL	Low	Medium	Medium	Low
QQL	High	Medium	Low	Low
QPSO	High	High	High	Medium
QA	Low	Medium	Low	Low
QDE	Low	Medium	Low	Low

CONCLUSION

This chapter provides a brief introduction to quantum cryptography, comparison between quantum key distribution and traditional public and private key distribution strategies. Also discuss the role of parameter prediction and optimization in achieving quantum key distribution in a finite time interval. Several potential quantum machine learning algorithms like QFFNN, QRNN, QBNN, QCNN, QRL,

QQL, QPSO, QA, and QDE are discussed. Among all the quantum machine learning models discussed the performances of the QCNN and QPSO are found to be good towards quantum key distribution.

REFERENCES

- Bennett, C. H., & Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560(12), 7–11. doi:10.1016/j.tcs.2014.05.025
- Biamonte, J., Wittek, P., Pancotti, N., Rebentrost, P., Wiebe, N., & Lloyd, S. (2017). Quantum machine learning. *Nature*, 549(7671), 195–202. doi:10.1038/nature23474 PMID:28905917
- Brassard, G., & Crepeau, C. (1996). 25 years of quantum cryptography. *ACM Sigact News*, 27(3), 13–24. doi:10.1145/235666.235669
- Chancellor, N. (2017). Modernizing quantum annealing using local searches. *New Journal of Physics*, 19(2), 23–24. doi:10.1088/1367-2630/aa59c4
- Cong, I., Choi, S., & Lukin, M. D. (2019). Quantum convolutional neural networks.
- Dong, D., Chen, C., Li, H., & Tarn, T. J. (2008). Quantum reinforcement learning. *IEEE Transactions on Systems, Man, and Cybernetics. Part B, Cybernetics*, 38(5), 1207–1220. doi:10.1109/TSMCB.2008.925743 PMID:18784007
- Dunjko, V., Taylor, J. M., & Briegel, H. J. (2017). Advances in quantum reinforcement learning. In *Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics (SMC)* (pp. 282–287). IEEE Press. 10.1109/SMC.2017.8122616
- Ellie, M. (2018). *4 Amazing Quantum Computing Applications*. DevOps. Retrieved from <https://devops.com/4-amazing-quantum-computing-applications/>
- Feynman, R. P. (1982). Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6), 467–488. doi:10.1007/BF02650179
- Fu, Y., Ding, M., Zhou, C., & Hu, H. (2013). Route planning for unmanned aerial vehicle (UAV) on the sea using hybrid differential evolution and quantum-behaved particle swarm optimization. *IEEE Transactions on Systems, Man, and Cybernetics. Systems*, 43(6), 1451–1465. doi:10.1109/TSMC.2013.2248146
- Gonçalves, C. P. (2016). Quantum neural machine learning-backpropagation and dynamics.
- Gottesman, D., Lo, H. K., Lutkenhaus, N., & Preskill, J. (2004). Security of quantum key distribution with imperfect devices. In *Proceedings of the International Symposium on Information Theory*. Academic Press. 10.1109/ISIT.2004.1365172
- Goyal, A., Aggarwal, S., & Jain, A. (2011). Quantum Cryptography & its Comparison with Classical Cryptography: A Review Paper. In *Proceedings of the 5th IEEE International Conference on Advanced Computing & Communication Technologies ICACCT-2011*. IEEE Press.
- Kutvonen, A., Sagawa, T., & Fujii, K. (2018). Recurrent neural networks running on quantum spins: memory accuracy and capacity.

- Lakshmi, P. S., & Murali, G. (2017). Comparison of classical and quantum cryptography using QKD simulator. In *Proceedings of the International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)* (pp. 3543-3547). Academic Press. 10.1109/ICECDS.2017.8390120
- Liu, G., Chen, W., Chen, H., & Xie, J. (2019). A Quantum Particle Swarm Optimization Algorithm with Teamwork Evolutionary Strategy. *Mathematical Problems in Engineering*.
- Luitel, B., & Venayagamoorthy, G. K. (2010). Quantum inspired PSO for the optimization of simultaneous recurrent neural networks as MIMO learning systems. *Neural Networks*, 23(5), 583–586. doi:10.1016/j.neunet.2009.12.009 PMID:20071140
- Spector, L., Barnum, H., Bernstein, H. J., & Swamy, N. (1999). Quantum computing applications of genetic programming. In *Advances in genetic programming* (pp. 135-160). Academic Press.
- Van Waart, O., & Thijssen, J. (2015). Traditional Cryptography.
- Wan, K. H., Dahlsten, O., Kristjansson, H., Gardner, R., & Kim, M. S. (2017). Quantum generalisation of feedforward neural networks. *NPJ Quantum Information*, 3(1), 36.
- Yimsiriwattana, A., & Lomonaco, S. J. Jr. (2004). Distributed quantum computing: A distributed Shor algorithm. *Quantum Information & Computation*, 2(5436), 60–372.
- Zalka, C. (1999). Grover's quantum searching algorithm is optimal. *Physical Review A*, 60(4), 2746–2751. doi:10.1103/PhysRevA.60.2746

This research was previously published in Quantum Cryptography and the Future of Cyber Security; pages 44-69, copyright year 2020 by Information Science Reference (an imprint of IGI Global).

Section 3

Industry Applications of Quantum Technology

Chapter 17

Quantum Cognition and Its Influence on Decrease of Global Stress Level Related With Job Improvement Strategies: Quantum Brain and Global Stress

Aleksandar Stojanovic

Federal University of Ceara, Brazil

Ana Starcevic

University of Belgrade, Serbia

ABSTRACT

The quantum mind or quantum consciousness group of hypotheses propose that classical mechanics cannot explain consciousness. Quantum theory is used to insert models of cognition that target to be more innovative than models based on traditional classical probability theory, which includes cognitive modeling phenomena in science. At the moment we can say that there is no clearly defined neurophysiological mechanisms of creation of the quantum-like representation of information in the brain, but we can mention the hypothesis of matching the information processing in the brain with quantum information and probability with contextuality as the key word. Using limited cognitive resources, incompatibility provides humans the means for answering an unlimited number of questions, thus promoting parsimony and cognitive economy.

DOI: 10.4018/978-1-7998-8593-1.ch017

INTRODUCTION

The idea that quantum mechanics has something to do with the workings of the mind was proposed by Eugene Wigner who suggested that wave function collapses due to its interaction with consciousness. Freeman Dyson argued that “mind, as manifested by the capacity to make choices, is to some extent inherent in every electron.” (“Quantum Approaches to Consciousness”, 2011; Dyson, 2004).

Many scientists considered this option as improbable describing it as a myth with no scientific basis.

David Chalmers argued against quantum consciousness. He instead discussed how quantum mechanics may relate to dualistic consciousness. Chalmers is skeptical of the ability of any new physics to resolve the hard problem of consciousness.

The main argument against the quantum mind hypothesis was the assertion that quantum states in the brain would lose coherency before they reached a scale where they could be useful for neural processing, which was elaborated by Tegmark, who made calculation in which quantum systems in the brain decohere at sub-picosecond timescales, which are considered to be too short to control brain function. If there is no brain-mind identity, mind-states could be in an abstract space that is not affected by decoherence. (Khrennikov,2009;Van den Noort,2016).

Quantum cognition represents an innovative field which applies the mathematical formalism of quantum theory to model of cognitive phenomena such as information processing by the human brain, language, decision making, human memory, concepts and conceptual reasoning, human judgment, and perception. This field makes a great difference from the quantum mind as it is not reliant on the hypothesis that there is something micro-physical quantum mechanical about the brain as it is based on the quantum structure paradigm. The main mechanism or concept is based on a information processing by complex systems such as brain structures. It is hypothesised that contextual dependence of information and probabilistic reasoning could be mathematically described in the framework of quantum information and quantum probability theory (Caves, 2002;Tversky, 1992; Savage, 1954).

Quantum theory is used to insert models of cognition that target to be more innovative than models based on traditional classical probability theory which includes cognitive modeling phenomena in science. Since the use of a quantum-theoretic framework is for modeling purposes, the identification of quantum structures in cognitive phenomena does not presuppose the existence of microscopic quantum processes in the human brain (Poitros, 2009).

We can observe the brain as macroscopic physical system operating on the scales (of time, space, temperature) which differ crucially from the corresponding quantum scales. But as alive organ it hold some temperature and is simply too hot to be able perform the real quantum information processing, and use the quantum carriers of information such as photons, ions, electrons. Neuron is by definition a morphological unit of central nervous system and the brain as well. From this perspective we can say that neuron presents also basic unit of information processing. Neuron couldn't be in the superposition of two states: firing and non-firing. Hence, it cannot produce superposition playing the basic role in the quantum information processing. Superpositions of mental states are created by complex neural networks of neurons. The activity of such neural networks can produce effects which are formally described as interference and entanglement (Khrennikov,2009).

The quantum cognition project is based on the observation that various cognitive phenomena are more adequately described by quantum information theory and quantum probability than by the corresponding classical theories.

At the moment we can say that there is no clearly defined neurophysiological mechanisms of creation of the quantum-like representation of information in the brain, but we can mention the hypothesis of matching the information processing in the brain with quantum information and probability with contextuality as the key word. Quantum systems do not have objective properties which can be defined independently of measurement context as contextuality implies existence of incompatible mental variables, violation of the classical law of total probability and interference effects, so we can summarize that quantum cognition approach can be considered as an attempt to formalize contextuality of mental processes by using the mathematical apparatus of quantum mechanics.

Consciousness and Quantum Brain

The quantum mind or quantum consciousness group of hypotheses propose that classical mechanics cannot explain consciousness. It posits that quantum mechanical phenomena, such as quantum entanglement and superposition, may play an important part in the brain's function and could form the basis of an explanation of consciousness (Yukalov, 2011; Allis, 1953).

If we want to discuss about the highest of all psychological functions, consciousness, let it define it first. The widest definition includes the state or quality of awareness the executive control system of the mind. Despite the difficulty in definition, many philosophers believe that there is a broadly shared underlying intuition about what consciousness is. As Max Velmans and Susan Schneider wrote in *The Blackwell Companion to Consciousness*: "Anything that we are aware of at a given moment forms part of our consciousness, making conscious experience at once the most familiar and most mysterious aspect of our lives.

Many philosophers tried to comprehend the nature of consciousness and identify its essential properties. Issues of concern in the philosophy of consciousness include whether the concept is fundamentally coherent; whether consciousness can ever be explained mechanistically; whether non-human consciousness exists and if so how can it be recognized; how consciousness relates to language; whether consciousness can be understood in a way that does not require a dualistic distinction between mental and physical states or properties; and whether it may ever be possible for computing machines like computers or robots to be conscious, a topic studied in the field of artificial intelligence (Allais, 1953; Ellsberg, 1961).

The base of the very well coordinated connection between the consciousness and brain physiological processes is seem to be separated in two very different kinds of processes.

Descartes and Pineal Gland

Descartes formulated the Cartesian dualism in which he proposed that consciousness resides within an immaterial domain he called the realm of thought, in contrast to the domain of material things, which he called the realm of extension. He suggested that the interaction between these two domains occurs inside the brain, perhaps in a small midline structure called the pineal gland.

Pineal gland is a midline, unpaired pine-cone shape brain structure. It is reddish-gray and about the size of a grain of rice (5–8 mm) in humans. The pineal gland, also called the pineal body, is part of the epithalamus, and lies between the laterally positioned thalamic bodies and behind the habenular commissure. It is located in the quadrigeminal cistern near to the corpora quadrigemina. It is also located behind the third ventricle and is bathed in cerebrospinal fluid supplied through a small pineal recess of the third ventricle which projects into the stalk of the gland.

Although it is widely accepted that Descartes considered the pineal gland as if it the heart of the soul and been supported by many philosophers of his age back than but no alternative solution has gained general acceptance. Proposed solutions can be divided broadly into two categories: dualist solutions that maintain Descartes' rigid distinction between the realm of consciousness and the realm of matter but give different answers for how the two realms relate to each other; and monist solutions that maintain that there is really only one realm of being, of which consciousness and matter are both aspects. Each of these categories itself contains numerous variants. The two main types of dualism are substance dualism (which holds that the mind is formed of a distinct type of substance not governed by the laws of physics) and property dualism (which holds that the laws of physics are universally valid but cannot be used to explain the mind). The three main types of monism are physicalism (which holds that the mind consists of matter organized in a particular way), idealism (which holds that only thought or experience truly exists, and matter is merely an illusion), and neutral monism (which holds that both mind and matter are aspects of a distinct essence that is itself identical to neither of them). There are also, however, a large number of idiosyncratic theories that cannot cleanly be assigned to any of these schools of thought (Machina, 2009).

A few theoretical physicists have argued that classical physics is intrinsically incapable of explaining the holistic aspects of consciousness, but that quantum theory may provide the missing ingredients. Several theorists have therefore proposed quantum mind (QM) theories of consciousness. Notable theories falling into this category include the holonomic brain theory of Karl Pribram and David Bohm, and the Orch-OR theory formulated by Stuart Hameroff and Roger Penrose. Some of these QM theories offer descriptions of phenomenal consciousness, as well as QM interpretations of access consciousness. None of the quantum mechanical theories has been confirmed by experiment. Recent publications by G. Guerreshi, J. Cia, S. Popescu, and H. Brieger could falsify proposals such as those of Hameroff, which rely on quantum entanglement in protein. At the present time many scientists and philosophers consider the arguments for an important role of quantum phenomena to be unconvincing.

Apart from the general question of the "hard problem" of consciousness, roughly speaking, the question of how mental experience arises from a physical basis, a more specialized question is how to square the subjective notion that we are in control of our decisions (at least in some small measure) with the customary view of causality that subsequent events are caused by prior events. The topic of free will is the philosophical and scientific examination of this conundrum.

Quantum Mechanics, Mind-Different Theories

The idea that quantum mechanics has something to do with the workings of the mind was proposed by Eugene Wigner who suggested that wave function collapses due to its interaction with consciousness. Freeman Dyson argued that "mind, as manifested by the capacity to make choices, is to some extent inherent in every electron."

Many scientists considered this option as improbable describing it as a myth with no scientific basis.

David Chalmers argued against quantum consciousness. He instead discussed how quantum mechanics may relate to dualistic consciousness. Chalmers is skeptical of the ability of any new physics to resolve the hard problem of consciousness.

The main argument against the quantum mind hypothesis was the assertion that quantum states in the brain would lose coherency before they reached a scale where they could be useful for neural processing, which was elaborated by Tegmark, who made calculation in which quantum systems in the brain

decohere at sub-picosecond timescales, which are considered to be too short to control brain function. If there is no brain-mind identity, mind-states could be in an abstract space that is not affected by decoherence (Khrennikov, 2008).

Quantum Cognition

Quantum cognition represents an innovative field which applies the mathematical formalism of quantum theory to model of cognitive phenomena such as information processing by the human brain, language, decision making, human memory, concepts and conceptual reasoning, human judgment, and perception. This field makes a great difference from the quantum mind as it is not reliant on the hypothesis that there is something micro-physical quantum mechanical about the brain as it is based on the quantum structure paradigm. The main mechanism or concept is based on a information processing by complex systems such as brain structures. It is hypothesised that contextual dependence of information and probabilistic reasoning could be mathematically described in the framework of quantum information and quantum probability theory.

Quantum theory is used to insert models of cognition that target to be more innovative than models based on traditional classical probability theory which includes cognitive modeling phenomena in science. Since the use of a quantum-theoretic framework is for modeling purposes, the identification of quantum structures in cognitive phenomena does not presuppose the existence of microscopic quantum processes in the human brain (Khrennikov, 2009).

Human Brain

Morphological substrate for the soul and all the psychological functions that applied refer to „inner me“ is generally referred to the brain with emphasis to specific brain structures that are parts of the telencephalon, their connections are correlations with other important structures inside the body. We can here try to describe the human brain from the neuroanatomical point, non metaphysical. The shape and size of the brain varies greatly between species, and identifying common features is often difficult, mostly the ones that are the most included in higher functions. There are a number of principles of brain architecture that apply across a wide range of species and some aspects of brain structure are common to almost the entire range of animal species (like rats).

The simplest way to gain information about brain anatomy is by visual inspection, where we can see the brain tissue in its natural state is too soft to work with, but it can be hardened by immersion in fixative, such as formaline. Visually, the interior of the brain consists of areas of so-called grey matter, with a dark color, separated by areas of white matter, with a lighter color. Inner microscopic description of the different brain structures and regions can be gained by staining followed by microscopic analysis, slices of brain tissue with a variety of chemicals that bring out areas where specific types of molecules are present in high concentrations. As a side effect of the electrochemical processes used by neurons for signaling, brain tissue generates electric fields when it is active. When large numbers of neurons show synchronized activity, the electric fields that they generate can be large enough to detect outside the skull (Van den Noort, 2016).

Many brain structures are involved in current investigation as a possible morphological substrates of consciousness, but the most examined are brain cortex, brainstem, diencephalon, amygdala and hippocampus.

These structures are also mentioned to be neuroanatomical markers involved in stress response and reaction both in acute and chronic state. However, stress can induce, if prolonged, chronic inflammation, or excitation state of the cell, and consequently volumetric changes as well.

We can observe the brain as macroscopic physical system operating on the scales (of time, space, temperature) which differ crucially from the corresponding quantum scales. But as a living organ it holds some temperature and is simply too hot to be able to perform the real quantum information processing, and use the quantum carriers of information such as photons, ions, electrons. Neuron is by definition a morphological unit of the central nervous system and the brain as well. From this perspective we can say that a neuron presents also a basic unit of information processing. A neuron couldn't be in the superposition of two states: firing and non-firing. Hence, it cannot produce superposition playing the basic role in the quantum information processing. Superpositions of mental states are created by complex neural networks of neurons. The activity of such neural networks can produce effects which are formally described as interference and entanglement. (Tversky, 1992)

The quantum cognition project is based on the observation that various cognitive phenomena are more adequately described by quantum information theory and quantum probability than by the corresponding classical theories.

At the moment we can say that there is no clearly defined neurophysiological mechanisms of creation of the quantum-like representation of information in the brain, but we can mention the hypothesis of matching the information processing in the brain with quantum information and probability with contextuality as the key word. Quantum systems do not have objective properties which can be defined independently of measurement context as contextuality implies existence of incompatible mental variables, violation of the classical law of total probability and interference effects, so we can summarize that the quantum cognition approach can be considered as an attempt to formalize contextuality of mental processes by using the mathematical apparatus of quantum mechanics.

Stress and Work

Work stress refers to the process of job stressors, or stimuli in the workplace, leading to strains, or negative responses or reactions. Organizational development refers to a process in which problems or opportunities in the work environment are identified, plans are made to remediate or capitalize on the stimuli, action is taken, and subsequently the results of the plans and actions are evaluated. When organizational development strategies are used to assess work stress in the workplace, the actions employed are various stress management interventions. Two key factors tying work stress and organizational development are the role of the person and the role of the environment. In order to cope with work-related stressors and manage strains, organizations must be able to identify and differentiate between factors in the environment that are potential sources of stressors and how individuals perceive those factors. Primary stress management interventions focus on preventing stressors from even presenting, such as by clearly articulating workers' roles and providing necessary resources for employees to perform their job. Secondary stress management interventions focus on a person's appraisal of job stressors as a threat or challenge, and the person's ability to cope with the stressors (presuming sufficient internal resources, such as a sense of meaningfulness in life, or external resources, such as social support from a supervisor). When coping is not successful, strains may develop. Tertiary stress management interventions attempt to remediate strains, by addressing the consequence itself (e.g., diabetes management) and/or the source of the strain (e.g., reducing workload). The person and/or the organization may be the targets of the intervention.

The ultimate goal of stress management interventions is to minimize problems in the work environment, intensify aspects of the work environment that create a sense of a quality work context, enable people to cope with stressors that might arise, and provide tools for employees and organizations to manage strains that might develop despite all best efforts to create a healthy workplace (Machina, 2009).

Why Quantum Cognition?

Rational models of cognition adhere to the laws of classical probability theories, although human thinking and decision making does not conform these laws. Quantum models present cognitive phenomena with proven recalcitrant with means of classical probability theory. This is all Referred to classical probability theory, Kolmogorov theory on which Bayesian model rests and it says that the Bayes rule is a simple theorem that follows from the classical probability definition of conditional probability. Suppose $\{H_1, \dots, H_N\}$ is a set of hypotheses that you wish to evaluate, and D represents some data that provide evidence for or against each hypothesis. Then according to the definition of conditional probability, $p(H_i|D) = p(H_i \cap D)/p(D)$. Bayes rule uses the classical definition of joint probability to rewrite the numerator on the right hand of the equation: $p(H_i \cap D) = p(H_i)p(D|H_i)$; and the Bayes rule uses the law of total probability to rewrite the denominator: $p(D) = \sum_j p(H_j)p(D|H_j)$. Bayesian models of cognition use these rules to construct models that predict how people make complex inferences from a set of observations. Why use quantum probability theory? After all, the prevalence of the Bayesian models is testament to the success of classical probability theory in modeling cognition. Despite this success, however, there has been a steady accumulation of puzzling, even paradoxical, cognitive phenomena that violate the axioms upon which classical probability theory (and hence Bayesian inference) is based. Thus far, these violations have been explained using heuristic rules such as the representativeness heuristic and the anchoring-and-adjustment heuristic. Rather than resorting to heuristics, quantum cognition successfully accounts for these violations using a coherent, common set of principles. Although this review focuses on judgment and decision making, we briefly highlight the expressive power of quantum models by pointing out that they have already been applied to a broad range of cognitive phenomena, including perception, memory, conceptual combinations, attitudes, probability judgments, causal reasoning, decision making, and strategic games. It is not possible to survey the myriad of applications in this review. We will restrict our attention to a representative set of examples which intuitively illustrate the basic quantum principles introduced previously. Quantum cognition also raises many new questions for cognitive scientists and psychologists to address. One is about rationality. Classical probability theory may provide an upper bound that achieves optimal performance irrespective of computational costs and resource limitations. Quantum models may provide a more realistic bound that performs close to optimal but with fewer computational demands. Consider, for example, a strategic game involving yourself and $n - 1$ other players, and each player can choose one of K actions. If human cognition directly implements classical probability theory (i.e., it treats all events as compatible), then K^n joint probabilities are required to represent your beliefs regarding the actions that could be taken by yourself and the other $n - 1$ players, producing an exponential growth in dimensionality. If instead, human cognition applies a new incompatible perspective to each player, then all of the required probabilities can be assigned by using a single state vector that is evaluated with respect to different bases within a fixed K -dimensional space (Caves, 2002).

CONCLUSION

Using limited cognitive resources, incompatibility provides humans the means for answering an unlimited number of questions, thus promoting parsimony and cognitive economy. However, the use of incompatibility comes at the cost of introducing non-commutativity and sequential effects. Our view is that incompatibility of events provides an effective solution to bounded resources, which is the reason for bounded rationality.

REFERENCES

- Allais, M. (1953). Le comportement de l'homme rationnel devant le risque: Critique des postulats et axiomes de l'école Américaine. *Econometrica*, 21(4), 503–546. doi:10.2307/1907921
- Caves, C. M., Fuchs, C. A., & Schack, R. (2002). Quantum probabilities as Bayesian probabilities. *Physical Review A*, 65(2), 022305. doi:10.1103/PhysRevA.65.022305
- Dyson, F. (2004). *Infinite in All Directions: Gifford Lectures Given at Aberdeen, Scotland April--November 1985*. New York: Perennial.
- Ellsberg, D. (1961). Risk, ambiguity, and the Savage axioms. *The Quarterly Journal of Economics*, 75(4), 643–669. doi:10.2307/1884324
- Khrennikov, A. (2008). The Quantum-Like Brain on the Cognitive and Subcognitive Time Scales. *Journal of Consciousness Studies*, 15(7).
- Khrennikov, A. (2009). *Contextual Approach to Quantum Formalism (Fundamental Theories of Physics 160)*. Springer. doi:10.1007/978-1-4020-9593-1
- Machina, M. J. (2009). Risk, ambiguity, and the dark-dependence axioms. *American Economical Review*, 99(1), 385–392. doi:10.1257/aer.99.1.385
- Pothos, E. M., & Busemeyer, J. R. (2009). A quantum probability explanation for violations of 'rational' decision theory. *Proceedings of the Royal Society B: Biological Sciences*, 276(1665), 2171–2178.
- Quantum Approaches to Consciousness. (2011). In *Stanford Encyclopedia of Philosophy*. Stanford University Press.
- Savage, L. J. (1954). *The Foundations of Statistics*. John Wiley & Sons.
- Tversky, A., & Shafir, E. (1992). The disjunction effect in choice under uncertainty. *Psychological Science*, 3(5), 305–309. doi:10.1111/j.1467-9280.1992.tb00678.x

Quantum Cognition and Its Influence on Decrease of Global Stress Level Related With Job Improvement

Van den Noort, M., Lim, S., & Bosch, P. (2016). On the need to unify neuroscience and physics. *Neuroimmunology and Neuroinflammation*, 3(12), 271–273. doi:10.20517/2347-8659.2016.55

Yukalov, V. I., & Sornette, D. (2011). Decision theory with prospect interference and entanglement. *Theory and Decision*, 70(3), 283–328. doi:10.1007/11238-010-9202-y

This research was previously published in Chronic Stress and Its Effect on Brain Structure and Connectivity; pages 155-167, copyright year 2019 by Medical Information Science Reference (an imprint of IGI Global).

Chapter 18

Complex Action Methodology for Enterprise Systems (CAMES): A System to Contextualize the Behavioral Management Issue as Quantum Mechanical Variable

Olaf Cames

 <https://orcid.org/0000-0002-3924-311X>

University of Liverpool, UK

Meghann L. Drury-Grogan

Fordham University, USA

ABSTRACT

This completed action research utilizes the conceptual framework of quantum mechanics in action science field studies for bias-free behavioral data collection and quantification. The research question tied to experimental verification if action research field studies can practically utilize the theory of communicative action and the theory of quantum mechanics to contextualize the quantification with pathological and distorted behavioral pattern. The result is a quantum-like formalism that provides intermediary conceptuality for organizational intervening initiatives. This process of contextualization behavior in projects via quantum probability experimentally evidenced. The chapter concludes by reviewing the results of two experiments that the hypotheses that the theory of quantum mechanics and the theory of communicative action qualifies as a building block for a planned methodological approach to intervene and steer problematic social structures in the desired direction.

DOI: 10.4018/978-1-7998-8593-1.ch018

INTRODUCTION

For more than two decades, practitioner studies have shown most Information Technology (IT) projects are not prosperous and state behavioural patterns as decisive factors for success or non-success. The IT practice lacks procedures to determine and predict project and organisational member behaviour with certainty.

Current action research methodologies bias observations severely and render quantification models of subjective data uncertain. Thus, this research thesis aims to design a scientifically rigorous action-science methodology process that is operational for action researchers and practitioners to lower the rate of non-successful IT projects where failure is attributable to human behaviour in organisational contexts. This investigation aims to apply scientific rigour to this issue and to verify the general applicability of mathematical formalism of quantum mechanics to address organisational venture that includes a wicked problem of how to communicate and collaborate appropriately. The subjective data collection and quantification models of this thesis build on the quantitative formalism of quantum mechanics and qualitative formalism of the theory of communicative action. Mathematical and ontological formalism combine into a novel research strategy with planned instrumentation for action research field studies summarised under the term ‘Complex Action Methodology for Enterprise Systems’ (CAMES). The outcome is a process to understand the behavioural action of project participants better. The process requires that participants act under a new identity, a virtual identity. Data collection occurs in one block with an average duration time of 10 minutes in a virtual location. The practice can, therefore, use these procedures for bias-free quantification of subjective data and prediction of an individual’s future behaviour with certainty. Prediction of an individual’s future behaviour with certainty provides to the IT practice what IT practice lacks but urgently requires. The certainty that claimed findings of behaviour in projects and organisational context requires to intervene and steer. Certainty and justification for planned intervening and steering initiatives secure funding.

Lack of Bias-Free Collection and Quantification of Subjective Data in Data Sciences

Conventional social sciences research methodologies bias observations and render quantification models of subjective data uncertain. Researcher bias on observations is severe and reason to dismiss classical quantification models. Influenced by the researcher and interaction of measuring research instrumentation on the observed result in methodological flaws, false measures and incomplete interpretation of data. Biased research renders observations unreliable and invalidates data gathered from such biased observations. Collecting and quantifying the interaction occurring by and through biased individuals is considered unsolvable. Behavioural inner dynamics of biased individuals for steering and intervening purposes is not measured. Prediction failures deepen the gap between theory and practice (Kieser & Leiner, 2009). Management science mainstream, traditional understanding to explain behaviour lead to severe deficiencies for its claimed findings. Direct influences from scientists on the observed or researcher contamination of environmental factors in research setup result in biased measurements and render the observed useless for bias-free quantification of subjective data and prediction of an individual’s future behaviour. To bias-free collect subjective data, the principles of quantification of subjective data and the researcher’s analytical procedures require a research strategy with upfront planned instrumentation.

Quantum Mechanical and Ontological Formalism for Bias-Free Collection and Quantification of Subjective Data in Social and Data Sciences

CAMES subjective data collection and quantification models build on the quantitative formalism of quantum mechanics and qualitative formalism of the theory of communicative action. Mathematical and ontological formalism combine into a novel research strategy with planned instrumentation for action research field studies summarised under the term ‘Complex Action Methodology for Enterprise Systems’ (CAMES).

General Principles for Bias-Free Research Strategies

A practical research design combining bias-free quantitative instrumentation with qualitative reviews is practical. Researcher utilising validated instruments on observations produce meaningful findings (Miles, Huberman & Saldana, 2014). Instrumentation that either measure or reduce or avoid biasing effects are validated instruments. Qualifying research instrumentation as bias-free research instrumentation requires validation procedures for the quantitative instrumentation deployed.

General Principles for Quantification of Subjective Data

The unifying interdisciplinary schema for quantification of subjective data is the interference pattern. The interference pattern proved successful to explain data in research aimed to understand behavioural paradoxes. Novel analytical routines and corresponding formal logic had been successfully applied to explain observed human behavioural reasoning phenomena not entirely explainable with traditional concepts (Busemeyer et al. 2009; Wang et al., 2018a). The interference effect is defined in quantum theory as measurable and predictable and is expected to be there, naturally occurring. The presence of interference indicates quantum behaviour. Measured interference represents a healthy, standard, natural emerging and measurable condition (Von Neumann, 1933). The disappearance of interference indicates loss of fully exposed quantum behaviour (Aerts, Broekaert & Smets, 1999).

Interference defines as noise and disturbance in conventional theories. Interference violates conventional theories basic assumptions and renders methodologies based on such conventional theories useless for further investigation of interferences (Conte et al., 2007).

Explanations for data resulting in better understanding of human behaviour by utilising interference pattern render other methods treating the interference phenomena as noise and annoying factor less appropriate for further consideration. A satisfactory explanation by using the conceptual framework of the theory of quantum mechanics is direct evidence for the flaws in the theory of total probability. Conservative, mainstream methodologies for an explanation of human behaviour base on the flawed theory of the law of total probability and apply methodologies based on the flawed assumption, e.g. all Markov property-based methodologies (Wang & Busemeyer, 2013; Wang et al., 2018a).

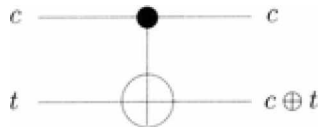
Measures and predictive analytics applying the conventional framework of quantum mechanics explain complete human behavioural phenomena (Aerts & de Bianchi, 2015). Clinical, experimental research inform about comparison studies applying both theories that resulted in better understanding for human behavioural phenomena like conceptual combination (Aerts, 2009), perception (Atmanspacher, et al., 2004; Conte et al., 2009), judgments (Khrennikov, 1999), disjunction effect (Busemeyer & Bruza, 2012), conjunction fallacy (Yukalov & Sornette, 2011; Busemeyer, Matthew & Wang, 2006; Franco, 2007;

Complex Action Methodology for Enterprise Systems (CAMES)

The procedure is designed to permit interaction and evolution between the target of evaluation and its environment as ongoing.

Ongoing observation of project and organisational member communicative actions focus on state changes. Evolution operators compare previous and actual user communicative actions. Measurement occurs on models of mirrored superposition of data collected rather than on superposition and data collected itself. Mathematical procedures target logical operations on the mirrored superposition of superposition (Marsh & Briggs, 2009). Operating on mirror avoids the direct interaction of a measuring apparatus with the observed (Figure 1).

Table 1. CAMES notation

CAMES Notation (Non-Linear Orthography Logograms (CNLOL))		
1	TI	Targeted Identity
2	VI	Virtual Identity
3	tix	Observed components
4	${}^t iy$	Observed components
5	vix	Superposition components
6	tix2	Additional environmental input
7	vix2	“AND” of TI observables
8	t2x0	Targeted Identity copied, observed component
9	t2x2	Targeted Identity additional copied, observed component
10	TI_r	Repository of environmental observed
11	v2x0	Copy of TI_{2x0}
12	v2x1	Copy of TI_{2x1}
13	VI_2	${}^t2x0, {}^t2x1, {}^t2x2$ repository Copy of TI
14	${}^A1 \leftarrow {}^v2$	Augmented Identity
15	IN	Instances of Quantum Algorithms
16	QN	Nullifiable results of quantum operations
17	CN	CNOT gate. The data representation of VI cognitive dissonance.
		 <p>Logogram visualisation of cognitive dissonance in mathematical formalism of the theory of quantum mechanics.</p>
18	IN-1	Reversible gate
19	QBIRAn	Quantum reversible algorithm
20	QBIDTP	Quantum data transformation injection point
21	adnTI	Attitudes, desires, needs (behavioural action preferences)
22	TIspace	Shared variable. Hosts all observed mental vectors and mental states
23	TIV	Mental vector
24	VIV	Mental vector

continues on following page

Table 1. Continued

CAMES Notation (Non-Linear Orthography Logograms (CNLOL))		
25	TIST	Mental state
26	qbiXY	qubit (pure state)
27	QRA1	Coding of companion TI, or VI or TIX/TIY influence on TI
28	QRA2	Additional Virtual Identity in- fluence freeze/defreeze procedures - preservation of time reversibility – anytime ad hoc previous TI state calculations from current VI state prediction analytics
29	QRA3	Acquire the original experimental environment observables from practitioner usage scenario participant (TI, Tlx, Tly) again at any given time from VI2 predictive analytics operations
30	AI	Augmented Intelligence / Artificial Intelligence
31	FMn	Formation of “vicious circles of mediocrity” Masuch, 1985, p. 28)
32	IAn	Initial amplitudes Preferences for actions.
33	TIEO	Time-indexed evolution operator
34	FPT	Focused predictive task
35	DM	Dynamic momentum. Cognitive dissonance.
36	GIF	General Interference Detection
37	DS	Dominating mindset
38	CV	2-argument research question
39	CV	Context variable
39	KPI	Meaningful measure. Key performance indicator. Magnitude baseline.
39	Prb	Predicted behaviour

Organisational and Project Interaction Data Encoding/Decoding

Work context interaction, organisational, and real-world project communication and typical, critical usage scenarios are subject of researcher’s notation encoding and decoding the observables. A defined listing of characters, numbers, symbols, punctuation, and letters sequence into a specific format ensures efficient co-negotiation between academics and practitioner (Table 1). Establishing a common language between academic driven further theoretical development and practice usability verification is vital to the translate the complexity and subtlety of ideas into evidence-based management in a particular work context (Rousseau, 2006). Encoding ensures project and organisational member interaction data persists. Decoding ensures project and organisational member interaction data retrieval between co-negotiation transmissions between an academic researcher and project practitioner. Those agreed notations obfuscate the complexity of the mathematical-logical procedures and eliminate the necessity for the project and organisational management to communicate in mathematical terminology (Table 1).

Transform Mathematical Complexity Into Ontological Simplicity

CAMES notation transforms the complexity of 4- dimensional Hilbert space state expressions into ontological state simplifications. Interventionists receive shorthand notation to apply quantum-like formalism into intermediary conceptuality (Aerts, Broekaert & Smets, 1999).

Complex Action Methodology for Enterprise Systems (CAMES)

CAMES formal notation is a diagnostic framework in which communicative pathologies identify, localise, diagnose, and therapize. Formal normative notation reveal techniques to empirically evidence distorted communication patterns. Such human behavioural phenomena are subject of already existing and scientifically proven quantum-like quantitative procedures like behavioural anomaly detection in conceptual combination (Aerts, 2009), illusionary effects in human perception (Atmanspacher, et al., 2004), disjunction effect (Busemeyer & Bruza, 2012), affinities to fall for conjunction fallacies (Yukalov & Sornette, 2011; Busemeyer, Matthew & Wang, 2006; Franco, 2007; Khrennikov, 2008), biasing judgments (Khrennikov, 1999), and truth irritations by liar paradoxes (Aerts, Broekaert & Smets, 1999).

Empirical data for behavioural anomaly detection apply as values to non-local variables by observing interactions in context. As CAMES notations are universally applicable across different action contexts, non-local validity for its findings is the logical consequence. In this sense, CAMES notations are universal (Habermas, 2002). Applying formalities of CAMES notation leads therefore to the identification of universal conditions. Those conditions are communicative pathological explanations.

Universal applicability is claimed by quantum mechanics as well. Quantum cognitive sciences claim universal applicability because of mathematical procedures capable of projecting all possibilities with certainty into and out of naturally occurring Hilbert space and interference phenomena (Aerts & de Bianchi, 2014; Aerts & de Bianchi, 2015).

Applying CAMES notations in conjunction with quantitative measures, therefore, results in new behavioural pathologies and re-interpretation of behavioural pathologies that had previously identified, localised, diagnosed and therapized (Lawless & Schwartz, 2002; Rich & Craig, 2012). Those results can only materialise if universal explanations and re-interpretation apply to a context.

Prediction of an Individual's Future Behaviour With Certainty

Equations and Procedure

For simplicity of illustration, the figures are limited to illustrate equations using the Dirac notation because of its notational minimalism (Miller, Resnick & Zeckhauser, 2005). Dirac notation is a useful, effective alternative to conventional mathematical notation. It is the standard notation in quantum mechanics. Every organisational member participant receives a new identity. This new identity is virtual identity. The virtual identity establishes anonymity and confidentiality. Virtual participation provides contextualised disruption of the status quo (Gioia & Chittipeddi, 1991). Anonymity, confidentiality and contextualised disruption of the status quo is therefore at the disposition of the action researcher's experimental setup.

The sample equation depicts a participant who received virtual identity Surrogate252@action-science2.org and his observed mental vectors and mental states variables (Figure 2; Figure 3).

Virtual identity resets prior internalised roles and influences to the level of influenced external elements set by the by the uncontaminated research setup (Figure 1).

Figure 2. Observed mental vectors and mental state variables

$$T_{\text{space1}} T_{\text{st}}(T_{\text{I}}(V_{\text{v}}(\text{Surrogate252@action-science2.org}))) = \{ |G,D\rangle, |G,F\rangle, |B,D\rangle, |B,F\rangle \}$$

Figure 3. Amplitude reset to zero at the initial start of an experimental observation

$$\begin{aligned}
 & (ia_{GD}(0), ia_{GF}(0), ia_{BD}(0), ia_{BF}(0)) \doteq (|IA_I|^2 = 1) \\
 & (ia_{GD}(0), ia_{GF}(0), ia_{BD}(0), ia_{BF}(0)) \doteq (|IA_I|^2 = 1) \\
 & (ia_{GD}(0), ia_{GF}(0), ia_{BD}(0), ia_{BF}(0)) \doteq (|IA_I|^2 = 1) \\
 & (ia_{GD}(0), ia_{GF}(0), ia_{BD}(0), ia_{BF}(0)) \doteq (|IA_I|^2 = 1)
 \end{aligned}$$

Attitudes, perceptions, inner thoughts, perspectives and emotion formulate according to implications and directions set by the researcher (Koles & Nagy, 2012; Paniaras, 1997). Each row of IAI (Figure 1; Figure 3) provides the reset of measures to zero for one of the states in TIspace1TIsT(TI(VIv(Surrogate252@action-science2.org)) (Figure 2).

Context Variables

A questionnaire asks the same question in a different context. Three questions obtain a particular individual's preferences and intentions to behave and act. The first question obtains values for two mental vectors. The second question obtains additional values for two other mental vectors. The third question obtains additional values to predict future behaviour by spin theory (Pauli, 1940).

Judgement 1

Every participant is forced into conflict. The conflict forces the participant to decide on one of two possible arguments.

This decision is a judgement on how to act and behave. Question 1 enforces judgement 1.

Figure 4. Judgment 1: Truth values for the research question (sample instance)

$$TIspace_1TIsT(TI(VIv(Surrogate252@action-science2.org))) \doteq \{|G,D\rangle, |G,F\rangle, |B,D\rangle, |B,F\rangle\}$$

This judgement (Figure 4) delivers observable truth values for the research question into a vector (VIv) of Hilbert spaces (TIspace1) (Figure 1) for good (G), bad (B), defensive (D) and friendly (F) (Townsend et al., 2000; Busemeyer, Wang & Lambert-Mogiliansky, 2009). In case the 0- hypothesis confirms, ranked values are obsolete. Truth logic of research questions enter as shared variables and transform into projectors (Figure 5 and Figure 6).

Figure 5. Judgment 1: Initial amplitude distribution for the research question hypothesis $|A_I| = |A_G|$

$$(ia_{GD}(1), ia_{GF}(1), ia_{BD}(0), ia_{BF}(0)) \doteq (|A_I|^2 = 1) \doteq |ia_{GD}|^2 + |ia_{GF}|^2 = 1$$

Figure 6. Judgment 1: Initial amplitude distribution for the research question 0-hypothesis $|A_I| = |A_B|$

$$(ia_{GD}(0), ia_{GF}(0), ia_{BD}(1), ia_{BF}(1)) \doteq (|A_I|^2 = 1) \doteq |ia_{BD}|^2 + |ia_{BF}|^2 = 1$$

Judgement 2

Every participant is forced into a new conflict. The conflict forces the participant to decide on one of two possible arguments. This decision is a judgement on how to act and behave. Question 2 enforces judgement 2.

Figure 7. Judgment 2: Truth values for the research questions (typified)

$$Tl_{space_1} Tl_{st}(Tl(VI_v(Surrogate252@action-science2.org))) = \{|G,D\rangle, |G,F\rangle, |B,D\rangle, |B,F\rangle\}$$

This judgement delivers additional observable truth values for another, different research question into another vector (VI_v) of modified state (Tl_{st}) in augmented Hilbert space (Tl_{space_1}) (Figure 7). In case the 0-hypothesis confirms, ranked values are obsolete.

Judgement 3

Every participant is forced into a new conflict. The conflict forces the participant to decide on five possible arguments. This decision is a judgement on how to act and behave. Question 3 enforces judgement 3. Truth logic of research questions enter as shared variables and transform into projectors (Figure 8). Judgement 3 superposes between states in judgement 1 (Figure 9).

Figure 8. Judgment 3: Initial amplitude distribution for intentions to act and behave

$$|A_I| = (ia_G \cdot |A_G| + ia_B \cdot |A_B|)$$

Figure 9. Judgment 1 states

$$|ia_G|^2 + |ia_B|^2 = 1$$

Result: General Interference Detection (GIF)

In judgement 3 the context variable is superposed between states in judgement 1 (Figure 9). The context variable represents an individual that is superposed between possibilities to act and behave (Busemeyer & Bruza, 2012). This decision conflict is measurable as interference (Wang et al., 2018a; 2018b). The Interference pattern applies (Aerts & de Bianchi, (2015).

The theory of quantum mechanics measures interference as a naturally occurring mathematical and physical phenomena. This methodology applies measures to test for the presence or absence of interference phenomena in observed behaviours in projects and organisational context (Aerts, Broekaert & Smets, 1999; Wang et al., 2018a).

The presence of interference at the time participants responded to research questions obtains two verifications. First, the certainty that fully quantum behaviour is observed (Sasaki & Carlini, 2002; Aerts, Broekaert & Smets, 1999; Busemeyer & Bruza, 2012). Second, the certainty that research instrumentation did not interact leading to biasing interferences on the naturally occurring phenomena (Wang et al., 2018). Both measures provide certainty that applying quantum models predicting the probability of behaviour lead to practical outcomes.

This methodology transforms an empirical case of field study observed behaviours in projects into multiple-valued two-argument logical observables in TIspace1 (Figure 1) (Tarlac & Pregnolato, 2016; Vaas, 2001a; Bruza, Widdows & Woods, 2006; Chadha et al., 2009; Cattaneo et al., 2009; Cignoli, d’Ottaviano & Mundici, 2013; Dubois & Toffano, 2016). Predictions derived from the quantum model generate intentions to act and behave for this individual, and the group made up of such individuals (Yukalov & Sornette, 2011; Ashtiani & Azgomi, 2016; Fuller, 2018; Wendt, 2015).

Judgement 2

Judging discrepancy measures per experiment participant per judgement. If variances are high, then context variables are of known truth, validity and utility. The larger the variance for judgement 2, the more significant the discrepancy between judgement 1 and judgement 2.

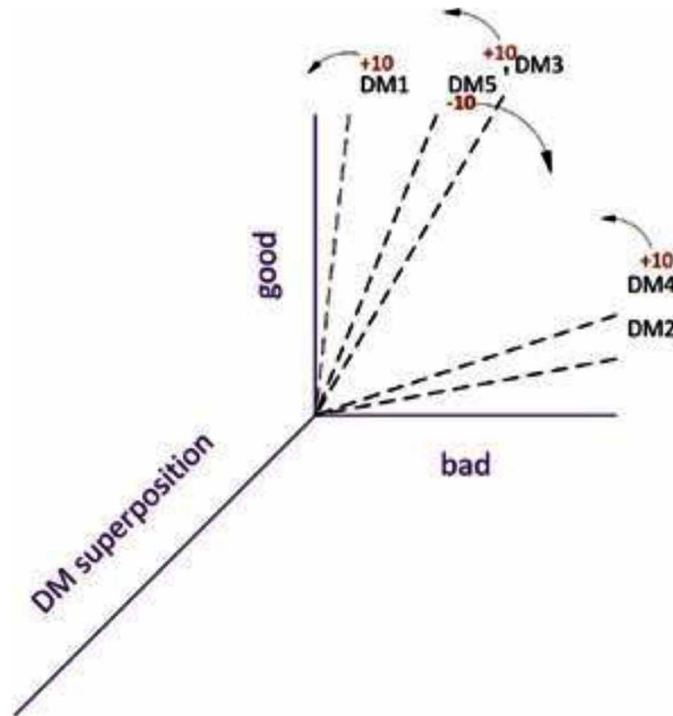
Judgement 3

Weighting expresses the degree of variance between decision making in question 1 and decision making in question 3. Weights are 0, 1, 3, 4, and 5. The smallest weight is 0, and 4 is the most substantial weight. A variance weighted as 0 represents no variance. A variance weighted as 4 represents the most substantial variance. The larger the variance for judgement 3, the more significant the discrepancy between judgement 1 and judgement 3.

Applying Interference Pattern

In case of GIF measure confirms the observation of fully quantum behaviour, literature researched pattern of interference effects in human behaviour apply (Sasaki & Carlini, 2002; Behrman et al., 2006). In the case of GIF, measure disconfirm observation of a fully quantum behaviour pattern of interference effects in human behaviour do not apply.

Figure 10. Quantum model prediction of post-questionnaire behavior (sample instance)



DISCUSSION

Project management applies false assumption that human behaviour is predictable by applying standard common sense and standard probability logic in conjunction with the lack of action research bias-free subjective data collection and quantification methodologies (Jaafari, 2004; Williams, 2002). Human affinity to disregard standard probability logic requires to switch to another probability logic.

CONCLUSION AND FUTURE WORK

Future research must substitute simple patterns for desired or undesired behaviour in projects with complex behavioural patterns, a.k.a. As organisational sciences power law (Wang & von Tunzelmann, 2000). Future research explores augmented intelligence tools to substitute failing humans as project manager.

The next step is to move on from the mathematical-analytical singletons of action science and action research into practical, mass scale execution on quantum computer.

REFERENCES

- Aerts, D. (2009). Quantum structure in cognition. *Journal of Mathematical Psychology*, *53*(5), 314–348. doi:10.1016/j.jmp.2009.04.005
- Aerts, D., Broekaert, J., & Smets, S. (1999). The Liar-paradox in a Quantum Mechanical Perspective. *Foundations of Science*, *4*(2), 115–132. doi:10.1023/A:1009610326206
- Aerts, D., & de Bianchi, M. (2014). The extended Bloch representation of quantum mechanics and the hidden-measurement solution to the measurement problem. *Annals of Physics*, *351*, 975–1025. doi:10.1016/j.aop.2014.09.020
- Atmanspacher, H., Filk, T., & Römer, H. (2004). Quantum Zeno features of bistable perception. *Biological Cybernetics*, *90*(1), 33–40. doi:10.1007/00422-003-0436-4 PMID:14762722
- Bruza, P., Kitto, K., Nelson, D., & McEvoy, C. (2009). Is there something quantum-like about the human mental lexicon? *Journal of Mathematical Psychology*, *53*, 362–377. doi:10.1016/j.jmp.2009.04.00
- Busemeyer, J., & Bruza, P. (2012). *Quantum Models of Cognition and Decision*. Cambridge University Press. doi:10.1017/CBO9780511997716
- Busemeyer, J., Matthew, M., & Wang, Z. (2006). A quantum information processing theory explanation of disjunction effects. In R. Sun & N. Miyake (Eds.), *Proceedings of 28th annual conference of the cognitive science society & the 5th international conference of cognitive science* (pp. 131–135). Academic Press.
- Busemeyer, J., Wang, Z., & Lambert-Mogiliansky, A. (2009). Empirical comparison of markov and quantum models of decision making. *Journal of Mathematical Psychology*, *53*(5), 423 – 433. doi: .2009.03.002 doi:10.1016/j.jmp
- Conte, E., Todarello, O., Federici, A., Vitiello, F., Lopane, M., Khrennikov, A., & Zbilut, J. P. (2007). Some remarks on an experiment suggesting quantum-like behavior of cognitive entities and formulation of an abstract quantum mechanical formalism to describe cognitive entity and its dynamics. *Chaos, Solitons, and Fractals*, *31*(5), 1076–1088. doi:10.1016/j.chaos.2005.09.061
- Franco, R. (2007). *Quantum mechanics, Bayes' theorem and the conjunction fallacy*. arXiv preprint quant-ph/0703222
- Khrennikov, A. (1999). Classical and quantum mechanics on information spaces with applications to cognitive, psychological, social, and anomalous phenomena. *Foundations of Physics*, *29*(7), 1065–1098. doi:10.1023/A:1018885632116
- Khrennikov, A. (2008). Bell-Boole inequality: Nonlocality or probabilistic incompatibility of random variables? *Entropy (Basel, Switzerland)*, *10*(2).

Complex Action Methodology for Enterprise Systems (CAMES)

Marsh, S., & Briggs, P. (2009). Examining trust, forgiveness and regret as computational concepts. In *Computing with social trust* (pp. 9–43). London: Springer.

Masuch, M. (1985). Vicious Circles in Organizations. *Administrative Science Quarterly*, 30(1), 14-33.

Von Neumann, J. (1933). Mathematische Grundlagen der Quantenmechanik. *Monatshefte Für Mathematik*, 40(1), A31.

Wang, B., Song, D., Wang, B., Zhang, P., Li, J., Song, D., & Shang, Z. (2018a). Exploration of Quantum Interference in Document Relevance Judgement Discrepancy. *Entropy (Basel, Switzerland)*, 18(4), 144. doi:10.3390/e18040144

Wang, Z., & Busemeyer, J. (2013). A Quantum Question Order Model Supported by Empirical Tests of an A Priori and Precise Prediction. *Topics in Cognitive Science*, 5(4), 689–710. doi:10.1111/tops.12040 PMID:24027203

Yukalov, V., & Sornette, D. (2011). Decision Theory with Prospect Interference and Entanglement. *Theory And Decision: An International Journal For Methods And Models In The Social And Decision. The Sciences*, 70(3), 283–328.

This research was previously published in the Handbook of Research on Strategic Communication, Leadership, and Conflict Management in Modern Organizations; pages 302-314, copyright year 2019 by Business Science Reference (an imprint of IGI Global).

Chapter 19

Multi-Process Analysis and Portfolio Optimization Based on Quantum Mechanics (QM) Under Risk Management in ASEAN Exchanges: A Case Study of Answering to the E-Commerce and E-Business Direction

Chukiat Chaiboonsri

Chiang Mai University, Thailand

Satawat Wannapan

Chiang Mai University, Thailand

ABSTRACT

This research attempts to classify, predict, and manage the financial time-series trends of the large stock prices of significant companies in the development of e-commerce and e-business in the ASEAN countries. Moreover, the Markowitz portfolio optimization analysis based on quantum mechanics was utilized to find out the direction of e-commerce and e-business in the future. Data collection for this study consists of Maybank, PPB Group Berhad, Golden Agri-Resource, SingTel, and Global Logistic Properties. And the stock prices of those companies were carried out to this study from 2004 to 2018 by daily data. Interestingly, the empirical results would provide a possible solution and efficiently suggest a beneficial for the development of both e-commerce and e-business in the ASEAN countries. The commerce and business based on electronics in ASEAN, especially agribusiness, energy business, and telecommunication business, still play a major important role in the economy of ASEAN countries.

DOI: 10.4018/978-1-7998-8593-1.ch019

INTRODUCTION

Financial time series can continuously have attentions from economists and statistical researchers. Obviously, this type of data is extremely difficult to precisely predict since its frequently daily updates and velocities of data fluctuations. Additionally, financial forecasting will become more complex and elusive when they have been trying to solve the estimated answer by initially assuming the normal distribution is fitted for this calculation. Results will be suspicious when only single method is employed to do econometrical predictions. Consequently, multi-analytic estimations are definitely suitable for financial issues, which are dynamically depended on time variations.

Generally, some interesting points that should be considerably focused are data classifications, data estimations, and data managements. Since it is inevitable that information is uncertainty, meaning there are error terms inside every time-series trends, this is why the classification process should be helpfully employed. For example, unit-root testing, regimes switching, and entropy analyses. For econometric forecasting, it is undeniable that linear calculations cannot be appropriated for financial data. This is the reason why data estimations such as non-linear simulations and structural analyses should be applied. For the section of data managements, this process is the tool that usefully explains the econometrical results to be more substantial for policy implementations. Hence, it is practical that multi-analytic processes are recently becoming crucial for financial econometric researches.

This research is to brightly clarify the mixed up tool regarding mathematics, statistics, and modern physics (Quantum mechanics). These are adopted to analyze data in capital markets or stock exchange markets which are the crucial part of economic systems. Deeply considering into the systems, business and economics, it is very well-known that E-commercial activities for online businesses are becoming a very important market and they are rapidly grown as numerical details in ASEAN economic development countries. Moreover, ASEAN continent is an emerging internet market in the world by increasing new users approximately 125,000 amateur and skilled users per day every day. Consequently, the digital economy of ASEAN shall be more significant to develop the ASEAN economy by predicting approximately \$1 trillion contributions to GDP in ASEAN member countries. This vast expansion shall be the possible financial catastrophe, if estimated predictive results suggest wrong scenarios.

The purpose of this research is to econometrically compute the multi-analytic methods to fulfill the research question that who is the player of E-commerce and E-business in ASEAN countries by observing from the log return of those stock prices. The daily stock prices of the five predominant companies were collected from ASEAN stock exchanges during 23rd April 2014 to 22nd May 2018 (994 daily samples). These significant companies are MayBank, referring to Indonesian financial index which are representative the substantial company in the financial field. The PPB GROUP BERHAD is presented as the company covering energy and agribusiness sectors in Malaysia. Golden Agri-Resource is the index representing the company producing food, beverage and agribusiness in Singapore. SingTel is the substantial company playing the role of the telecommunication sector in Singapore. Global Logistic Properties stands for the business builder in the logistics sector and real estate sector. Headquarter is located in Singapore. All selected companies are major to develop E-Commerce and E-Business in ASEAN countries.

BACKGROUND

Interestingly, the research purpose aims to solve the question is that who is an important player in E-commerce and E-business in ASEAN countries. By observing from the modified log-returns of those stock prices during 2014 to 2018, the companies in ASEAN were chosen to be good examples for this study. For financial sector, the company, Maybank, plays an important role in the financial sector in Malaysia. The company is implied as a Malaysian universal bank, with key operating “home markets” of Malaysia. Additionally, the network is internationally located in the major countries in ASEAN. The electronic business activities are the crucial role for the company since the 2018 Brand Finance Banking 500 Brand Value Report issued by global brand valuation and strategy consulting firm.

Considering into the section of food and beverage, the company, PPB Group Berhad, is a Malaysian diversified corporation which assembles in food production, agriculture, waste management, etc. The company was founded in 1968 as Perlis Plantations Berhad (from which it derives the name of the company in the moment) by Robert Kuok to cultivate and mill sugar cane in the northern Malaysian state of Perlis. The main business is the supply of flour to downstream food producers. Because of the company has over 500 manufacturing plants and an extensive distribution network covering China, India, Indonesia and some 50 other countries. E-commercial networks shall be an efficient connection among its factories.

For agribusiness, the selected stock index, Golden-Agri Resources (GAR), is a Singaporean agricultural companionship. Palm oil is the main product, and the company has owned a subsidiary in Liberia called Golden Veroleum, which in 2018 is removed from the roundtable on sustainable palm oil for alleged land acquisition violations. GAR’s target is the roadmap to share with employees, smallholders, suppliers, and customers for corroboration and realizing the GAR’s vision of a sustainable palm oil industry. E-commerce is the key.

According to information and technologies, the index, SingTel, is the major telecom operating in the Republic of Singapore. With directly implied as the company was known as a telecommunications equipment producer, referred to mobile phone networks and fixed line telephony services, SingTel was the true e-commerce company which was the title sponsor of the first Formula One night race in Singapore. They have continued sponsoring the race through 2010. The last predominant stock index observing in the paper is Global Logistic Properties. The company is Singaporean leading developer and operator of logistics facilities, which is internationally established in the main market such as China, Japan and Brazil. This can be implied as a real estate supplier. It is undeniable that the e-commercial tool is one of the essential tools for strongly standing on the global economy.

MAIN FOCUS OF THE CHAPTER

An important point is a statistical inference. Since it is not like the traditional way of statistics (objective thinking) which was applied in many econometrical research. Bayesian inference employed in this extended version research is stated as “modern” in econometrics, which is called subjective thinking. Conceptually, the models’ posteriors are relied on “belief” or “prior”, which can be generated from truth and academic references. Usefully, Bayesian statistics can be practical in data classification methods such as the ADF unit-root testing (Dickey and Fuller, 1979) and regimes switching models (Hamilton, 1989). These empirical researches can be found in Wannapan et al. (2018), Chaiboonsri (2018), and Wannapan et. al. (2018). Additionally, the important methods for the data classification; entropy, can

be found in Vinod (2013) and cross-entropy analyses are used by Vázquez (2011). This statistical tool has been usefully applied in many fields, for examples, Mannor et. al. (2003), He et. al. (2010), and Goschin et. al. (2013).

Considering into the part of econometric forecasting, it is undeniable that the main problem is the number of observations. In particular, to verify the prior and posterior really needs simulations such as the bootstrapping approach (Efron, 1993) or Markov chain Monte Carlo: MCMC (Gilks and Wild, 1992) for modeling interpretations in Bayesian inference. Empirical works can be found in Chaitip et. al. (2014) and Wannapan and Chaiboonsri (2017). It is obvious simulations are useful to overcome the robustness problem and practical to help economists finding the sensible data distribution.

Furthermore, The huge challenge goes to the most essential component which predominantly changes the way to do econometric methods. In the meantime, the development of physics, especially the theory of relativity (Einstein) and the quantum theory (Max Planck) clearly showed defects of the mechanistic view on the world in explaining some natural circumstances; the science needed new approach – so called holistic view on the world. Inevitably, the world mostly known is not understood as the set of the isolated pieces or the causality principle (cause – consequence) (Vukotic, 2011).

Quantum computing techniques are hybridized with genetic algorithms. For instance, quantum rotation gate operations for the big data such as chromosomes or DNA are employed to the whole evolutionary process. Econometrically, it has lots of superior advantages and deals with speedy convergence, time saving, little population scale, and robustness (Cheng-Wen and Ling, 2017).

Nowadays, economists start to academically and practically study quantum mechanism, especially quantum economic computations for seeking parametric outcomes. For example, Baaquie (2007), Orrell (2016), Orrell and Chlupatý (2016), and Colin (2017). To step out a simple, natural, low-dimensional family of smooth probability distributions over the reals, modeling regression residuals, the wave function indication of continuous probability densities is a practical solution to the requirement for a general class of well-behaved probability densities. Additionally, any smooth density resists to over-fitting. This is the novel way combining with quantum mechanical states to be effective in a production data analysis system for modeling a wide variety of user-uploaded data (Thompson, 2018).

Applying to the section of data managements, this is in financial time-series analyses. Most of final solutions are focused on the efficiencies of investments. To implement this objective, the Markowitz portfolio optimization (Markowitz, 1952) is necessary to clarify the portion of possibilities to invest in stock markets. The empirical works were stated following Lai (2011), Marasovic et. al. (2011), Wannapan et. al. (2018). Hence, this research tries to effort the quantum mechanics in the Markowitz portfolio optimization analysis based on Modern Portfolio Theory (MPT).

Phase One: Data Analysis and Classification

The ADF Unit Root Test Based on Bayesian Inference

The ADF test regression (Said and Dickey, 1984) can be also written in an alternative formation, which is described in Equation (1),

$$\Delta y_t = c + \alpha' D_t + \phi y_{t-1} + \sum_{j=1}^p \gamma_j \Delta y_{t-j} + \varepsilon_t, \quad (1)$$

where $\phi = \varphi - 1$. Considering the null hypothesis, $\Delta y_t \sim I(0)$ which indicates that a non-stationary model is $\phi=0$. In this research, the main Bayesian had been used to test unit roots. Being $\phi=(\varphi, a^*)$ the parameter vector, $\phi = \sum_{i=1}^p \varphi_i$ and $a^*=(c, \alpha, \gamma)$, and assuming σ^2 is fixed. The prior density of ϕ is factorized as (Diniz et al, 2011)

$$p(\phi) = p(\varphi)p(a^*|\varphi)$$

The marginal likelihood for φ is

$$l(\varphi | D) \propto \int l(\phi | D) \varphi(a^* | \varphi) da^*, \tag{2}$$

where D is the observation vector. A prior for is the main ingredient used by standard Bayesian procedures to test the existence of unit root. Basically, all of them employ Bayes factors and posterior probabilities, which are described in the equation (3),

$$B_{01} = \frac{l(\varphi = 1 | D)}{\int_0^1 l(\varphi | D) \varphi(\varphi) d\varphi}. \tag{3}$$

Bayesian statistics considers hypotheses regarding multiple parameters by adapting Bayes factor comparisons. The Bayes factors are flexible allowing multiple hypotheses to be a synchronized comparison, and nested models are not used in order to make comparisons (Jeffrey, 1961).

The Markov-Switching Bayesian Vector Autoregression Model (MSBVAR) for Classification

Based on the journal research of Hamilton (1989) who employed a Markov-switching autoregressive model to study on the quarterly data of US GNP, the Markov-switching version of Bayesian vector autoregressive model is invented for breaking down normality assumptions in time series forecasting. The structural equation of Markov-switching Bayesian VAR (MS-BVAR) is expressed as

$$\sum_{i=0}^p y_{t-i} A_i (s_t) = d (s_t) + \varepsilon_t (s_t), t = 1, 2, \dots, T. \tag{4}$$

Considering into the equation (4), $S_t = j$ is an h-dimensional vector state of the process, j is the term of integer labels for the state, with a $h \times h$ Markov transition matrix. The matrix is given the probability of transitioning from the state S_{t-1} to S_t , which can be mathematically expressed as $Pr(S_t = k | S_{t-1} = j)$. For setting the prior in MSBVAR, the parameters A_i and d are determined by beliefs, the random walk prior in the Sims and Zha model (Sims and Zha, 1998). Thus, the predictions from a Markov-switching VAR model like the equation (4) are the weighted combination of the forecasts for each state or phase.

Phase Two: The maximum entropy principle and cross entropy for the market leader and follower

Fundamentally, the distinction of complete ignorance when we do not really know information is possible (Shore and Johnson, 1980). As express by Vinod (2013), Maximum entropy is a powerful method for avoiding all unnecessary distributional assumptions. This computational estimation is depended on a given finite state space and constraints, which are finite sets of n states with probabilities q and they were defined as a prior estimation form with new information I ; $\sum_i q_i a_{ki} = 0$ or $\sum_i q_i b_{ki} \geq 0$, where known numbers are a_{ki} and b_{ki} . Thus, the entropy maximization is written as

$$H(q) = \sum_i q_i \log(q_i) - \log(n), \tag{5}$$

where this is equivalent to maximize the entropy $-\sum_i q_i \log(q_i)$. The minimizing function, $H(q)$, satisfies uniqueness, permutation invariance, and subset independence. It is equivalent to the unique that can be obtained by maximizing entropy (Shore and Johnson, 1980),

$$H(q) = \sum_i f(q_i). \tag{6}$$

Furthermore, another method that is simultaneously employed to parallel the entropy, the cross entropy (CE) is the mutual support degree that can be used to determine the weights of the information sources, where a larger weight represented higher mutual supports (Men et.al. 2016). The cross entropy of two likelihood distribution was expressed as $D(g||f)$, and the cross entropy of discrete cases was formulated as

$$D(g || f) = \sum_1^n g_i \ln \left(\frac{g_i}{f_i} \right), \tag{4}$$

and continuous cases was

$$D(g || f) = \int g(x) \ln \frac{g(x)}{f(x)} dx = \int g(x) \ln g(x) dx - \int g(x) \ln f(x) dx, \tag{5}$$

where f and g indicate the probability vector in discrete cases and the probability density function in the continuous case, respectively.

Phase Three: Quantum mechanical states for parametrically estimating

Unlike any parametric estimation, this research applies quantum mechanical states of parametric computations. This is specifically modified for aiding and empowering the precision of weight portions under MPT in ASEAN stock exchanges. As Baaquie, Belal E. (2007). Orrell, David (2016), Orrell, David

and Chlupatý, Roman (2016), Teese, Colin (2017), Orrell, David (2018), and Clegg, Brian(2018) believe that classical physics or microeconomics behavior did not understand this behavior clearly, especially the elusive classification of data distributions. Consequently, to serve the need of the risk-averse investor for avoid high risky in the stocks, the fundamental of quantum mechanics (QM) is potentially the solution to describe phenomena or information of nature at smallest, for example, atomic or subatomic scales by the wave function. In 2018, Madeleine B. Thompson tried to develop the wave function for understanding this phenomena. Mathematically, the formula is presented as follows:

$$P_i = \left(\sum_{k=0}^K \frac{\omega_{k+1}}{\sqrt{\pi 2^k k!}^{1/2}} H_k(\chi_i) \right)^2 e^{-\chi_i^2} . \quad (6)$$

From Equation (20), K is the maximum degree and ω is a vector of coefficient from the wave function. Also, H_k is the Hermite polynomial (1864) of degree k and χ_i is a numerical vector for log returns of all predominant five financial indexes in ASEAN are computed by Markowitz Portfolio optimization.

Phase Four: Markowitz portfolio optimization based-on quantum mechanics

The theory of optimal selection of portfolios was proposed by Harry Markowitz in the 1950s, which raised him the 1990 Nobel Prize for Economics. Fundamentally, directly related to the financial time-series forecasting, the concept of his work considered about an investor who has a certain amount of money to be invested in a number of different factors (bonds, equities, and macroeconomic variables) with random returns. According to this research, the proportion of the total amount in variables i and x_i can be computed the expected return and the variance of the resulting portfolio $x_i = (x_1, \dots, x_n)$ as follows

$$E(x)_{Bull} = x_1 u_1 + \dots + x_n u_n = u^T x , \quad (7)$$

then

$$Var(x)_{Bull} = \sum_{ij} \rho_{ij} \sigma_i \sigma_j x_i x_j = x^T x , \quad (8)$$

and

$$E(x)_{Bear} = x_1 u_1 + \dots + x_n u_n = u^T x , \quad (9)$$

then

$$Var(x)_{Bear} = \sum_{ij} \rho_{ij} \sigma_i \sigma_j x_i x_j = x^T x , \quad (10)$$

where $\rho_{ij} = 1, Q_{ij} = \rho_{ij} \sigma_i \sigma_j$.

RESEARCH RESULTS OF THIS CHAPTER

The Results of Data Analysis and Classification

First of all, every time-series trends must be checked for clarifying the type of suspicious data. In this research, the ADF testing based on Bayesian statistics is employed to do data stationary classifications. With 100,000 simulated observations by the MCMC approach and Bayesian factor comparison, the empirical unit-root outcomes shown in the table 1 can be stated that all of collected five financial indexes are stationary.

Table 1. The Bayesian ADF testing for data stationary

Country	Hypothesis	Posterior odds ratio	Inference	Result
May Bank (MB) (Banking)	H0 (Mi): Non-stationary data H1 (Mj): Stationary data	7.09e-05	Strong evidence of Mj	Stationary data
PPB group (PPB) (Energy)	H0 (Mi): Non-stationary data H1 (Mj): Stationary data	0.388	Moderate evidence of Mj	Stationary data
GoldAgri (GA) (Agriculture)	H0 (Mi): Non-stationary data H1 (Mj): Stationary data	0.00604	Strong evidence of Mj	Stationary data
SingTel (ST) (Telecommunication)	H0 (Mi): Non-stationary data H1 (Mj): Stationary data	0.00207	Strong evidence of Mj	Stationary data
LogProb (GLP) (Real estate)	H0 (Mi): Non-stationary data H1 (Mj): Stationary data	0.000251	Strong evidence of Mj	Stationary data

Sources: authors

Additionally, since it is obvious that the movement of financial trends is not the linear line, which is not absolutely easy to predict. For the part of data switching analyses, the results estimated from the MSBVAR model with 35 sampling iterations empirically expressed that data has been divided into two types such as Bull and Bear periods, which are 195 times and 800 times, respectively. They are all daily data and represented in the table 2.

Table 2. The regimes switching result estimated by the MSBVAR model (995 observations (days))

Sector	Duration (daily times)
Bull periods (MayBank, PPBgroup, GoldAgri, SingTel, LogProb)	195
Bear periods (MayBank, PPBgroup, GoldAgri, SingTel, LogProb)	800

Sources: authors

As this research has seen that one of interesting points in financial analyses is which index has to be considered as a primary sign, the results calculated by entropy and cross-entropy approaches helpfully express the solution, which can efficiently verify the leader and follower among large five financial stock indexes in ASEAN countries by comparing the overall entropy value ($H(p)$) and cross-entropy values ($H(p,mi)$). The results were shown in the table 3 and 4, respectively. The former table explained that Golden Agri-Resource in Singapore’s stock exchange is the leader during bull market. The cross value of this index is the nearest value to the main entropy. On the other hand, in the bear periods, the latter table stated the similar solution, which is the index of Golden Agri-Resource is the leader indicator to fluctuate when the ASEAN financial market is down. As a result, at this stage, in order to classify the highlight index for setting variables to do the structural dependence prediction is implemented.

Table 3. The presentation of entropy and cross-entropy approaches for indicator classification during bull periods

Entropy	MB (p)	PPB(p)	GA(p)	ST(p)	GLP (p)
	Cross Entropy	Cross Entropy	Cross Entropy	Cross Entropy	Cross Entropy
H(p) = 27.753	$H(p,m1) = 34.396$	$H(p,m2) = 38.247$	$H(p,m3) = 31.087$	$H(p,m4) = 41.311$	$H(p,m5) = 38.815$
Ordered by Cross Entropy	2	3	1	5	4

Sources: authors

Table 4. The presentation of entropy and cross-entropy approaches for indicator classification during bear periods

Entropy	MB (p)	PPB(p)	GA(p)	ST(p)	GLP (p)
	Cross Entropy	Cross Entropy	Cross Entropy	Cross Entropy	Cross Entropy
H(p) = 114.349	$H(p,m1) = 140.682$	$H(p,m2) = 164.385$	$H(p,m3) = 123.088$	$H(p,m4) = 164.170$	$H(p,m5) = 134.547$
Ordered by Cross Entropy	3	5	1	4	2

Sources: authors

Again, the cross-entropy approach confirms that the Golden Agri-Resource (GA) originally established in Indonesia and this company also supported the agribusiness sector. Therefore, the result of estimation in this research part still confirmed E-Commerce and E-Business in ASEAN especially agribusiness still play a major important role in economy of ASEAN countries. Since the Golden Agri-Resource (GA) as a leader of the stock market to influence whenever the ASEAN stock market has a fluctuation both up and down

The Results of Computation Based on Wave Function

In the ultimate section of multi-analytic methods, the portfolio optimization based on wave function (QM) (see appendix A) is essentially applied to conclude the empirical results for the way which can potentially be invested. It is crystal clear that doing data management is more efficient than investment

Multi-Process Analysis and Portfolio Optimization Based on QM Under Risk Management

by only human's instinct. To optimize the investment plans and portions for putting funds in the financial market, the result obviously stated two optimal ways such as minimizing variances and maximizing expected returns have higher sharp ratios than the investment without optimizing calculating in both bull and bear periods based on wave function. In other words, the way of maximizing expected value should be the highlight suggestion for financially investing in bull periods. On the other hand, the aspect of minimizing variances (risks) is suitable for bear periods. The results were presented in the table 5.

Table 5. The proportion of money invested in all Stocks under the decision by Portfolio Optimization under Quantum Mechanical (QM) analysis in bull market

Portfolios				
		Max Return	Min SD	Max SR
Constraining Variables	None.	at $\sigma \leq 0.0043$	at $\mu = 1.2328$	Non
Values constrain	N/a	0.0043	1.2328	(Max Sharpe Ratio)
MB	20%	0%	0%	0%
PPB*	20%	97%	74%	74%
GA	20%	0%	0%	0%
ST*	20%	3%	26%	26%
GLP	20%	0%	0%	0%
ΣW	100%	100%	100%	100%
μ	1.22716	1.2328	1.2327	1.2327
σ_p	0.021334	0.0043	0.0041	0.0041
μ/σ	57.52004	286.6958	301.7818	301.7818

Noted: ** stands for the possible portions to financially invest in ASEAN stock indexes during bull *Sources: authors*

Conceptually, two types of optimizing managements which are the risk aversion (minimizing variances) and risk lover (maximizing expected returns) obviously express that there are different strategies to financially invest bull periods. To explain in each situation, firstly, the result strongly confirmed the PPB group (PPB) and the SingTel (ST) are considerably highlighted to be the most interesting indicator, which contains the lowest rate of risks among five stock indexes during bull periods. In addition, the portfolio management under the quantum mechanical (QM) analysis suggested that the investors should be allocated their money in the PPB group (PPB) about 74% and afterward, they need to invest their money in the SingTel (ST) approximately around 26% under their behavior undergoing protection of the risky for investment. In the second case, the maximizing returns optimization calculated during bull periods, the optimal weight portions based on quantum mechanical (QM) stages suggest that the investors should allocate their money in the PPB group (PPB) increase as 97%. Afterward, they need to invest their money in the SingTel (ST), decreasing an investing portion at 3% relied on their behaviors to protect the risky. In terms of the strategies to focus on the minimum sharp ratio emphasis, the investors should allocate their money in the PPB group (PPB), which is a high return portion as 76%. However, for spreading risks and avoiding losses, investors need to more widely invest funds in the SingTel (ST) as a significant increasing portion at 3%. Under suggested by the optimal minimum portfolio calcula-

tion parametrically estimated by quantum mechanical (QM) analysis, this is the scenario that can be the possible choice for inputting funds into the market, the answer is confirmed by the best sharp ratio which is 301.7818.

Table 6. The proportion of money invested in all Stocks under the decision by Portfolio Optimization under Quantum Mechanical (QM) analysis in bear market

Portfolios				
		Max Return	Min SD	Max SR
Constraining Variables	None.	at $\sigma \leq 0.054$	at $\mu = 1.2295$	Non
Values constrain	N/A	0.054	1.2295	(Max sharp ratio)
MB	20%	0%	0%	0%
PPB	20%	0%	0%	0%
GA	20%	0%	0%	0%
ST	20%	100%	100%	100%
GLP	20%	0%	0%	0%
ΣW	100%	100%	100%	100%
μ	1.20808	1.2295	1.2295	1.2295
σ_p	0.0785	0.0541	0.0541	0.0541
μ/σ	15.3860	22.7412	22.7412	22.7412

Noted: ** stands for the possible portions to financially invest in ASEAN stock indexes during bull

Sources: authors

As seen details in Table 6, in a bear period, this situation affects investors have more serious considerations to invest their money in the stocks. Under this situation, the portfolio optimization parametrically estimated by quantum mechanism provides a strong decision for the case of maximizing profits that investors should directly invest their money in SingTel (ST). There is an interesting point for this outcome since whatever the strategies it is, the weight portion implies the predominant e-commerce leader should be the company which is a specialist in information and technologies. SingTel is potential to fill the gap. The result also stands on the same weight portion in the case of minimizing risks. The quantum portfolio optimization technically shows SingTel is the base for implementing e-commerce activities. Telecommunication sectors are still the major player to drive e-commerce and e-business in ASEAN. Particularly, the collaboration between the business and telecommunication system is significantly required.

CONCLUSION

It is reasonable to conclude that there is not acceptable for doing only one econometrical process and answering that calculated parameters are precise and strongly stand for telling the truth of collected data. In particular, financial time-series information is one of the most difficult data types, which cannot be easily predicted. Financial time-series trends need to be checked, classified, ordered, estimated, forecasted, and managed. Consequently, the multi-analytic processes for econometrics are successfully

employed in this research to do an efficient combination for solving the question that what will do next when the data has been already predicted.

Obviously, financial trends are the variables that investors have been considerably focusing since financial markets have been established. In this research, five predominantly stock index returns in ASEAN Exchange such as MayBank, PPB GROUP BERHAD, Golden Agri-Resource, SingTel, and Global Logistic Properties are observed as daily trends during 2004 to 2018. Technically, one of importantly econometrical methods is a data classification, especially checking the condition of suspicious data to prevent fake parametric estimations. Interestingly, the Bayesian approach and MCMC simulations are statistically applied to do checking data stationary. These approaches are used to parametrically estimate the ADF unit-root testing. The result was clear that all collected data is stable. Next, the financial trends are moved to classify data fluctuations by the MSBVAR model. Empirically, the result is evident that the trends are divided into two types relied on time variations, which are bull and bear periods. Then, the data was transferred to the section of entropy processes. In this stage, the financial indexes are classified to be a leader and followers for ordering the variables in forecasting equations. The result was obvious that the energy business sector (PPB GROUP BERHAD) is the leader during bull market situations since energy is the simulator for boosting up economic systems. For policy cultivations, energy productions should be with the expansion of telecom and information technologies. In the upcoming future, e-commercial business shall blossom in these financial indexes and spread to practical areas of real business sectors.

The decision, on the other hand, is difference when considering into bear situations. In the case of downsizing financial market flows, little sunshine among unfavorable signs is the index of telecommunication and information technologies. However, the difficulty is the way to contribute the company to make more a profitability (during the period economic boom) to be more influence in other stock prices in financial markets sustainably. From these investigations, it can give more information for economic movement reaction at least in two dimensions.

The section of the Markowitz portfolio optimization parametrically estimated by quantum mechanics evidently suggested PPB group (PPB) in Malaysia and SingTel (ST) are the two companies could be preferment for investors to put funds in ASEAN exchanges underneath the efficient risk management. Because of SingTel, the ITs provider, is the financial index plays an essential role in any situation in ASEAN stock markets. This is obvious e-commercial activities shall be also spread following the growth of the company. Thus, the ultimate implication of this research is pointing out that the blossom of e-commercial businesses in this continent can be observed by the sign of the financial market. Moreover, the mission in the future is how to run businesses between e-commercial activities and labor forces to playing an important role in economic development.

ACKNOWLEDGMENT

This research work was partially supported by the Chiang Mai University.

REFERENCES

- Chaiboonsri, C. and Wannapan, S. (2018). *The extreme value forecasting in dynamics situations for reducing of economic crisis: cases from Thailand, Malaysia, and Singapore*. Global Approaches in Financial Economics, Banking, and Finance, Springer Cham.
- Chaitip, P., Chaiboonsri, C., & Inluang, F. (2014). The production of Thailand's sugarcane: Using Panel Data Envelopment Analysis (Panel DEA) based decision on bootstrapping method. *Procedia Economics and Finance*, 14, 120–127. doi:10.1016/S2212-5671(14)00693-5
- Cheng-Wen, L. & Bing-Yi, Tim. (2017). Applications of the chaotic quantum Genetic algorithm with support vector regression in load forecasting. *Energies*, 10, 1–18.
- Clegg, B. (2018). *Quantum Economics - David Orrell*. Retrieved from <http://popsiencebooks.blogspot.com/2018/07/quantum-economics-david-orrell.html>
- Deci, E. L., & Ryan, R. M. (1991). A motivational approach to self: Integration in personality. In *Proceedings of Nebraska Symposium on Motivation* (vol. 38, pp. 237-288). Lincoln, NE: University of Nebraska Press.
- Dickey, D. A., & Fuller, W. A. (1979). Distribution of the estimators for autoregressive time series with a unit root. *Journal of the American Statistical Association*, 74(366), 427–431. doi:10.2307/2286348
- Efron, B., & Tibshirani, R. (1993). *An Introduction to the Bootstrap*. Chapman & Hall/CRC. doi:10.1007/978-1-4899-4541-9
- Geweke, J. F. (2004). Getting it right: Joint distribution tests of posterior simulators. *Journal of the American Statistical Association*, 99(467), 799–804. doi:10.1198/016214504000001132
- Gilks, W. R., & Wild, P. (1992). Adaptive rejection sampling for Gibbs sampling. *Journal of the Royal Statistical Society. Series C, Applied Statistics*, 41(2), 337–348.
- Goschin, S., Weinstein, A., & Littman, M. L. (2013). The cross-entropy method optimizes for quantiles. In *Proceedings of the 30th International Conference on Machine Learning* (Vol 28, pp. 1193-1201). Atlanta, GA Academic Press.
- Hamilton, J. (1994). *Time Series Analysis*. Princeton University Press.
- Hamilton, J. A. (1989). A new approach to the economic analysis of nonstationary time series and business cycle. *Econometrica*, 57(2), 357–384. doi:10.2307/1912559
- He, D., Lee, L. H., Chen, C. H., Fu, M. C., & Wasserkrug, S. (2010). Simulation optimization using the cross-entropy method with optimal computing budget allocation. *ACM Transactions on Modeling and Computer Simulation*, 20(1), 4.1 – 4.21.
- Hermite, C. (1864). Sur un nouveau développement en série de fonctions. *C. R. Acad. Sci. Paris*, 58, 93–100.

- Jaques, P. A., & Viccari, R. M. (2006). Considering students' emotions in computer-mediated learning environments. In Z. Ma (Ed.), *Web-based intelligent e-learning systems: Technologies and applications* (pp. 122–138). Information Science Publishing. doi:10.4018/978-1-59140-729-4.ch006
- Jeffreys, H. (1961). *Theory of probability* (3rd ed.). New York: Oxford University Press.
- Joe, H., Li, H., & Nikoloulopoulos, A. K. (2010). Tail dependence functions and vine copulas. *Journal of Multivariate Analysis*, *101*(1), 252–270. doi:10.1016/j.jmva.2009.08.002
- Junho, S. (in press). Roadmap for e-commerce standardization in Korea. *International Journal of IT Standards and Standardization Research*.
- Lai, T., Xing, H., & Chen, Z. (2011). Mean-variance portfolio optimization when mean and covariance are unknown. *The Annals of Applied Statistics*, *5*(2A), 1–27. doi:10.1214/10-AOAS422
- Lanktree, C., & Briere, J. (1991, January). *Early data on the trauma symptom checklist for children (TSC-C)*. Paper presented at the meeting of the American Professional Society on the Abuse of Children, San Diego, CA.
- Mannor, S., Rubinstein, R., & Gat, Y. (2003). The cross entropy method for fast policy search. In *Proceedings of the Twentieth International Conference on Machine Learning (ICML-2003)*, (pp. 512–519). Washington, DC: Academic Press.
- Marasovic, B., Poklepovic, T., & Aljinovic, Z. (2011). Markovitz' model with fundamental and technical analysis – complementary methods or not. *Croatian Operational Research Review*, *2*, 122–132.
- Markowitz, H. M. (1952). Portfolio selection. *The Journal of Finance*, *7*(1), 77–91.
- Men, B., Long, R., & Zhang, J. (2016). Combined forecasting of stream flow based on cross entropy. *Entropy (Basel, Switzerland)*, *18*(336), 1–12.
- Nelsen, R. (2006). *An introduction to copulas*. Springer.
- Orrell, D. (2016). A quantum theory of money and value. *Economic Thought*, *5*(2), 19–28.
- Orrell, D. (2018). *Quantum economics: the new science of money*. Icon Books.
- Orrell, D. (2019). *Quantum economics: the new science of money (reissue)*. Icon Books.
- Orrell, D., & Chlupatý, R. (2016). *The evolution of money*. Columbia University Press. doi:10.7312/orre17372
- Said, S. E., & Dickey, D. (1984). Testing for unit roots in autoregressive moving-average models with unknown order. *Biometrika*, *71*(3), 599–607. doi:10.1093/biomet/71.3.599
- Sawyer, S., & Tapia, A. (2005). The sociotechnical nature of mobile computing work: Evidence from a study of policing in the United States. *International Journal of Technology and Human Interaction*, *1*(3), 1–14. doi:10.4018/jthi.2005070101
- Shore, J., & Johnson, R. W. (1980). Axiomatic Derivation of the principle of maximum entropy and the principle of minimum cross-entropy. *IEEE Transactions on Information Theory*, *26*(1), 26–37. doi:10.1109/TIT.1980.1056144

- Sims, C. A., & Zha, T. A. (1998). Bayesian methods for dynamic multivariate models. *International Economic Review*, 39(4), 949–968. doi:10.2307/2527347
- Teese, C. (2017). *Money and quantum physics*. Retrieved from <http://newsweekly.com.au/article.php?id=57574>
- Thompson, M. B. (2018). *Wave function representation of probability distributions*. Retrieved <https://arxiv.org/pdf/1712.07764.pdf>
- VandenBos, G., Knapp, S., & Doe, J. (2001). *Role of reference elements in the selection of resources by psychology undergraduates*. Retrieved from <http://jbr.org/articles.html>
- Vázquez, E. F. (2011). Updating weighting matrices by cross-entropy. *Investigaciones Regionales*, 21, 53–69.
- Vukotic, V. (2011). Quantum economies. *Panoeconomicus*, 2(2), 267–276. doi:10.2298/PAN1102267V
- Wannapan, S., & Chaiboonsri, C. (2017). Sustainable international tourism demand in Thailand: The case of Chinese tourists. *Actual Problems in Economics*, 191, 163–177.
- Wannapan, S., Chaiboonsri, C., & Sriboonchitta, S. (2018). Identification of the connection between tourism demand and economic growth in ASEAN-3. *International Journal of Trade and Global Markets*, 11(1/2), 12–20. doi:10.1504/IJTGM.2018.092487
- Wannapan, S., Chaiboonsri, C., & Sriboonchitta, S. (2018). Macro-econometric forecasting for during periods of economic cycle using Bayesian extreme value optimization algorithm. In *International Conference of the Thailand Econometrics Society*, (Vol 18, pp. 706-723). Springer Cham. 10.1007/978-3-319-70942-0_51
- Wannapan, S., Rukpuang, P., & Chaiboonsri, C. (2018). The optimizing algorithm for economic cycles in ASEAN stock indexes. In *International Symposium on Integrated Uncertainty in Knowledge Modelling and Decision Making*, (Vol 10758, pp. 420-432). Springer Cham. 10.1007/978-3-319-75429-1_35
- Wilfley, D. (1989). *Interpersonal analyses of bulimia: Normal-weight and obese* (Unpublished doctoral dissertation). University of Missouri, Columbia, MO.
- Zhao, F. (Ed.). (2006). *Maximize business profits through e-partnerships*. IRM Press. doi:10.4018/978-1-59140-788-1

ADDITIONAL READING

- Ash, R. B. (1990). *Information Theory*. Dover Publications, Inc.
- Bernardo, J. M., & Smith, A. F. M. (1994). *Bayesian Theory*. Wiley. doi:10.1002/9780470316870
- Mehra, J., & Rechenberg, H. (1982). *The historical development of quantum theory*. Springer-Verlag. doi:10.1007/978-1-4612-5783-7
- Reza, F. M. (1994). [1961]. *An Introduction to Information Theory*. Dover Publications, Inc.

Smith, H. (1991). *Introduction to Quantum Mechanics*. World Scientific Pub Co Inc. doi:10.1142/1271

KEY TERMS AND DEFINITIONS

ASEAN Exchange: The stocks market consist of six stock exchange such as the stock exchange of Indonesia, Malaysia, Philippines, Singapore, Thailand and Vietnam aims to promote the growth of the ASEAN capital market.

Bayesian Inference: It is some kind of statistics branch as a based stand on by Bayes theorem and this statistics method was based on the subjective or prior distribution mixed with a likelihood function of data by computed for posterior distribution.

E-Business: It is some kind of activity to run the business process mainly on the internet.

E-Commerce: It is some kind of activity to run the Commercial transactions on mainly the internet.

Modern Portfolio Theory (MPT): The Mean-Variance analysis is to manage a Portfolio of assets by depending on the efficiency frontier concept.

Quantum Mechanics: It is a modern physics to describe the properties of nature especially the smallest of atom behavior such as the movement of the electron was described by the wave function.

This research was previously published in the Handbook of Research on Innovation and Development of E-Commerce and E-Business in ASEAN; pages 46-61, copyright year 2021 by Business Science Reference (an imprint of IGI Global).

Chapter 20

A Quantum NeuroIS Data Analytics Architecture for the Usability Evaluation of Learning Management Systems

Raul Valverde

Concordia University, Canada

Beatriz Torres

University of Quebec in Outaouais, Canada

Hamed Motaghi

University of Quebec in Outaouais, Canada

ABSTRACT

NeuroIS uses tools such as electroencephalogram (EEG) that can be used to measure high brainwave frequencies that can be linked to human anxiety. Past research showed that computer anxiety influences how users perceive ease of use of a learning management system (LMS). Although computer anxiety has been used successfully to evaluate the usability of LMS, the main data collection mechanisms proposed for its evaluation have been questionnaires. Questionnaires suffer from possible problems such as being inadequate to understand some forms of information such as emotions and honesty in the responses. Quantum-based approaches to consciousness have been very popular in the last years including the quantum model reduction in microtubules of Penrose and Hameroff (1995). The objective of the chapter is to propose an architecture based on a NeuroIS that collects data by using EEG from users and then use the collected data to perform analytics by using a quantum consciousness model proposed for computer anxiety measurements for the usability testing of a LMS.

DOI: 10.4018/978-1-7998-8593-1.ch020

INTRODUCTION

NeuroIS uses neurotechnology tools such as galvanic skin response (GSR) and Electroencephalogram (EEG) for research in Information Systems (IS) (Dimoka et al 2010). High brainwave frequencies can be linked to human anxiety and neurotechnology can be used to measure these frequencies (Valverde 2015). Past research showed that computer anxiety influences how users perceive ease of use of a learning management system (Saade & Kira 2009). Although computer anxiety has been used successfully to evaluate the usability of learning management systems, the main data collection mechanisms proposed for its evaluation has been questionnaires. Questionnaires suffer from possible problems such inadequate to understand some forms of information such as emotions, lacks validity, possible lack of thought and honesty in the responses (Ackroyd & Hughes 1981).

Learning management systems (LMS) are designed to facilitate the learning process and have been used in recent years extensively in Business Schools (Condon & Valverde 2014). However, it has been reported that as many as fifty percent of adults, including first-year University students, have some sort of computer-related phobia and previous studies have shown that computer anxiety influences how users perceive ease of use and computer self-efficacy an information system (Saade & Kira 2009). Much effort has been devoted to creating user friendly interfaces in recent years (Venkatesh & Morris, 2000) in particular with the use of NeuroIS (Dimoka et al 2010). Motivated by previous computer-anxiety studies and the lack of studies that incorporate data collection and analytical techniques using neuroscience that can better capture the perception of computer users for the purpose of usability evaluations, the objective of this study is to provide an understanding on how to use neuroscience techniques for data collection of the use of a LMS and provide the analytical tools that can process computer anxiety measurements for usability testing.

Quantum based approaches to consciousness have been very popular in the last years. Some of the approaches include the Quantum emission probabilities (Eccles, 1986), where the two-way mental-neural interaction (with the electric/magnetic fields as a link) is supposed to be realized in a manner analogous to probability fields in quantum Mechanics, the Photon-corticon interaction (Jibu & Yasue, 1995), where consciousness was reduced to the creation and annihilation dynamics of photons (as quanta of an electromagnetic field) and corticons (as quanta of a rotational field of water dipoles) and the quantum model reduction in microtubules (Hameroff, 1998; Penrose & Hameroff, 1995), where quantum coherence occurs by exciting quasicrystalline water molecules as dipoles buried in microtubules.

The objective of the chapter is to propose an architecture based on a NeuroIS that collects data by using neurotechnology from users and then use the collected data to perform analytics by using the quantum consciousness model proposed by Pop-Jordanov & Pop-Jordanova (2010) for computer anxiety measurements that can be used for the usability testing of a learning management system. This model proposes a theoretical approach to explain the characteristic empirical interdependence between the states of arousal (representing the level of consciousness) and EEG activity.

As a NeuroIS does not use surveys for data collection and instead uses direct brain wave measurements from the user's brain, the proposed approach contributes to the literature by incorporating data collection techniques based on neuroscience that can better capture the perception of computer users and also propose a set of analytical tools by using a quantum based approach that can be used for the purpose of usability evaluations of LMS.

LITERATURE REVIEW

Quantum Neural Network

Quantum Neural Networks (QNNs) are models, systems or devices that combine features of quantum theory with the properties of neural networks. Neural networks (NNs) are models of interconnected units based on biological neurons feeding signals into one another. A large class of NNs uses binary McCulloch-Pitts neurons, thus reducing the complex process of signal transmission in neural cells to the two states ‘active/resting’. The analogy with the two-level qubit serving as the basic unit in quantum computing gives an immediate connection between NN models and quantum theory. The majority of proposals for QNN models are consequently based

on the idea of a qubit neuron (or ‘quron’ as we suggest to name it), and theoretically construct neurons as two-level quantum systems. Although close to discussions about the potential ‘quantumness of the brain’, QNNs do not intend to explain our brain functions in terms of quantum mechanics. Neurons are macroscopic objects with dynamics on the timescale of microseconds, and a quron’s theoretically introduced two quantum states refer to a process involving millions of ions in a confined space, leading to estimated decoherence times in the order of 10–13 sec and less, thus making quantum effects unlikely to play a role in neural information processing. However, QNNs promise to be very powerful computing devices. Their potential lies in the fact that they exploit the advantages of superposition-based quantum computing and parallel-processed neural computing at the same time. QNN research can furthermore be seen as a part of a growing interest of scientist and IT companies to develop quantum machine learning algorithms for efficient big data processing. Artificial neural networks thereby play an important role as intelligent computational methods for pattern recognition and learning (Schuld & Petruccione 2014).

Brain-computer interface (BCI) has been identified to function as an extra channel between brain and external environment to transmit information bypassing the spinal and peripheral neuromuscular systems and has also found applications in rehabilitation, neuroscience and cognitive psychology. Existing research in applications of BCI is composed of two main areas. For assistive technology, BCI makes it possible for people with motor disabilities to regain the interactions with external environment in order to improve the quality of their lives. The second area aims at training the subject to emit a specific brain activity. In this application, BCI is called as Neurofeedback (NFB), it becomes a therapy tool which helps subjects recover their cognitive function by consciously altering some features of their electroencephalographic (EEG) signals in order to stay in certain brain state. These features can be used to activate a certain action, including visual/ auditory representations. By continuous neurofeedback training humans can learn how to change their brain electrical activity in a desired direction. It can assist individuals with a variety of conditions and disabilities in which the brain is not working as well as it might be (Wang et al. 2007).

Memory for Learning

Replication of the outstanding functions of the human brain in a computer, based on analysis and modeling of the essential functions of a biological neuron and its complicated networks has recently become an active research field. Several studies in this field have revealed successful developments of learning and memory which inspired by neural architectures in the brain. In general, from the engineering view, quantum mechanics (QM) has been developed as a theory to explain the fundamental principles of substance. QM provides several mathematical concepts, such as duality of waves and particles, complementarity,

and nonlocality, to improve the comprehension of the microworld. From the biological perspective, on the other hand, it is hypothesized that QM is based on mesoscopic features in the physical and biological or physiological processes of the brain, and it has the potential to illustrate the dynamics of neurons in the human brain by the quantum information. In fact, in the internal structure of neuron in the brain, the presence of the two quantum states in tubulin, which are proteins of the size 4 nm×8 nm and having a 20-nm gap between the synapse, suggest that artificial neural networks would be handled as a descriptive subject from QM perspective. In other words, the QIC is expected to be possible to bring a new standpoint for cognitive process of brain from a biological viewpoint.

Memory Capacity is a significant factor for performance in associative memory. The memory capacity, in general, is responsive to the number of neurons, e.g., the memory capacity of model is directly affected by the magnitude of number of neurons. Moreover, the differences in number of neurons between layers is another significant factor for the performance of memory capacity. Therefore, in regards to memory capacity, the two types of conditions are considered; the constant

number of neurons being set in layers, and different number of neurons applied to layers. From the above-mentioned two conditions, it can be evaluated that the sensitivity of the memory capacity from the viewpoint number of neurons. Here, the layer 1 is assigned with desired information while others are assigned the random bipolar patterns as the initial conditions (Masuyama et. al 2017).

The Early Quantum Model of Brain

In the quantum model, the brain elementary constituents are not the neurons and the other cells (which cannot be considered as quantum objects), but, in analogy with the QFT approach to living matter, they have been identified with the vibrational electric dipole field of the water molecules and other biomolecules present in the brain, and with the NG bosons (called the dipole wave quanta (dwq)) generated in the breakdown of the rotational symmetry of the electrical dipoles.

Memory printing is achieved under the action of external stimuli producing the breakdown of the continuous phase symmetry. In the quantum model of brain it is thus imported all the machinery of the spontaneous breakdown of symmetry introduced in the previous Section. The information storage function is thus represented by the coding of the ground state (the lowest energy state, or vacuum) through the coherent condensation of dwq collective modes. The memory capacity can be enormously enlarged by considering the intrinsic dissipative character of the brain dynamics: the brain is an open system continuously coupled to the environment. The dissipative quantum model seems to imply that the conscious identity emerges at any instant of time, in the present, as the minimum energy brain state which separates the past from the future, that point on the mirror of time where the conjugate images A and \tilde{A} join together. In the absence of such a mirroring there is neither consciousness of the past, nor its projection in the future: the suggestion is that consciousness does not arises solely from the subject (first person) inner activity,

without opening to the external world. In the dissipative quantum model the intrinsic dissipative character of the brain dynamics strongly points to consciousness as dialogue with the inseparable own Double (Vitiello 2003).

Stochastic Neurodynamics

Stochastic dynamics of relative membrane potential in the neural network is investigated. It is called stochastic neurodynamics. The least action principle for stochastic neurodynamics is assumed, and used to derive the fundamental equation. It is called a neural wave equation. A solution of the neural wave equation is called a neural wave function and describes stochastic neurodynamics completely. As a simple application of stochastic neurodynamics, a mathematical representation of static neurodynamics in terms of equilibrium statistical mechanics of spin system is derived (Yasue et. al. 1988).

Quantum Neural Computing

A quantum neural computer is a single machine that reorganizes itself, in response to a stimulus, to perform a useful computation. Selectivity offered by such a reorganization appears to be at the basis of the gestalt style of biological information processing. Clearly, a quantum neural computer is more versatile than the conventional computing machine.

Paradigm of science and technology draw on each other. Thus Newton's conception of the universe was based on the clockworks of the day; thermodynamics followed the heat engines of the 19th century; and computer followed the development of telegraph and telephone. From another point of view, modern computers are based on classical physics. Since classical physics has been superseded by quantum mechanics in the microworld and animal behavior of being seen in terms of information processing by neural networks, one might ask the question if a new paradigm of computing based on quantum mechanics and neural networks can be constructed. (Kak 1995)

We define a quantum neural computer as a strongly connectionist system that is nevertheless characterized by a wavefunction. In contrast to a quantum computer, which consists of quantum processes are supported. The neural network is a self-organizing type that becomes a different measuring system based on association triggered by an external or an internally generated stimulus. We consider some characteristics of a quantum neural computer and show that information is not a locally additive variable in such a computer (Kak 1995).

Virtual Learning Environment

Virtual learning environments and quantum mechanics efforts have made possible the virtual learning environment StudentResearcher proposed by Pedersen et al. (2016) for the learning of Quantum mechanics. Learning management systems (LMS) are designed to facilitate the learning process and have been used during many years in the academic environment (Condon & Valverde 2014). It has been reported that as many as fifty percent of adults have some sort of computer-related phobia (Saade & Kira 2009). Past research shows that computer anxiety influences how users perceive ease of use of an information system. Saade & Kira (2009) identified several variables of computer self-efficacy and computer anxieties. Self-efficacy is determined by levels of anxiety such that reduced anxiety and increased experience improves performance indirectly by increasing levels of self-efficacy (Saade & Kira 2009). Saade & Kira (2009) investigated the influence of computer anxiety on perceived ease of use and the mediating effect of computer self-efficacy on this relationship, within an e-learning context.

Although Saade & Kira (2009) contributed with computer anxiety effect in computer systems usability, the studied relied mainly in a survey methodology approach. Ackroyd and Hughes (1981) acknowledge some of the main disadvantages of surveys as:

- Is argued to be inadequate to understand some forms of information - i.e. changes of emotions, behaviour, feelings etc.
- Lacks validity.
- There is no way to tell how truthful a respondent is being.
- There is no way of telling how much thought a respondent has put in.
- The respondent may be forgetful or not thinking within the full context of the situation.
- People may read differently into each question and therefore reply based on their own interpretation of the question - i.e. what is 'good' to someone may be 'poor' to someone else, therefore there is a level of subjectivity that is not acknowledged.
- There is a level of researcher imposition, meaning that when developing the questionnaire, the researcher is making their own decisions and assumptions as to what is and is not important... therefore they may be missing something that is of importance.

Given the arguments of Ackroyd and Hughes (1981), surveys might not be the best way to measure levels of anxiety among computer users. Although computer anxiety has been proven as effective in the measurement of computer usability, biofeedback and neuro biofeedback might have better solutions to measure computer anxiety. Demoka et al (2010) highlighted the potential of cognitive neuroscience for IS research in particular for the domain of human-computer interaction (HCI).

Biofeedback and neuro biofeedback instruments measure muscle activity, skin temperature, electrodermal activity (sweat gland activity), respiration, heart rate, heart rate variability, blood pressure, brain electrical activity and blood flow. These technologies are able to capture analog electrical signals from the body and translate those signals into meaningful information through complex algorithmic software that a technician can then decipher. Biofeedback is also used by computer scientists in order to build human computer interactions (Valverde, 2011).

Biofeedback has been applied in the field of psychology for the measurement of anxiety. (Valverde 2015). Biofeedback uses sensors to monitor physiological relaxation indicators, like skin temperature and muscle tension. It expands classical biofeedback by using galvanic skin response (GSR) together with modern computer technology to detect the response of the built-mind-spirit body to a large array of stress indicators (Valverde 2015). Galvanic skin response is one measurable quantity generated involuntarily by the body. It's well known as the basis for the polygraph, or lie detector. The theory behind is that a user sweats more when stressed, and that telling a lie is stressful (Valverde 2011).

The brain and muscles generate small electrical signals that can be picked up by electrodes strapped to the body (Valverde 2011). Neuro biofeedback is based on electroencephalographic (EEG) measurements taken from the frontal cortex of the brain. This EEG information is presented to the user who then tries to consciously change their internal reactions to modify their brainwave state (Valverde 2015). Our brain works primarily with bioelectrical energy. Although the power of electricity that handles our neurons is low (measured in mill volts), this power processes, manage, distribute and use vast amounts of information and generates multiple answers (almost infinite in possibilities). So by using micro electricity, we can conclude that the brain is a machine of low frequencies. The first types of brain frequencies that were discovered were the "alpha" and "theta". Later, these findings were complemented by research in

the range frequencies captured by the electroencephalograph (Valverde 2015). Each type of wave results in a different neuropsychological state. That is, our mind, our body and our physical and physiological activity are completely different in each of these states or frequencies. The most common consciousness are wakefulness and sleep; however, changes in expressing both cerebral and psycho states change according to conscious or subconscious feelings of each person are distinguished. These changes are directly related to the electrical activity of the brain. This activity can be measured by the number of oscillations per second (Hz) that are linked to different states of consciousness in the brain: our brain only perceives a limited range of frequencies indispensable to operate with ease in this three-dimensional medium. 20 to 20,000 vibrations per second are perceptible by our ears, the colors perceived by our eyes range from red to violet (although extending beyond, up and down), all possible smells and tastes (which are also vibrations) and the endless textures that we can distinguish with our skin. But the brain is not only receiver but also is sends vibrations. It has been proven thanks to the EEG that the brain emits waves of varying intensity and frequency depending on the mental state of the person being observed (Valverde 2015). These waves are classified according to table 1.

As table 1 indicates, beta brain waves can be associated with stress and anxiety while alpha waves are associated with calmness and relaxation.

Table 1. Types of Brainwaves (Valverde 2015).

Types of Brain Waves	States of Consciousness
BETA WAVES: 14 Hz to 30 Hz	This type of waves is recorded when the person is awake in a state of normal activity. Correspond to states of conscious attention, anxiety, surprise, fear, stress.
GAMMA WAVES: 25 and 100 Hz	They express pathological conditions of maximum tension, excitement and the individual enters a state of STRESS in which the coordination of ideas and normal physical activity are seriously altered.
ALPHA WAVES: 8 Hz to 13 Hz	Relaxation and rest, calm, reflective state. Reduction of bodily sensations. The subconscious begins to emerge: Abstraction, suggestibility. Assimilation of the study. Ease of visualization of mental images.
THETA WAVES: 3.5 Hz to 7 Hz	During sleep or in deep meditation, autogenous training, hypnosis, yoga (whenever the formations of the subconscious act). The state stimulates creative inspiration. Considered a state for maximum capacity of learning. Fantasy, imagination. Hypnagogic images.
DELTA WAVES: 1 Hz to 3 Hz	It arises mainly in the states of deep sleep and unconsciousness. Very rarely can be experienced being awake unless with a very hard training (Yoga, Meditation, Zen, Hypnosis, Self-hypnosis) or with a synchronizer of hemispheres. It corresponds to deep sleep, hypnotic trance, REM sleep. It corresponds to sleep without dream, trance, deep hypnosis. Delta waves are very important in the healing process and strengthening the immune system.

NeuroIS

During the past decade, increasingly more scholars from the social and economic sciences and from computer science have started to use methods and tools from Neuroscience. This development is expected to result in a better theoretical understanding of human behavior such as decision making. Moreover, using Neuroscience methods and tools may contribute to the design and development of innovative information systems as demonstrated. (Hevner 2014).

Physiological reactions of humans in IS contexts (e.g., human interaction with computers) are usually measured by sensors placed on the body surface, even though the bodily reaction actually occurs “in” the body. The unit of signal frequency used is Hertz (Hz). The HZ is equivalent to cycles per second (Riedl, Davis, & Hevner, 2014).

Over the past decade, many scholars from various disciplines of social, economic science, computer science have started to pay particular attention to methods used and tools in neuroscience, to measure and conduct research in their respective fields (Riedl, Davis, & Hevner, 2014). In this vein, scholars in the field of Information Systems, have also incorporated on how to incorporate the neuroscience tools and measurement methods, in order to understand the human behavior by directly getting the results from the brain of human body.

Scholars in Information Systems have introduced the concept of NeuroIS into the IS literature (Dimoka et al., 2010; Dimoka, Pavlou, & Davis, 2007). The base of this concept of NeuroIS is to use neuroscience and neurophysiological methods, tools and theories to better understand, design, develop, and use of information communication technologies (ICT) in the society (Riedl et al., 2014).

Traditionally, IS researchers conduct data collection from various means and methods, notably from surveys, lab experiments, interviews, secondary data collection, ethnography, and many more methods (Dimoka et al., 2010; Dimoka et al., 2007). Considering that these methods of data collection are indeed useful, and have contributed importantly on the advancement of this field (IS research), asking directly the brain, and not the person opens an entirely new era of data collections, which is not biased, interpreted, and does not interfere with the subjectivity of human being. In other words, these methods, by means of directly asking the brain (data directly collected), tools offer unbiased measurements of decision-making, cognitive, emotional and social processes (Dimoka et al., 2010; Dimoka et al., 2007).

Moreover, one of the keys figures of neurological data collection is the advantage of continuous real-time measurement that allows collecting data continuously (Dimoka et al., 2010). In addition, this type of data collection, enables a level of precision, on a given period of time, permitting powerful time-series analysis and comparison (Loos et al., 2010). Applications of these types of data collection have been tested and conducted on various processes, for example on decision-making processes, understanding emotional processes (by capturing pleasure, enjoyment, displeasure, happiness, sadness, anxiety, sadness, disgust and etc.), understanding social processes (by capturing series of feelings, such as trust/distrust, cooperation/competition and etc.) and many more.

There are numerous opportunities provided by NeuroIS tools and its measurements in IS. According to Dimoka et al., (2010), these opportunities are illustrated as of the followings: 1) localize the various brain areas associated with IS constructs (neural correlates of IS constructs) and link them to the cognitive neuroscience literature to map IS constructs into specific brain areas, learn about the functionality of these brain areas, and better understand the nature and dimensionality of IS constructs. 2) Capture hidden (automatic and unconscious) mental processes (e.g. habits, ethics, deep emotions) that are difficult or even impossible to measure with existing measurement methods and tools. 3) Complement existing source of data with brain imaging data that can provide objective responses that are not subject to measurement biases (e.g., subjectivity bias, social desirability bias, common method bias). 4) Identify antecedents of IS constructs by examining how brain areas are activated in response to IT stimuli (e.g., designs, systems, websites) that intend to enhance certain outcomes (use behaviours, productivity). 5) Test consequences of IS constructs by showing whether, how, and why brain activation that is associated with certain IS constructs can predict certain behaviours (e.g., system use, online purchasing). 6) Infer causal relationships among IS constructs by examining the temporal order of brain activations (timing of

brain activity) stimulated by common IT stimulus that activates two or more IS constructs. 7) Challenge IS assumptions by identifying differences between existing IS relationships and the brain's underlying functionality, thus helping to build IS theories that correspond to the brain's functionality.

There are numerous tools in NeuroIS which enable to the point measurements. These tools, according to Dimoka et al. (Dimoka et al., 2010; Riedl et al., 2014) are categorized under neurophysiological tools and focus measurement tools. The examples are these tools are Eye Tracking, Skin Conductance Response (SCR), Facial Electromyography (eEMG), Electrocardiogram (EKG), Functional Magnetic Resonance Imaging (fMRI), Positron Emission Tomography (PET), and many more (Dimoka et al., 2010). As mentioned above, there are various advantageous of using these devices in order to conduct the research directly from the brain (body) of human. However, these devices are very expensive, and require extensive laboratory settings. Moreover, these experiments are conducted in artificial settings, and scholars might have validity concerns about whether neurophysiological data captured are the construct that they are intended to measure (Dimoka et al., 2010; Dimoka et al., 2007).

The Pop-Jordanov and Pop-Jordanova Quantum Consciousness Model

In the quantum approach to consciousness model, the brain elementary constituents are not the neurons and the other cells (which cannot be considered as quantum objects), but, in analogy with the quantum field theory approach to living matter (Del Giudice et al. 1985), they have been identified (Jibu & Yasue, 1995) with the vibrational electric dipole field of the water molecules and other biomolecules present in the brain, and with the NG bosons (called the dipole wave quanta) generated in the breakdown of the rotational symmetry of the electrical dipoles.

The description of the observed non-locality of brain functions, especially of memory storing and recalling, was the main goal of the quantum brain model proposed in the 1967 by Ricciardi and Umezawa (Ricciardi and Umezawa 1967). This model is based on the Quantum Field Theory of many body systems and its main ingredient is the mechanism of spontaneous breakdown of symmetry. Spontaneous symmetry breaking is a spontaneous process of symmetry breaking, by which a physical system in a symmetrical state ends up in an asymmetrical state.

In Quantum Field Theory the spontaneous breakdown of symmetry occurs when the dynamical equations are invariant under some group, say G , of continuous transformations, but the minimum energy state (the ground state or vacuum) of the system is not invariant under the full group G . When this occurs, the vacuum is an ordered state and massless particles (the Nambu-Goldstone bosons (NG) also called collective modes) propagating over the whole system are dynamically generated and are the carriers of the ordering information (long range correlations): order manifests itself as a global, macroscopic property which is dynamically generated at the microscopic quantum level (Vitiello 2003).

According to the model, memory recording is achieved under the action of external stimuli producing the breakdown of the continuous phase symmetry. In the quantum model of brain, it is thus imported all the machinery of the spontaneous breakdown of symmetry. The information storage function is thus represented by the coding of the ground state (the lowest energy state, or vacuum) through the coherent condensation of dipole wave quanta collective modes (Stuart et al. 1978). The non-locality of the memory is therefore derived as a dynamical feature rather than as a property of specific neural circuits, which would be critically damaged by destructive actions or by single neuron death or deficiency.

According to Pop-Jordanov & Pop-Jordanova (2010), based on their initial assumptions, the present quantum approaches to consciousness can be separated into four groups:

- Quantum emission probabilities (Eccles, 1986), where the two-way mental-neural interaction (with the electric/magnetic fields as a link) is supposed to be realized in a manner analogous to probability fields in quantum mechanics.
- Photon-corticon interaction (Jibu & Yasue, 1995), where consciousness was reduced to the creation and annihilation dynamics of photons (as quanta of an electromagnetic field) and corticons (as quanta of a rotational field of water dipoles) mechanics.
- Objective reduction in microtubules (Hameroff, 1998; Penrose & Hameroff, 1995), where quantum coherence occurs by exciting quasicrystalline water molecules as dipoles buried in microtubules.
- Virtual photons (Romijn, 2002), where the fleeting patterns of electric and magnetic fields, substituted by virtual photons, encode for conscious experiences.

Reviewing these approaches it can be inferred that, although being mainly conceptual and lacking numerical results, practically all of them have identified electric field and cortical dipoles as crucial elements of neural-mental correlation. With this in mind, the Pop-Jordanov and Pop-Jordanova Quantum Consciousness Model (2010) applies a field-dipole approach as a starting assumption.

Quantum Transitions Model

The transitions between the states of dipole water molecules as quantum rotators interacting with the time-dependent electric field have been studied recently, both analytically and numerically (Pop-Jordanov & Pop-Jordanova 2010). The corresponding nonstationary Schrödinger equation is not solvable analytically and it is too complicated for abinitio numerical calculation. Applying the adiabatic approach from the theory of atomic collisions, Pop-Jordanov & Pop-Jordanova (2010) proposes the solution in the following form:

$$\psi(\hat{d}, t) = \varphi_a(\hat{d}, F(wt)) e^{-\frac{i}{\hbar} \int E_a(F(wt)) dt}.$$

Where F is the electric field, \hat{d} is the direction of direction of the dipole vector, while φ_a are the eigenfunctions of the stationary Schrödinger equation. Adiabatic approximation requires the signal frequency to be much less than rotational frequency $\omega_{rot} = 10^{11}$ Hz, which is obviously fulfilled in the case of EEG frequency (Pop-Jordanov & Pop-Jordanova 2010). The periodic variation of the electric field $F = F_0 \sin(\omega t)$ leads to transitions with exponential probabilities as indicated in the formula below:

$$P_{ab} = e^{-\frac{2C_{ab}F_0}{F_0\omega}}.$$

Where a and b are sets of quantum numbers specifying the initial and the final state of the system, while C_{ab} is a parameter that depends on physical characteristics of the system (magnitude of the dipole and its moment of inertia). Thus, the probability of transition from one to another quantum energy state appears to be independent of the amplitude of the periodic external field, i.e., this mechanism is related to transition of information content rather than energy (Pop-Jordanov & Pop-Jordanova 2010).

the case of a system of N dipoles, each energy level splits into N sublevels (because of interaction between di-poles) with the distance between sublevels being approximately N-times smaller. Hence, the probability of transitions for such a system is (Pop-Jordanov P-Jordanova 2010).

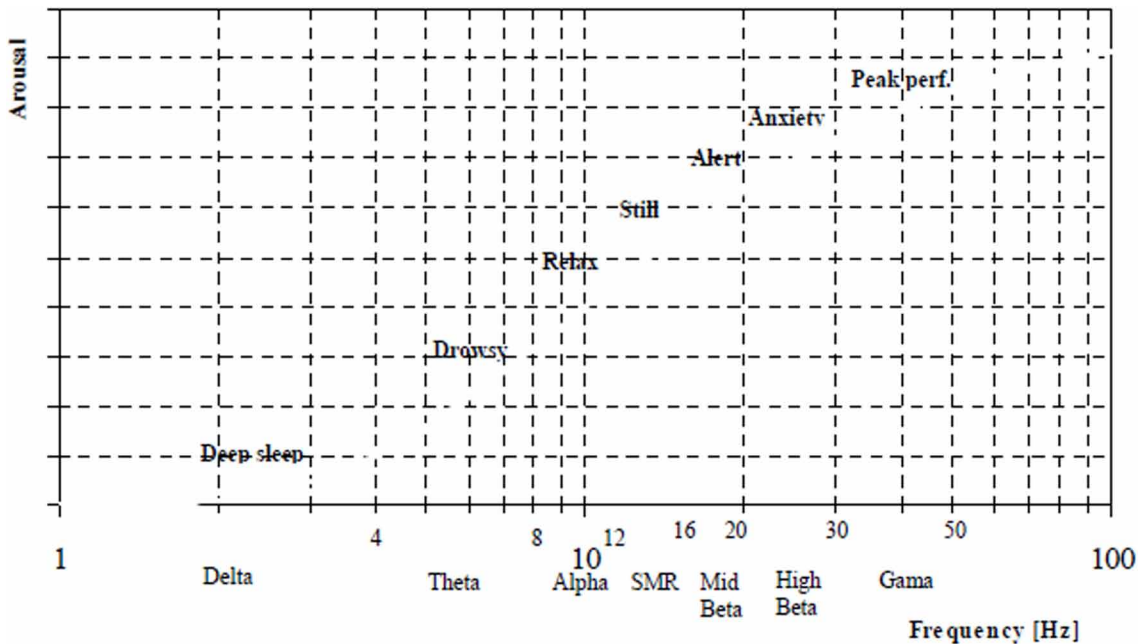
$$P_{ab} = e^{\frac{2C_{ab}}{Nw}}$$

The Correlation of the Quantum Transitions With Consciousness Level

Examine the eventual correlation of the transition probability P_{ab} with e probability of mental/neural excitations related to consciousness level (arousal), it is of interest to analyze the variation of P_{ab} with the spectral variable $f = w/2\pi$ for a neuron with $N = 10^{12}$ dipole molecules. This indicates that the arousal sensitivity to EEG frequency may be correlated to the transition probability variation for a system of quantum dipoles in the cortical electric field. The obtained theoretical result, suggesting the correlation of consciousness level with quantum transition probabilities, seems to be reasonable, since wakefulness can be conceived as a general activation, tonic state, and non-focused readiness to change the state, here identified as the probability of transitions between quantum states (Pop-Jordanov & Pop-Jordanova, 2009).

The basic dependence of mental arousal on EEG frequency, established empirically by Pop-Jordanov & Pop-Jordanova, (2005), is summarized in Figure 1 and establishes the level of consciousness that ranges from deep sleep, drowsy, relax, alert, anxiety and peak performance.

Figure 1. Mental arousal (Pop-Jordanov & Pop-Jordanova 2005)



A possible objection could be that mental acts cannot be reduced to one neuron. However, since only synchronized neurons of neuronal assemblies contribute to EEG, the relevant frequency is just the one-neuron (representative) frequency we are dealing with, when considering the consciousness level. The obtained formula connecting arousal (A) and field frequency (f) may be rewritten in the form:

$$P_{ab} = A = 2^{\frac{f_e}{f}}$$

Where the equilibrium frequency f_e actually corresponds to the dominant frequency with eyes closed, known to be age dependent – ranging from around 6 Hz to around 10 Hz, for children and adults, respectively (Thompson & Thompson, 2003).

The variable f , related to the dominant frequency band, can be identified as a spectrum weighted mean frequency (Pop-Jordanov & Pop-Jordanova, 2005). Characterizing the EEG spectrum, it may serve as a quantitative indicator of the general brain activation, and it is term as “brainrate” (in analogue to e.g. heart-rate). As such, it can contribute to the gross, initial assessment, not substituting the subtle, differential investigations of disorders corresponding to the same general level of arousal.

Being defined as the mean frequency of brain oscillations weighted over the all bands of the EEG potential (or power) spectrum, the brain-rate (f_b) may be calculated as:

$$f_b = \sum_i f_i P_i = \sum_i f_i \frac{V_i}{V}$$

With

$$V = \sum_i V_i$$

where the index i denotes the frequency band (for delta $i = 1$, for theta $i = 2$, etc.) and V_i is the corresponding mean amplitude of the electric potential. Following the standard five-band classification, one has $f_i = 2, 6, 10, 14$ and 18 , respectively.

Quantitative Electroencephalography

EEG technology generates raw data, this data can be broken into different frequencies (alpha, theta, etc) by using Fourier analysis. The Fourier analysis decomposes the EEG time series into a voltage by frequency spectral graph commonly called the “power spectrum”, with power being the square of the EEG magnitude, and magnitude being the integral average of the amplitude of the EEG signal, measured from (+) peak-to(-)peak, across the time sampled, or epoch. The epoch length determines the frequency resolution of the Fourier, with a 1-second epoch providing a 1 Hz resolution (plus/minus 0.5 Hz resolution), and a 4-second epoch providing $\frac{1}{4}$ Hz, or plus/minus 0.125 Hz resolution (Kececi & Degirmenci 2008). The Fourier equation to transform time dependent raw data can be defined by the equation below:

$$X(f) = \int_{-\infty}^{\infty} x(t) e^{-i2\pi ft} dt$$

ARCHITECTURE

The proposed architecture is mainly to support usability testing for a selected learning management system. Usability testing helps to determine how people use systems and where they may encounter difficulty of use (Valverde 2011).

Dumas and Redish (1999) identify five tasks must be completed for a usability test:

1. Define goals and concerns.
2. Determine who your test participants are.
3. Select, organize, and create test scenarios.
4. Determine to measure usability.
5. Prepare test materials.

In the first step of a usability test, goals are identified from the task analysis and quantitative usability goals for the LMS used for the study. For the second step, a sample of user should be selected. In the third step, test scenarios should be designed to detect potential usability problems. Test scenarios are normally prepared based on the HCI designer's experiences on what the user will do with the product (Valverde 2011).

Test scenarios should identify the activities to perform the tasks. The test case should number each task to complete it and provide a description for each task that is clear enough for the user to perform it. Each task should show the time it will take and the high-level instructions and procedures required to complete the task (Valverde 2011).

The fourth step of defining usability tests requires determining usability measures performance and subjective measures. Performance measures are quantitative measures of specific actions and behaviours that are observed during the test. The subjects performing the usability test will be wearing a EEG device as indicate in figure 2 in order to measure computer anxiety. The Quantum NeuroIS acquires de EEG signal and applies a Fourier analysis in order to brake the data into different frequencies (alpha, theta, etc) (figure 2). The different levels of power of the different frequencies is used to calculate a bit rate that is related to the dominant frequency band in the brain as an indicator of the main level of consciousness (Pop-Jordanov & Pop-Jordanova, 2005). The quantum level of arousal sensitivity is calculated based on the bit rate, this level of arousal is correlated to the consciousness level given its quantum transition probabilities (Pop-Jordanov & Pop-Jordanova, 2009). The brain rate and arousal level are used to establish a particular level of consciousness (deep sleep, drowsy, relax, alert, anxiety and peak performance) as indicated in figure 1.

The time taken to perform each task and task will be recorded as part of the usability test with a video camera that is part of the NeuroIS. This will help the researcher to log each time a user exhibits a certain behaviour during the test, like expressing frustration with a criterion for performance measures (Valverde 2011). The task time and actions are linked to a particular level of consciousness calculated by the NeuroIS and recorded in a permanent storage for further analysis (figure 2).

A Quantum NeuroIS Data Analytics Architecture for the Usability Evaluation of LMSs

The collected data from the NeuroIS are a video that records the different activities required to complete a set of tasks associated with a consciousness level that is intended to measure Computer Anxiety. It is expected that there is a linear relation between Computer Anxiety and Ease of Use and Computer Anxiety and Computer Self-Efficacy. The NeuroIS can produce two regression models with the collected data. The first regression will have Ease of Use as a dependent variable and Computer Anxiety as the independent variable. The model can be prepared with the Computer Anxiety measurements in terms of the different level of consciousness. The Ease of Use data that will be used for the regression model will be the log for the behaviour during the test with a four-point scale that evaluates the task from positive to negative ease of use (figure 2).

A second regression model will be produced with Computer Self-Efficacy (CSE) as dependent variable and Computer Anxiety as the independent variable. The CSE data will be computed by calculating the difference between the time taken to perform a task and the expected time to complete the task for each test. A lower CSE factor means a more efficient task while a higher factor means a less efficient task (figure 2).

Figure 2. Quantum NeuroIS data analytics architecture

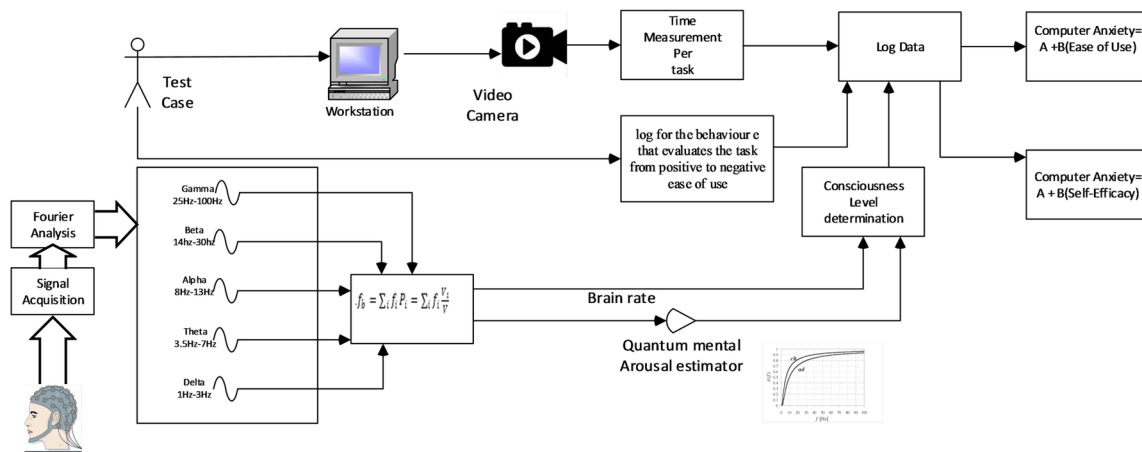


Figure 3 shows a prototype of the Quantum NeuroIS, the figure shows an image capturing the video recording of the user interacting with the LMS at a particular time on the top right. The first graph on the top displays the raw data collected from the EEG by displaying amplitude in time. The second graph is displaying the Power Spectrum of the raw data signal displaying the concentration of power over the different frequencies, the graph at the bottom displays the Gamma, Beta, Alpha, Theta and Delta signals that are the result of the Fourier analysis.

Test Results

A test was conducted with the prototype, an online course given at Concordia University in Introduction to Information Technology was used for the pilot test. Five users followed a usability test protocol for usability for about 15 minutes by using an EEG device and raw data was recorded for all the sessions.

Raw data was used to calculate dominant frequencies and arousal rates and videos were recorded for the sessions. The average of these results for the five students are given in Figure 4 and 5.

Figure 4 shows that dominant frequencies ranges from 18 Hz (Beta state) to 2 Hz (Delta state). It seems that some parts of the course caused stress and there were jumps of frequencies that go from very calm to stress. Videos need to be examined and change of frequencies would help to detect the areas that cause stress to users.

Figure 3. Quantum NeuroIS Prototype

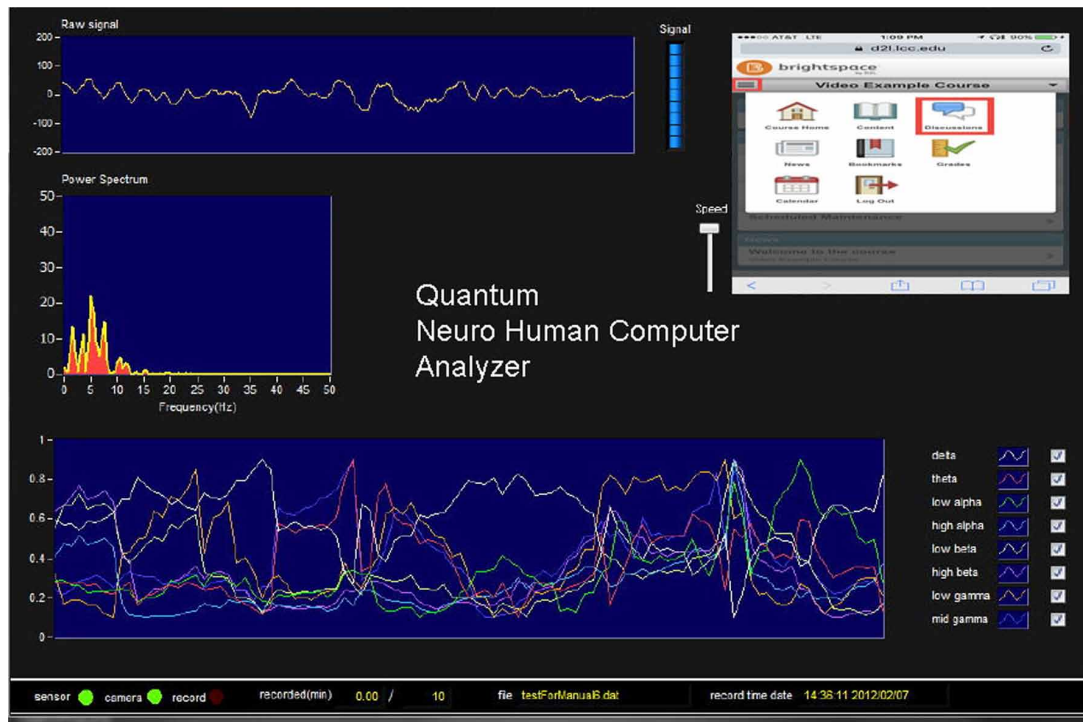


Figure 4. Dominant frequency

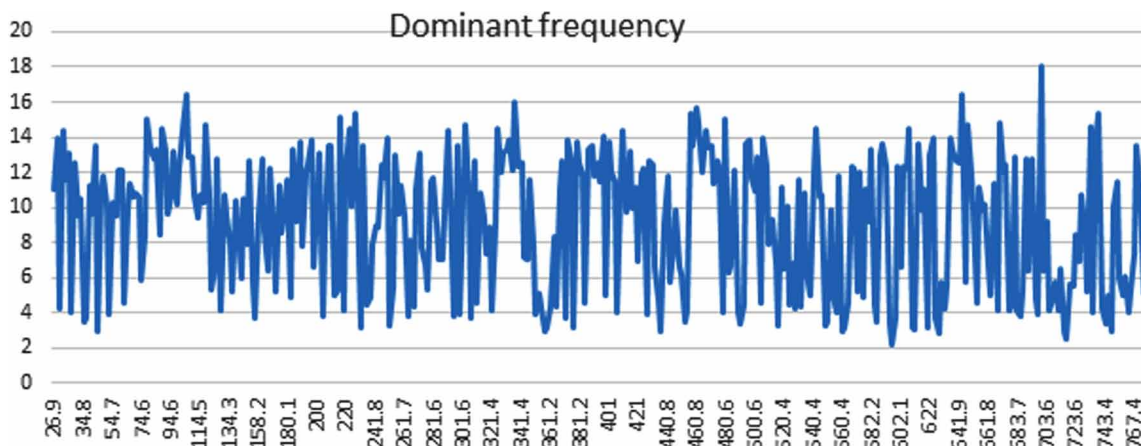
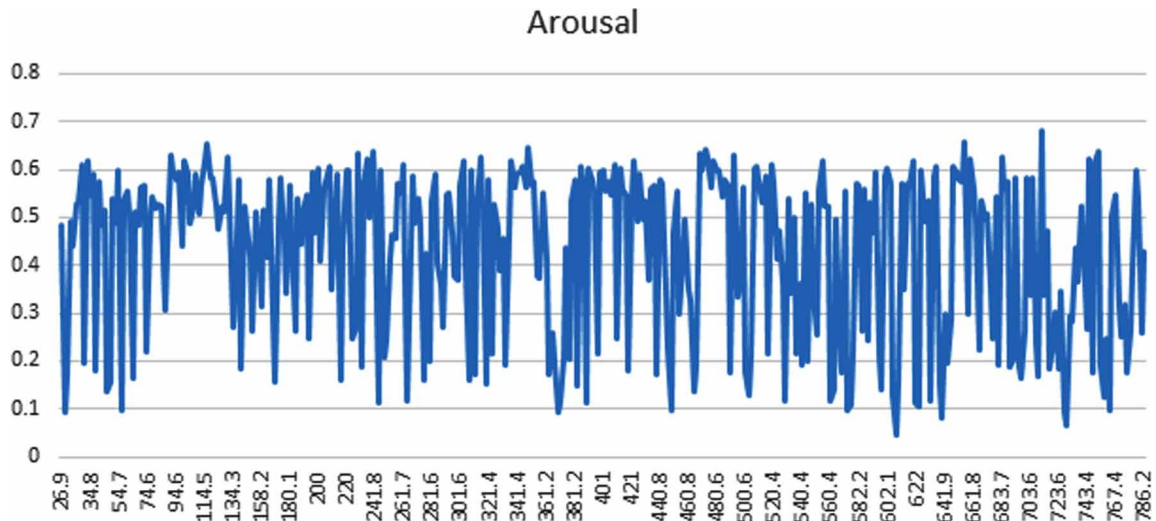


Figure 5 shows arousal rates. Arousal rates go from 0 to 1. A sudden jump in the arousal indicates a sudden change of state of consciousness that can indicate problems with the usability. Videos would need to be examined in order to detect the tasks that generated sudden changes of states as possible indication of problems with usability.

Figure 5. Arousal



CONCLUSION

The proposed NeuroIS is based on a quantum approach to measure consciousness proposed by Pop-Jordanov & Pop-Jordanova (2010), this model captures the levels of anxiety of the user from very relaxed to very stressed. An architecture with the different required components for the NeuroIS and the mathematics to make it work were identified. A software prototype with a possible interface was developed in order to show the feasibility of this architecture. A test with five students was performed in order to show the feasibility of the architecture and use in detecting problems with usability. The NeuroIS provides a tool for the measurement of computer anxiety can help to improve the usability of an LMS. The main advantage of the NeuroIS is that it does not use surveys for data collection and instead uses direct brain wave measurements from the user's brain. Future research should focus on the development of a software based on the proposed architecture for the validation of this design including the implementation of different usability tests for several LMS. In general, the research shows the potential of quantum consciousness research in the development of computer evaluation systems, quantum consciousness models can not only measure state of consciousness but also mental arousals that can detect changes of these states of consciousness. This type of models could have many other applications including NeuroIS for marketing and financial applications and any type of application that can benefit the with the measurement of consciousness and anxiety levels.

REFERENCES

- Ackroyd, S., & Hughes, J. A. (1981). *Data Collection in Context*. Longman.
- Chandler, K., & Hyatt, K. (2002). *Customer-Centered Design: A New Approach to Web Usability*. Prentice-Hall.
- Condon, C., & Valverde, R. (2014). Increasing Critical Thinking in Web-Based Graduate Management Courses. *Journal of Information Technology Education*, 13.
- Del Giudice, E., Doglia, S., Milani, M., & Vitiello, G. (1985). A quantum field theoretical approach to the collective behavior of biological systems. *Nucl Phys*, 375-400.
- Dimoka, A., Banker, R. D., Benbasat, I., Davis, F. D., Dennis, A. R., Gefen, D., & Pavlou, P. A. (2010). On the use of neurophysiological tools in IS research: Developing a research agenda for NeuroIS. *Management Information Systems Quarterly*, 36(3), 679–702.
- Dimoka, A., Pavlou, P. A., & Davis, F. D. (2007). Neuro-IS: The potential of cognitive neuroscience for information systems research. *Proceedings of the 28th International Conference on Information Systems*.
- Dimoka, A., Pavlou, P. A., & Davis, F. D. (2011). Research commentary-NeuroIS: The potential of cognitive neuroscience for information systems research. *Information Systems Research*, 22(4), 687–702. doi:10.1287/isre.1100.0284
- Dumas, J. S., & Redish, J. C. (1999). *A Practical Guide to Usability Testing*. Portland, OR: Intellect Books.
- Eccles, J. C. (1986). Do mental events cause neural events analogously to the probability fields of quantum mechanics? *Proceedings of the Royal Society of London. Series B, Biological Sciences*, 227(1249), 411–428. doi:10.1098/rspb.1986.0031 PMID:2873576
- Hameroff, S. (1998). *Quantum computation in brain microtubules? The Penrose-Hameroff' Orch OR' model of consciousness*. Philosophical Transactions-Royal Society of London Series A Mathematical Physical and Engineering Sciences.
- Jibu, M., & Yasue, K. (1995). *Quantum brain dynamics: An introduction*. Amsterdam: John Benjamins.
- Kak, S. (1995). On quantum neural computing. *Information Sciences*, 83(3-4), 143–160. doi:10.1016/0020-0255(94)00095-S
- Kalbach, J. (2007). *Designing Web Navigation*. O'Reilly Publications.
- Kececi, H., & Degirmenci, Y. (2008). Quantitative EEG and cognitive evoked potentials in anemia. *Neurophysiologie Clinique. Clinical Neurophysiology*, 38(2), 137–143. doi:10.1016/j.neucli.2008.01.004 PMID:18423335
- Loos, P., Riedl, R., Müller-Putz, G. R., Vom Brocke, J., Davis, F. D., Banker, R. D., & Léger, P.-M. (2010). NeuroIS: Neuroscientific approaches in the investigation and development of information systems. *Business & Information Systems Engineering*, 2(6), 395–401. doi:10.1007/12599-010-0130-8

- Masuyama, N., Loo, C. K., Seera, M., & Kubota, N. (2017). Quantum-Inspired Multidirectional Associative Memory With a Self-Convergent Iterative Learning. *IEEE Transactions on Neural Networks and Learning Systems*, 1–11. doi:10.1109/TNNLS.2017.2653114 PMID:28182559
- Pedersen, M. K., Skyum, B., Heck, R., Müller, R., Bason, M., Lieberoth, A., & Sherson, J. F. (2016). Virtual learning environment for interactive engagement with advanced quantum mechanics. *Physical Review Physics Education Research*, 12(1), 013102. doi:10.1103/PhysRevPhysEducRes.12.013102
- Pop-Jordanov, J., & Pop-Jordanova, N. (2010). Quantum transition probabilities and the level of consciousness. *Journal of Psychophysiology*, 24(2), 136–140. doi:10.1027/0269-8803/a000025
- Pop-Jordanova, N., & Pop-Jordanov, J. (2005). Spectrum-weighted EEG frequency (“brain-rate”) as a quantitative indicator of mental arousal. *Prilozi Makedonska Akademija na Naukite i Umetnostite*, 26(2), 35–42. PMID:16400227
- Popper, K. (2004). *The Logic of Scientific Discovery* (2nd ed.). Routledge, Taylor & Francis. (originally published 1959)
- Ricciardi, L. M., & Umezawa, H. (1967). Brain physics and many-body problems. *Kibernetik*, 4(2), 44–48. doi:10.1007/BF00292170 PMID:5617419
- Riedl, R., Davis, F. D., & Hevner, A. R. (2014). Towards a NeuroIS research methodology: Intensifying the discussion on methods, tools, and measurement. *Journal of the Association for Information Systems*, 15(10), I.
- Saadé, R. G., & Kira, D. (2009). Computer anxiety in e-learning: The effect of computer self-efficacy. *Journal of Information Technology Education*, 8(1), 177–191. doi:10.28945/166
- Schuld, M., & Petruccione, F. (2014). *The quest for a Quantum Neural Network*. QNN Research.
- Schuld, M., Sinayskiy, I., & Petruccione, F. (2014). The quest for a quantum neural network. *Quantum Information Processing*, 13(11), 2567–2586. doi:10.1007/11128-014-0809-8
- Stuart, C. I. J., Takahashi, Y., & Umezawa, H. (1978). On the stability and non-local properties of memory. *Journal of Theoretical Biology*, 71(4), 605–618. doi:10.1016/0022-5193(78)90327-2 PMID:661325
- Thompson, M., & Thompson, L. (2003). *The neurofeedback book: An introduction to basic concepts in applied psycho-physiology*. Wheat Ridge, CO: Association for Applied Psychophysiology & Biofeedback.
- Valverde, R. (2011). *Principles of Human Computer Interaction Design: HCI Design*. LAP Lambert Academic Publishing.
- Valverde, R. (2015). Neurotechnology as a Tool for Inducing and Measuring Altered States of Consciousness in Transpersonal Psychotherapy. *NeuroQuantology: An Interdisciplinary Journal of Neuroscience and Quantum Physics*, 13(4). doi:10.14704/nq.2015.13.4.870
- Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, 46(2), 186–204. doi:10.1287/mnsc.46.2.186.11926
- Vitiello, G. (2003). Quantum dissipation and information: A route to consciousness modeling. *NeuroQuantology: An Interdisciplinary Journal of Neuroscience and Quantum Physics*, 1(2).

A Quantum NeuroIS Data Analytics Architecture for the Usability Evaluation of LMSs

Wang, J., Yan, N., Liu, H., Liu, M., & Tai, C. (2007). Brain-computer interfaces based on attention and complex mental tasks. *Digital Human Modeling*, 467-473.

Yasue, K., Jibu, M., Misawa, T., & Zambrini, J. C. (1988). Stochastic neurodynamics. *Annals of the Institute of Statistical Mathematics*, 40(1), 41–59. doi:10.1007/BF00053954

This research was previously published in Quantum-Inspired Intelligent Systems for Multimedia Data Analysis; pages 277-299, copyright year 2018 by Engineering Science Reference (an imprint of IGI Global).

Chapter 21

An Efficient Handwritten Character Recognition Using Quantum Multilayer Neural Network (QMLNN) Architecture: Quantum Multilayer Neural Network

Debanjan Konar

Sikkim Manipal Institute of Technology, India

Suman Kalyan Kar

Sikkim Manipal Institute of Technology, India

ABSTRACT

This chapter proposes a quantum multi-layer neural network (QMLNN) architecture suitable for handwritten character recognition in real time, assisted by quantum backpropagation of errors calculated from the quantum-inspired fuzziness measure of network output states. It is composed of three second-order neighborhood-topology-based inter-connected layers of neurons represented by qubits known as input, hidden, and output layers. The QMLNN architecture is a feed forward network with standard quantum backpropagation algorithm for the adjustment of its weighted interconnection. QMLNN self-organizes the quantum fuzzy input image information by means of the quantum backpropagating errors at the intermediate and output layers of the architecture. The interconnection weights are described using rotation gates. After the network is stabilized, a quantum observation at the output layer destroys the superposition of quantum states in order to obtain true binary outputs.

DOI: 10.4018/978-1-7998-8593-1.ch021

INTRODUCTION

Owing to wide variations in writing styles, variations in sizes and orientation of the handwritten characters, recognition of characters remains an uphill task in computer vision and pattern recognition community. Numerous image processing applications are relying on the techniques of identification and recognition of characters from real-life applications of text documents and images. The primary objective of handwritten character recognition lies in the conversion of characters present in an image into character codes pertaining to text and image processing. Artificial Neural Networks (ANN) often offers to solve unorganized machine learning problems like associative pattern recognition tasks, image processing tasks in parallel processing mode. Basic feed forward ANN is employed by many computer vision researchers to solve pattern recognition problems with high time complexity. The character recognition problem can be solved using various feature selection techniques and neural network classifiers. The significant contributions of feed forward ANNs assisted by back-propagation algorithms in character recognition problems deserves special mention (Devireddy, 2005). The Bayesian Network classifiers (Bouchain, 2007; Bonci et al, 2006) are one of the most suitable probabilistic approach for recognition of characters. In handwritten character recognition, high recognition accuracy can be obtained using back-propagation learning algorithm in multilayer neural network architectures.

A Hidden Markov Model (HMM) based approach is proposed by Kundu and Chen (2002) achieved 88% recognition accuracy working with 100 postal words. Tomoyuki *et al.* (2002) also achieved 80% recognition accuracy in experiment while considering 1646 city names of Europe as data sets. A K-NN classifier has been employed by Gatos et al. (2006) to recognize 3799 words from IAM database which yields 81% accuracy. A plethora of supervised artificial neural networks (Samadiani et al, 2005; Chi et al, 1995) have been suggested to obtain real time results. In addition, numerous neighborhoods based supervised neural network architectures have been entrusted upon for pattern recognition and it has been found efficient in recognizing handwritten characters. However, owing to interconnection weight adjustments using standard back-propagation algorithms in these supervised network architectures, the time complexity increases manifold. Efforts have been made to combine quantum computing with the standard back-propagation algorithm resulting in time efficient network architectures.

Micro-quantum level effects offer to perform computational tasks using time effect procedures in Quantum computing and also outperform the classical computing approaches in terms of computational time (Mcmohan, 2008). The popularity of artificial neural network combined with quantum computing is growing in leaps and bounds due to implied parallelism offered by quantum computing. An array of quantum dots -assisted Quantum Neural Network (QNN) architecture is proposed by Behrman *et al.* (1994). Matsui *et al.* (2000) also projected a quantum multilayer feed forward neural network model referred as QNN using quantum learning technique. Quantum associative memory (Ventura et al, 2000; Perus, 1998) and neural network quantum dots (Behramam 1994) are the basic components of QNN research. An automated pattern recognition algorithm is proposed by Aytekin *et al.* (2013) guided by the principle of quantum mechanics. A novel model of QNN is also suggested by Ezhov (2001) to solve classification problems. Moreover, quantum back-propagation based neural network architecture is introduced in (2013) to encounter the pattern recognition tasks.

In this chapter, a time efficient novel quantum inspired neural network architecture referred to as Quantum Multilayer Neural Network architecture (QMLNN) for handwritten character recognition has been proposed. The novelty of the proposed QMLNN lies in the fact that learning and classification can be performed simultaneously. The QMLNN architecture comprises of *qubits* and rotation gates. This

architecture is composed of an input, an intermediate and an output layer of neurons in quantum environment. The input information as *qubits* are feed forwarded from input layer to intermediate layer and output layer. It also counter propagates its network states from output to intermediate layer. The interconnected weights are adjusted using quantum back-propagation algorithm illustrated below. The standard sigmoid activation function is employed to characteristic activation through the quantum cardinality estimates of 8-connected neighborhoods pixels. The performance of the proposed QMLNN architecture is focused on the time efficiency and recognition accuracy from noisy handwritten characters, as compared to the classical MLNN (Devireddy et al, 2005; Matan et al, 1990; Patil et al, 2011).

LITERATURE SURVEY

In the field of pattern recognition and machine learning, the problem of recognition of handwritten characters has gained much attention. With growing popularity and requirement for office automation, it has become to provide effective and real time solutions (Rahman et al, 2005; Dineshkumar et al, 2005; Samadiani et al, 2015). However, owing to wide variations in structural, topological and statistical information do not assist in handwritten character recognition (Shelke et al, 2011). Self Organizing Feature Map (SOM) neural network based method suggested by Najmeh Samadiani *et al.* for recognition of printed English characters (Samadiani et al, 2015) received much attention. The contribution of integrated neural network for feature extraction task of alpha alphanumeric characters has been projected by using Junchuan Yang *et al.* (2012). Several pattern recognition approaches have been reported in this paper with improved accuracy. The contribution of pattern transformations and additive input noise annealing approach for handwritten character recognition proposed by J.M. Alonso-Weber *et al.* (2014) is also notable. In this paper, the proposed combined approach achieved less than 0.43% test error while compared with Convolution Neural Network and Deep Learning Neural Networks. Handwritten character recognition in Marathi language has been proposed by Amitkumar Shinde *et al.* (2015) incorporating forty-six Marathi sign language alphabets and 500 words of sign language. The some work based on fuzzy model based handwritten number recognition proposed by O.V. Ramana Murthy *et al.* (2007) contributed fuzzy model based handwritten character recognition which deals with number detection of both Hindi and English numerals. In this fuzzy logic based model, fuzzy exponential membership functions, suitable for deriving character features, are modified.

In the field of online handwritten character recognition, the combination of Hidden Markov Model (HMM) and dynamic programming has contributed significantly for cursive handwritten character recognition (Sin et al, 1999).

In the last decade, Artificial Neural Network (ANN) has gained huge popularity in research areas such as pattern recognition and machine learning. The simplified ANN could not match with the rising demands of volume of data and complexity of information. The large scale of data and complexity, therefore lead to the construction of more complex hybridized ANN with more biological and physical features and mathematical basics (Cheng et al, 2006). One of the notable examples in this direction is Quantum Neural Networks (QNN), a hybridization of quantum computation and neural networks. Perus proposed a QNN which draws much attention in international research community. In addition, multi-universe theory of quantum mechanics has been introduced by Menneer and Narayanan, which deals with neural network training and the superposition of the networks to construct the complete network. An array of quantum dots -assisted Quantum Neural Network (QNN) architecture is proposed by

Behrman *et al.* (1994). According to quantum mechanics, the suggested system is evolved in real-time by incorporating single quantum dot molecule for every input neuron. The hidden layer neurons are presented as different time interval. Therefore, the number of hidden neurons is directly proportional to measures applied to the time pieces. In recent times, there are wide applications of QNN, which includes the Quantum Associative Memory (QAM) (Ventura *et al.*, 200; Perus 1998), the quantum competition learning (Pylkkänen *et al.*, 1995), quantum dots associated neural network (Behrman 1996), quantum Hopfield networks and quantum transform function. Neural networks, which are constituted by quantum gated nodes, facilitate features of biological systems more efficiently than their classical counterparts (Shafee, 2007). Recently, a quantum back-propagation algorithm based neural model (Li *et al.*, 2008) has been proposed and the quantum back-propagation learning algorithm is completely relying on single-*qubit* rotation gate and two-*qubit* controlled-NOT gates.

Quantum Computing Concepts

Quantum mechanics and quantum algorithms are two basic components exploited in the field of soft computing research. Quantum mechanical operations like superposition, entanglement (Shor, 1994) are applied on them. The efficacy of quantum computing over classical computation has thrown open new horizons in current developments. Quantum factoring problem is one of the notable examples in this direction using a polynomial type RSA-129 algorithm over classical factoring problem and it has been found that quantum factoring problem can be solved in few seconds (Grover, 1996). A quantum algorithm for data base search is developed by Grover (1996) whose time complexity was reduced to $O(\sqrt{n})$. Both proposed quantum algorithms are guided by inherent parallelism offered by quantum computing. In order to gain maximum parallelism in quantum computing, a superposition procedure is followed on all inputs to obtain suitable possible outputs. The primary disadvantage with this superposition approach is that parallelism fails due to the unavailability of all possible outputs once quantum observation is performed.

Deutsch first developed true Quantum Turing Machine (QTM) (Nielson *et al.*, 2000), draws significant features in quantum computing. This novel feature has turned out to be the key to most successful quantum algorithms. The following subsections merely review the basic concepts of quantum computation.

Concept of Qubits

In quantum computing basic building block is a quantum bit or *qubit* (Mcmohan, 2008) for processing of information. The linear superposition of dual eigenstates $|0\rangle$ and $|1\rangle$ constitutes a qubit in quantum computer. It is defined as

$$|\rho\rangle = a|0\rangle + b|1\rangle \quad (1)$$

The probabilities for occurrence of $|0\rangle$ and $|1\rangle$ are $|a|^2$ and $|b|^2$ respectively where, a and b are complex numbers and subjected to normalization constraint

$$|a|^2 + |b|^2 = 1 \quad (2)$$

An Efficient Handwritten Character Recognition Using QMLNN Architecture

The quantum logic gates are implemented on Hilbert space using various linear and unitary operations (Aytekin et al, 2013).

Single Qubit Rotation Gate

Updation of single *qubit* is done using a rotation gate is as follows

$$\begin{bmatrix} a' \\ b' \end{bmatrix} = \begin{bmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} \quad (3)$$

A *qubit* (a, b) is modified to (a', b') using single qubit rotation gate with a rotation angle α .

Quantum Observation

A postulate of quantum mechanics (Feynman et al, 1965; Mu et al, 2013) states that “if a coherent or linearly superposed system interacts with its environment, then on measurement, the superposition is destroyed”. A quantum system, μ containing quantum states, $|\rho_i\rangle$ exists in a Hilbert space and is defined as

$$|\mu\rangle = \sum_{j=1}^p d_j |\rho_j\rangle \quad (4)$$

The coherence of basic states $|\rho_i\rangle$ forms $|\mu\rangle$. The quantum system $|\mu\rangle$ is observed in the state $|\rho_i\rangle$ and the occurrence of $|\mu\rangle$ measured using probability with amplitude $|d_j|^2$ where d_j is the complex coefficient.

Quantum Multilayer Neural Network (QMLNN) Architecture

The information processing neurons in QMLNN architecture are composed of *qubits*. There are three layers of neurons namely the input, intermediate and output layers which are described by *qubit* representation. The following matrices are used to illustrate all three layers.

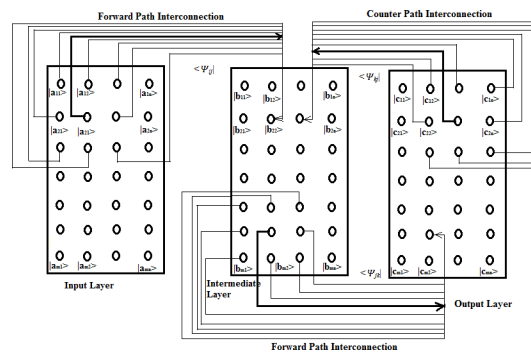
$$\text{Input layer} \begin{bmatrix} |x_{11}\rangle & \dots & |x_{1n}\rangle \\ |x_{21}\rangle & \dots & |x_{2n}\rangle \\ \dots & \dots & \dots \\ \dots & \dots & \dots \\ |x_{m1}\rangle & \dots & |x_{mn}\rangle \end{bmatrix}$$

$$\text{Intermediate layer} \begin{pmatrix} |y_{11}\rangle & \dots & |y_{1n}\rangle \\ |y_{21}\rangle & \dots & |y_{2n}\rangle \\ \dots & \dots & \dots \\ \dots & \dots & \dots \\ |y_{m1}\rangle & \dots & |y_{mn}\rangle \end{pmatrix}$$

$$\text{Output layer} \begin{pmatrix} |z_{11}\rangle & \dots & |z_{1n}\rangle \\ |z_{21}\rangle & \dots & |z_{2n}\rangle \\ \dots & \dots & \dots \\ \dots & \dots & \dots \\ |z_{m1}\rangle & \dots & |z_{mn}\rangle \end{pmatrix}$$

The network inputs in terms of quantum bits are fed into the input layer of QMLNN architecture which acts like a switching layer. The input layer of QMLNN architecture accepts image information as *qubits* and propagated to the hidden layer for further processing.

Figure 1. Quantum Multilayer Neural Network (QMLNN) architecture (Intra-layer connections are not shown for clarity). (Konar et. al, 2016)



The 8-connected neighborhood based neurons of all three layers are accumulated at the seed neuron of next subsequent layer and stored as quantum information through interconnected strengths.

There are twofold techniques for inter-layer connections introduced in this presented QMLNN architecture. The rotation gates have been employed to set inter-connection weights between the adjacent layers of corresponding neurons. The relative measure of quantum bits at the constituent neurons of each layer of QMLNN architecture determines the angle of rotation for rotation gates. Figure 1 illustrates the architecture of QMLNN. The sigmoid function governs the activations of the constituent neurons of the intermediate and the output layer, is one of the salient features of the network. The counter propagation of intermediate states in terms of *qubits* are transformed in to outputs at back propagation layer of the QMLNN architecture.

Network Operation Using Quantum Back-Propagation Algorithm

The novelty of the proposed algorithm lies in the fact that learning and classification can be performed simultaneously. The input handwritten image pixel informations are received at the switching or input layer of QMLNN architecture and input binary values [0, 1] are converted into the quantum phase [0, $\pi/2$].

$$q_j = \frac{\pi}{2} b_j \tag{5}$$

where, q_i is quantum bits and b_i is the binary information.

Qubits have been employed to present the interconnected weights and activation values are presented in QMLNN architecture. The angle of rotation and activation are expressed as α and ρ respectively where

$$\langle \rho | = \begin{bmatrix} \cos \phi \\ \sin \phi \end{bmatrix} \tag{6}$$

The constituent neurons of each adjacent layer of QMLNN architecture are associated through input-output (Konar et al, 2015; Konar et al, 2016) as

$$\hat{a}q_l = gsig \left(\sum_{j=1}^p b_j \hat{\mu}_{jl} \right) \rho_k \tilde{n} = gsig (b_j c_o s(\alpha_j - \phi)) \tag{7}$$

where q is the true outcome, μ_j is interconnection weight and $gsig$ is the standard sigmoid function defined as

$$gsig (y) = \frac{1}{1 + e^{-y}} \tag{8}$$

The single *qubit* rotation gate has been employed to suitably set inter-layer interconnection weights and the activation values using the following process.

$$|\mu (i+1)\tilde{n}\rangle = \begin{bmatrix} \cos ' \alpha & -\sin ' \alpha \\ \sin ' \alpha & \cos ' \alpha \end{bmatrix} |\mu (i)\tilde{n}\rangle \tag{9}$$

$$|\eta (i+1)\tilde{n}\rangle = \begin{bmatrix} \cos ' \beta & -\sin ' \beta \\ \sin ' \beta & \cos ' \beta \end{bmatrix} |\eta (i)\tilde{n}\rangle \tag{10}$$

where $\alpha(i+1) = \alpha(i) + \delta\alpha_i (1_i)$

$$\beta(i+1) = \beta(i) + \delta\beta_i \tag{12}$$

If \bar{q} and q are target normalized output and real output respectively then, the network error function is defined as follows:

$$\text{Err} = (\bar{q} - q)^2 \frac{1}{2} \tag{13}$$

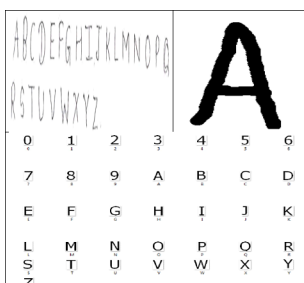
The real outputs are obtained after quantum measurement of each quantum states and the network is stabilized once the error *Err* is achieved tolerable limit.

EXPERIMENTAL RESULTS AND DISCUSSIONS

The proposed QMLNN and its classical counterpart Classical Multilayer Neural Network (CMLNN) have been trained and classified with exactly 50 samples of each character image of size 32 x 32. During learning and classification procedure, the characters with lowest error value at the output layer with the input handwritten image have been considered for classification. The overall average classification accuracy found to be very promising and it is above 88%.

In the proposed handwritten character recognition experiment, the QMLNN network has been tested by each of the 26 characters 50 times i.e. 1300 (50× 26=1300) character image samples from the database has been involved in the learning process. Input handwritten characters and target output images are provided in Figure 2.

Figure 2. Original Input and Target Images



The efficacy of the proposed QMLNN over classical MLNN has been reported in Table 1 and Table 2. The comparative result reflects the superiority of the QMLNN with its classical counterpart in terms of recognition accuracy and time complexity. In order to match the true output with the target normalized image, the percentage of correct classification pixels (pcc) is evaluated as:

$$pcc = tcc / tnp * 100 \tag{14}$$

An Efficient Handwritten Character Recognition Using QMLNN Architecture

where tcc and tnp denotes the total number of pixels matched with target output and the total number of pixels on an image.

Table 1. Comparative performance results of QMLNN and CMLNN

English Characters	QMLNN		CMLNN	
	t (secs)	% of Accuracy	t (secs)	% of Accuracy
C	8.666	89.0328	10.533	88.0017
A	8.026	89.4966	10.501	79.3338
E	8.060	69.2785	10.102	63.8994
1	8.406	94.0380	10.323	84.5355
2	8.647	93.5917	10.302	89.0240
3	8.127	92.7813	10.312	88.9866

Table 2. Comparative performance results of QMLNN and CMLNN

English Characters	QMLNN		CMLNN	
	t (secs)	% of Accuracy	t (secs)	% of Accuracy
X	8.216	91.8043	10.372	88.8154
Y	8.526	87.7326	10.249	84.8165
Z	8.316	88.4941	10.934	85.1285
8	8.607	84.9063	10.372	84.5345
7	8.286	82.3846	10.891	79.9292
9	8.086	80.4917	10.133	78.7587

CONCLUSION

This chapter illustrates an efficient quantum back propagation algorithm refereed as Quantum Multi-layer Neural Network (QMLNN) architecture for handwritten character recognition in real-time. The quantum version of classical Multilayer neural network (MLNN) architecture assisted by back-propagation algorithm has been proposed in this work. The novelty of suggested network architecture lies in its functioning and its operations.

The basic components used in the suggested QMLNN architecture are designated by qubits for each constituent processing node and in order to reduce computation time of the back-propagation algorithm rotation gates have been employed. The weighted interconnections between different layers are also represented using *qubits* and quantum thresholding have been incorporated to propagate quantum fuzzified information. At the output layer of the proposed network QMLNN, a quantum measurement is performed to obtain the true output (Recognized Characters) by changing the quantum bits or states into 0's and 1's according to the probability.

The effectiveness of the suggested network architecture is established using comparative analysis of the results as far as the quality of extracted output images are concerned and recognition time over

the classical MLNN. In addition, the future direction of research of suggested QMLNN is aiming for recognition of handwritten characters using self-supervised neural network architecture. Currently, the authors are engaged in this new paradigm of research.

REFERENCES

- Alonso-Weber, J. M., Sesmero, M. P., & Sanchis, A. (2014). Combining additive input noise annealing and pattern transformations for improved handwritten character recognition. Elsevier.
- Aytekin, C., Kiranyaz, S., & Gabbouj, M. (2013). Quantum Mechanics in Computer Vision: Automatic Object Extraction. *Proc. ICIP 2013*, 2489–2493. doi:10.1109/ICIP.2013.6738513
- Behraman, E. (1994). A quantum dot neural network. *Proc. Workshop on Physics of Computation*, 22–24.
- Bhattacharyya, S., Pal, P., & Bhowmick, S. (2014). Binary Image Denoising Using a Quantum Multilayer Self Organizing Neural Network. *Applied Soft Computing*, 24, 717–729. doi:10.1016/j.asoc.2014.08.027
- Bonci, A., Leo, T., & Longhi, S. (2005). A Bayesian approach to the Hough transform for line detection. *IEEE Trans. Systems Man Cybernet., Part A. Syst. Humans*, 35(6), 945–955. doi:10.1109/TSMCA.2005.853481
- Bouchain, D. (2007). *Character Recognition Using Convolutional Neural Networks*. Seminar Statistical Learning Theory University of Ulm, Germany Institute for Neural Information Processing.
- Cheng, J. L., Feng, D. H., & Liu, F. (2006). *Immune Optimization Computation, Learn and Recognition*. Beijing: Science Press.
- Chi, Z., Wu, J., & Yan, H. (1995). Handwritten numeral recognition using self-organizing maps and fuzzy rules. *Pattern Recognition*, 28(1), 59–66. doi:10.1016/0031-3203(94)00085-Z
- Deutsch, D. (1985). Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer. *Proceedings of the Royal Society of London, A400(1818)*, 97–117. doi:10.1098/rspa.1985.0070
- Devireddy, S., & AppaRao, S. (2005). Hand Written Character Recognition Using Back Propagation Network. *Journal of Theoretical and Applied Information Technology*, 257-269.
- Dineshkumar, R., & Suganthi, J. (2015). Sanskrit Character Recognition System using Neural Network. *Indian Journal of Science and Technology*, 8(1), 65–69. doi:10.17485/ijst/2015/v8i1/52878
- Ezhov, A. A. (2001). Pattern Recognition with Quantum Neural Networks. *Proc. Advances in Pattern Recognition ICAPR:2001*, 60–71.
- Feynman, R. P., Leighton, R. B., & Sands, M. (1965). *The Feynman Lectures on Physics* (Vol. 3). Addison-Wesley Publishing Company.
- Gatos, B., Pratikakis, I., & Perantonis, S. J. (2006). Hybrid off-line cursive handwriting word recognition. *Proceedings of 18th international conference on pattern recognition (ICPR'06)*, 2, 998–1002. doi:10.1109/ICPR.2006.644

An Efficient Handwritten Character Recognition Using QMLNN Architecture

- Grover, L. (1996). A Fast Quantum Mechanical Algorithm for Database Search. *Proc. 28th Annual ACM Symposium on the Theory of Computing*, 212–221. 10.1145/237814.237866
- Hanmandlu, M., & Ramana Murthy, O. V. (2007). Fuzzy model based recognition of handwritten numerals. *Pattern Recognition*, 40, 1840 – 1854.
- Konar, D., Bhattachrayya, S., Das, S., & Panigrahi, B. K. (2015). A quantum bi- directional self-organizing neural network (QBDSOINN) for binary image denoising. *Proc. ICACCI*, 54-68. 10.1109/ICACCI.2015.7275780
- Konar, D., Bhattachrayya, S., Panigrahi, B. K., & Nakamatsu, K. (2016). Quantum bidirectional self-organizing neural network (QBDSOINN) architecture for binary object extraction from a noisy perspective. *Applied Soft Computing*, 46, 731–752. doi:10.1016/j.asoc.2015.12.040
- Kundu, Y. H., & Chen, M. (2002). Alternatives to variable duration HMM in handwriting recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 20(11), 1275–1280. doi:10.1109/34.730561
- Li, C. P., & Li, S. Y. (2008). Learning algorithm and application of quantum BP neural networks based on universal quantum gates. *Journal of Systems Engineering and Electronics*, 19(1), 167–174. doi:10.1016/S1004-4132(08)60063-8
- Matan, O. (1990). Handwritten Character Recognition Using Neural Network Architecture. *Proceedings of the 4th USPS Advanced Technology Conference*, 1003-1011.
- Matsui, N., Takai, M., & Nishimura, H. (2000). A network model based on qubit-like neuron corresponding to quantum circuit. *Inst. Electr. Inform. Commun. Jpn. (Part III: Fundam. Electr. Sci)*, 83(10), 67–73.
- Mcmohan, D. (2008). *Quantum Computing Explained*. Hoboken, NJ: John Wiley & Sons, Inc.
- Mu, D., Guan, Z., & Zhang, H. (2013). Learning Algorithm and Application of Quantum Neural Networks with Quantum Weights. *IJCTE*, 5, 788–792. doi:10.7763/IJCTE.2013.V5.797
- Mu, D., Guan, Z., & Zhang, H. (2013). *Learning Algorithm and Application of Quantum Neural Networks with Quantum Weights* (Vol. 5). IJCTE.
- Nielson, M. A., & Chung, I. L. (2000). *Quantum computation and quantum information*. Cambridge University Press.
- Perus, M., & Ecimovic, P. (1998). Memory and pattern recognition in associative neural networks. *International Journal of Applied Science and Computation*, 4, 283–310.
- Perus, M., & Ecimovic, P. (1998). Memory and pattern recognition in associative neural networks. *International Journal of Applied Science and Computation*, 4, 283–310.
- Pyllkkanen, P., & Pylkko, P. (1995). New directions in cognitive science. *Proc. the International Symposium*, 77-89.
- Rahman, M., Akhand, M. A. H., Islam, S., & Shill, P. S. (2005). *Bangla Handwritten Character Recognition using Convolutional Neural Network*. I.J. Image, Graphics and Signal Processing.

Samadiani, N., & Hassanpour, H. (2005). *A neural network based approach for recognizing Multi-font printed English characters*. Academic Press.

Samadiani, N., & Hassanpour, H. (2015). *A neural network based approach for recognizing Multi font printed English characters*. Academic Press.

Shafee, F. (2007). Neural networks with quantum gated nodes. *Engineering Applications of Artificial Intelligence*, 20(4), 429–437. doi:10.1016/j.engappai.2006.09.004

Shelke, S., & Shaila, A. (2011). A Multistage Handwritten Marathi Compound character recognition scheme using Neural Networks and Wavelet Features. *International Journal of Signal Processing, Image Processing and Pattern Recognition*, 4.

Shinde, A., & Kagalkar, R. (2015). Sign Language to Text and Vice Versa Recognition using Computer Vision in Marathi. *International Journal of Computers and Applications*, 23–28.

Shor, P. W. (1994). Algorithms for Quantum Computation: Discrete Logarithms and Factoring. *Proc. 35th Annual Symposium on the Foundation of Computer Science*, 20-22. 10.1109/SFCS.1994.365700

Sin, B.-K., & Ha, J.-Y. (1999). Network-Based Approach to Online Cursive Script Recognition. *IEEE Transactions on Systems, Man, and Cybernetics. Part B, Cybernetics*, 29(2), 321–328. doi:10.1109/3477.752808 PMID:18252307

Tomoyuki, H., Takuma, A., & Bunpei, I. (2007). An analytic word recognition algorithm using a posteriori probability. *Proceedings of the 9th international conference on document analysis and recognition*, 2, 669–673.

Ventura, D., & Martinez, T. R. (2000). Quantum associative memory. *Information Science*, 124(1-4), 237–296. doi:10.1016/S0020-0255(99)00101-2

Vijay Patil, V., & Shimpi, S. (2011). Handwritten English Character Recognition using Neural Network. *Journal of Elixir Comp. Sci. & Engg*, 41, 5587–5591.

Yang, J., Yan, X., & Yao, B. (2012). Character Feature Extraction Method based on Integrated Neural Network. *AASRI Procedia*, 3, 197–202. doi:10.1016/j.aasri.2012.11.033

This research was previously published in Quantum-Inspired Intelligent Systems for Multimedia Data Analysis; pages 262-276, copyright year 2018 by Engineering Science Reference (an imprint of IGI Global).

Chapter 22

Quantum Local Binary Pattern for Medical Edge Detection

Somia Lekehali

University of M'sila, M'Sila, Algeria

Abdelouahab Moussaoui

University of Ferhat Abbas Setif 1, El Bez, Algeria

ABSTRACT

Edge detection is one of the most important operations for extracting the different objects in medical images because it enables delimitation of the various structures present in the image. Most edge detection algorithms are based on the intensity variations in images. Edge detection is especially difficult when the images are textured, and it is essential to consider the texture in edge detection processes. In this article, the authors propose a new procedure to extract the texture from images, called the Quantum Local Binary Pattern (QuLBP). The authors introduce two applications that use QuLBP to detect edges in magnetic resonance images: a cellular automaton (CA) edge detector algorithm and a combination of the QuLBP and the Deriche-Canny algorithm for salt and pepper noise resistance. The proposed approach to extracting texture is designed for and applied to different gray scale image datasets with real and synthetic magnetic resonance imaging (MRI). The experiments demonstrate that the proposed approach produces good results in both applications, compared to classical algorithms.

INTRODUCTION

Medical image segmentation is necessary as a preliminary stage for several of medical image analysis. Medical images often exhibit poor image quality, such as low contrast, decoy structures, and the complex shape and appearance of some anatomical structures, which makes segmentation in medical imaging a difficult and challenging problem. Several algorithms have been developed to address these problems and enhance such segmentation. These algorithms fall into two categories: region-based methods and boundary-based methods.

DOI: 10.4018/978-1-7998-8593-1.ch022

Region-based segmentation methods group pixels with similar properties together to produce regions that represent meaningful objects or areas in the images. The grouping methods include region growing (Zhang, Li, & Feng, 2015) splitting and merging, and watershed methods (Shen, et al., 2015).

Boundary-based segmentation involves identifying the boundaries of adjacent regions in an image by detecting edges and isolated points. The classical boundary-based algorithms use abrupt changes and discontinuities of intensity, e.g., Roberts (1963), Prewitt and Sobel (1970) calculate the first-order derivative of a pixel value as a measure of the edge's magnitude and orientation. The Canny operator (Canny, 1986) is a more optimal edge detector that is capable of good detection and localization with a low error rate.

In real-world applications, each of these classical methods still has challenging limitations and drawbacks depending on different variables in the medical images, such as several objects with similar intensities, noise, and even the edge structures.

To enhance medical image edge detection, this paper has investigated the use of another image feature, namely, texture. In MRI images, texture is the most important characteristic for distinguishing between different brain tissues. Several texture analysis operators for extracting texture features are described. In (Massich et al., 2014) the self-invariant feature transform (SIFT) with low-level and high-level descriptors is used to differentiate the tissues present in breast images, a Gaussian Markov random field has also been used for texture recognition (Krishnamachari & Chellapa, 1997) and the Gabor filtering method (Manjunath & Ma, 1996) has shown good results in comparative studies of texture analysis. In addition, Ojala et al. (1996) have developed a robust, fast, and simple texture analysis operator to meet the requirements of real-world applications.

Many variants of the local binary pattern (LBP) procedure in the literature that cover several tasks for medical image analysis. Ghose et al. (2011) proposed a segmentation method for prostate images that used the LBP to propagate their Active Appearance Model (AAM) and provided an enhancement of texture features for its training. Their approach was validated on a transrectal ultrasound (TRUS), and it showed good results in the presence of intensity heterogeneities and imaging artifacts as well as computationally efficient performance. In (Oliver, Lladó, Freixenet, & Martí, 2007) the authors used another efficient and effective LBP-based model to describe the salient mass micro-patterns in mammographic images in order to reduce false positives; in this model, a support vector machine (SVM) was used to classify the detected masses.

Lakovidis et al. (2008) combined fuzzy logic and the LBP, which proved to be a good, efficient combination for ultrasound texture extraction. They used the Fuzzy LBP (FLBP) approach for supervised classification of nodular and normal samples from thyroid ultrasound images.

The present work proposes the Quantum Local Binary Pattern (QuLBP) as a new variant involving quantum information. The QuLBP model is proposed for characterizing the MR images, and two main applications are presented. The first application performs an edge detection task using a CA as a next process to obtain the edges of images, and the second combines the edge filter with Deriche-Canny edge detection for salt and pepper noise resistance (Deriche, 1987). Compared to traditional edge detection operators, the QuLBP efficiently and accurately obtained edges for several datasets.

The remainder of this paper is organized as follows. Section 2 discusses the technical preliminaries for the LBP and its variants. Section 3 describes the QuLBP descriptor used in both applications. Section 4 introduces and discusses robustness experiments, and Section 5 concludes the paper.

THE LOCAL BINARY PATTERN AND THE PROPOSED MODEL

This section begins by describing the LBP, followed by an adaptation of the LBP for the edge detection task presented in two applications. This section also reviews the different methods used in the model.

LBP

The LBP is a local texture descriptor for an image divided into overlapping windows of 3x3 blocks of pixels, as shown in Figure 1. Computation of the original LBP is simple and fast. It is obtained by thresholding the pixel values in the neighborhood with the center pixel. If a neighborhood pixel value is not less than the value of the central pixel, the result will be set to one. Otherwise, it is set to zero. Then the results are multiplied by weights given by powers of two, and these are summed up together, resulting in the LBP code for each pixel as follows:

$$LBP_{N,R}(i_c, j_c) = \sum_{n=0}^{N-1} s(gv_n - gv_c) 2^n \quad (1)$$

where:

$$s(gv_n - gv_c) = \begin{cases} 1, & gv_n - gv_c \geq 0 \\ 0, & gv_n - gv_c < 0 \end{cases} \quad (2)$$

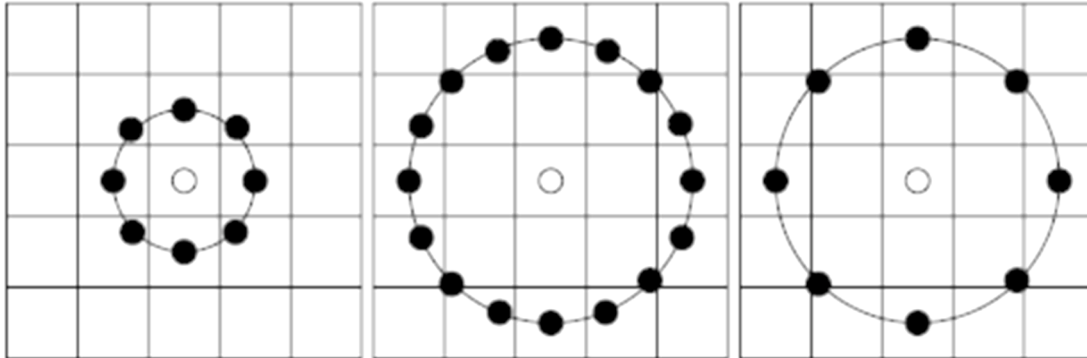
gv_n and gv_c are the gray values of the n th neighbor and the central pixel, respectively. The LBP is characterized by two parameters; N and R , where N is the number of neighborhood pixels and R is the radius of the LBP operator (see Figure 2).

Brain MR Images differ from other types of images in the number of textures that are presented. There are four basic textures: white matter, gray matter, spinal fluid in the background, and, in some pathological images, the texture of the pathologies. The textures of the same tissue may vary, producing an intensity inhomogeneity.

Figure 1. LBP model for a 3x3 window taken from the T1 MRI white matter region



Figure 2. The circular (8, 1), (16, 2) and (8, 2) neighborhoods



In (Figure 1), the LBP outputs are 1 or 0. However, since the window is taken from the same region of white matter, all outputs should be 1. Based on this concept, the QuLBP is a local classifier for a 3x3 window that preserves the simplicity of the original LBP with number of neighbors $N=8$ and radius $R=1$.

To reach this goal, a quantum mechanical system model is incorporated, that of the quantum bit, to generate a probabilistic numerical output as the unit state instead of the strict binary presentation in the LBP.

Incorporation of Quantum Information

Quantum information uses the specificities of quantum mechanics for manipulating information. According to Narayanan (1999), Narayanan and Menneer (2000) computational methods can use quantum-computing resources to obtain good performance. In quantum computing, the qubit is used instead of the classical bit to quantify information. The Bloch sphere qubit, represented in (Figure 3), can be found in quantum system states 0 and 1, denoted as $|0\rangle$ and $|1\rangle$ to differentiate these states from those of the classical bit. Unlike the classical bit, the qubit also can be found in a superposition state:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (3)$$

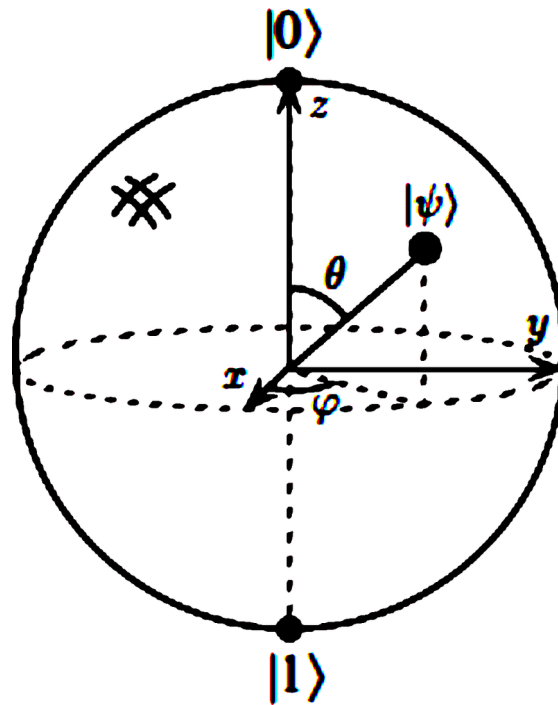
such that:

$$\alpha^2 + \beta^2 = 1 \quad (4)$$

where α and β are equivalent to $\cos \theta$ and $\sin \theta$, respectively, for a quantum angle θ that satisfies the fundamental probability:

$$|\cos(\theta)|^2 + |\sin(\theta)|^2 = 1 \quad (5)$$

Figure 3. Representation of the Bloch sphere for a qubit



Quantum information has been integrated as a mathematical concept with the LBP. The qubit can take an infinite number of states according to the superposition of the quantum system (Equation 3); the probability function has been used to force these and obtain a qubit value ($|0\rangle$ or $|1\rangle$).

Incorporating this concept in the LBP, the QuLBP is modeled as follows:

$$QuLBP_{N,R}(i_c, j_c) = \sum_{n=0}^{N-1} \mathcal{Q}(gv_n, gv_c)^{2^n} \quad (6)$$

$$\mathcal{Q}(gv_n, gv_c) = \begin{cases} |1\rangle, & \text{if } \sin(\theta) \geq \cos(\theta) \text{ and } \theta > 0 \\ |0\rangle, & \text{otherwise} \end{cases} \quad (7)$$

θ is the similarity angle between the central pixel gv_c and its neighbor gv_n and represents a local relationship between the two pixels. θ is measured as follows:

$$\theta = \left(1 - \frac{|gv_n - gv_c|}{T} \right) \frac{\pi}{2} \quad (8)$$

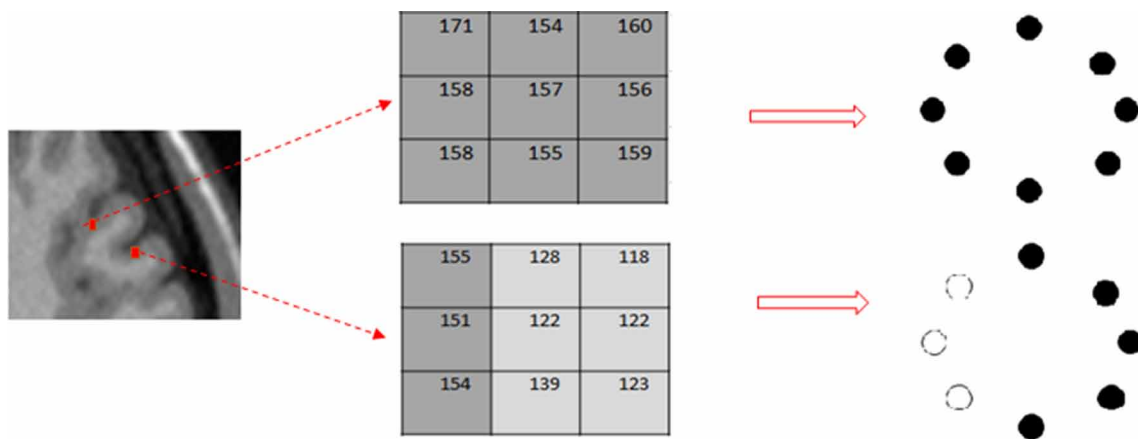
\cos and \sin are two probability functions used to obtain $|0\rangle$ and $|1\rangle$, respectively, where $|0\rangle$ means that the pixels gv_c and the pixel gv_n belong to different regions and $|1\rangle$ means that they belong to the

same region. T is based on the difference between the highest peak and its next valley in the image histogram. The expression is multiplied by $\frac{\pi}{2}$ to return the result value an angle in the range of $\left[0 \dots \frac{\pi}{2}\right]$.

From (Figure 4) it can be seen that the QuLBP classifies the 3x3 neighborhood pixels for two classes, one class with the value 1 as its central pixel and with its neighbor belonging to the same region, and one class with value 0 where the two pixels belong to different regions.

A simple example of the local classification is shown in (Figure 5). The QuLBP model has exceeded the LBP at the number of pixels with value 1 (patches taken from the same region). For more clarification, (Figure 6) shows the QuLBP model as applied to different types of images: a real, a synthetic MRI, and a famous cameraman image. It can be seen that the QuLBP algorithm plays a discriminative role between regions and boundary areas in the brain MRI image.

Figure 4. QuLBP binary patterns obtained for two image patches, the first row coming from a homogenous region and the second from an edged region



CA USING THE QULBP MODEL AND DERICHE-CANNY EDGE DETECTION FOR NOISE RESISTANCE

In this section, the application of the model is presented in two cases: first, the QuLBP is combined with the CA procedure for edge detection, and second, the model for edge detection is combined with the Deriche-Canny operator for noise reduction.

Cellular Automaton Edge Detection

CAs are mathematical, dynamic, and discrete models that are used to investigate the behavior of compound systems. Among its advantages, each cell in a CA contains only a few simple, basic rules. The interactions of cells in a neighborhood area and their communications lead to more sophisticated emergent global behavior.

Quantum Local Binary Pattern for Medical Edge Detection

Figure 5. Comparison of the QuLBP and LBP for a window of 11x11 pixels belonging to the same regions in a nonhomogeneous brain MRI image with 20% non-uniformity

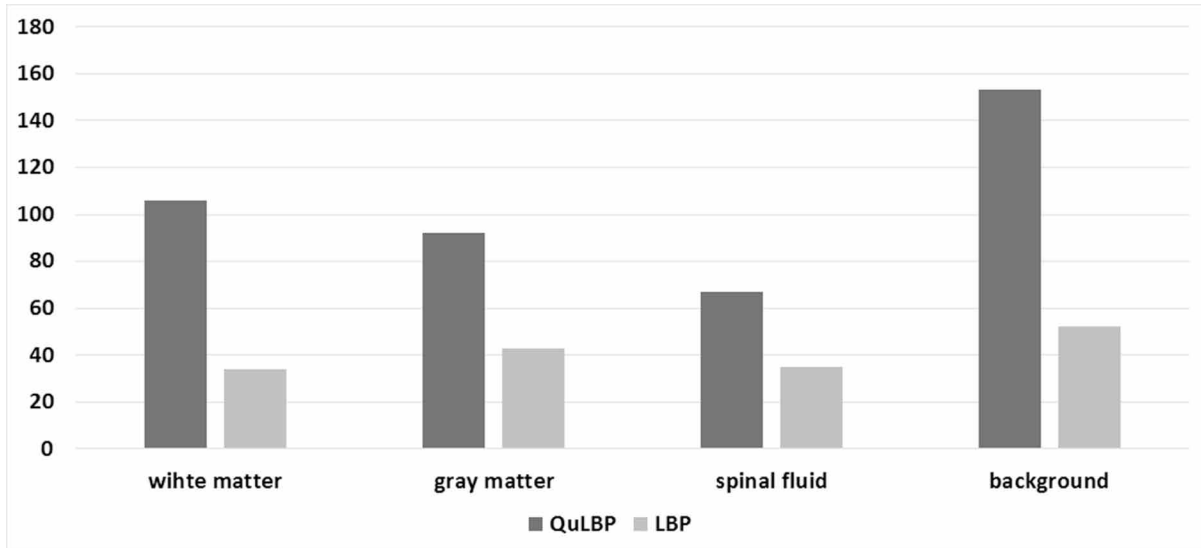
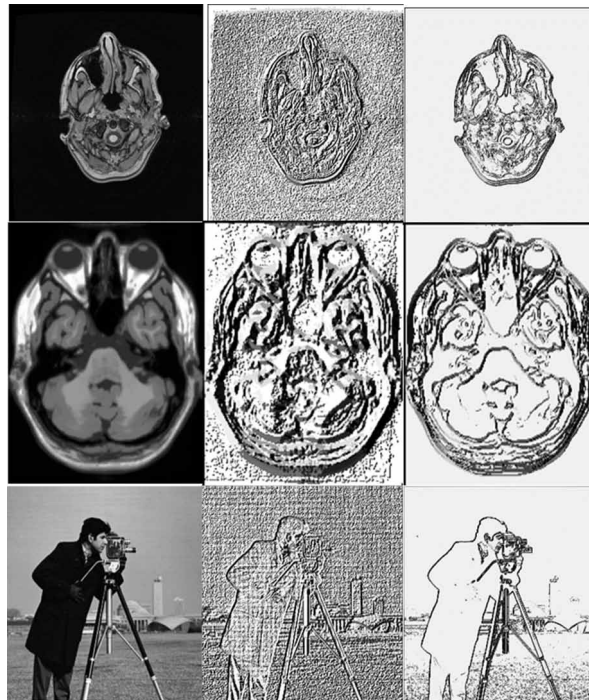


Figure 6. Application of LBP and QuLBP models, in 2nd and 3rd columns, respectively, to a real T2 weighted MR image, a synthetic brain T1 weighted MR Image, and a cameraman image



In recent years, CAs have been investigated for many image-processing applications. In (Rosin, 2010), CAs were trained to deal with convex hulls, feature selection, and noise filtering. Other tasks for which they have been used include object recognition (Dyer & Rosenfeld, 1981), calculating the properties of binary regions (Hernández & Herrmann, 1996), image enhancement, smoothing, and noise filtering (Rosin, 2006), and edge detection (Rosin & Sun, 2014; Slatnia, Batouche & Melkemi, 2007).

Before introducing the CA edge detector, first, a brief introduction is presented to the two-dimensional (2D) CA model in the next section.

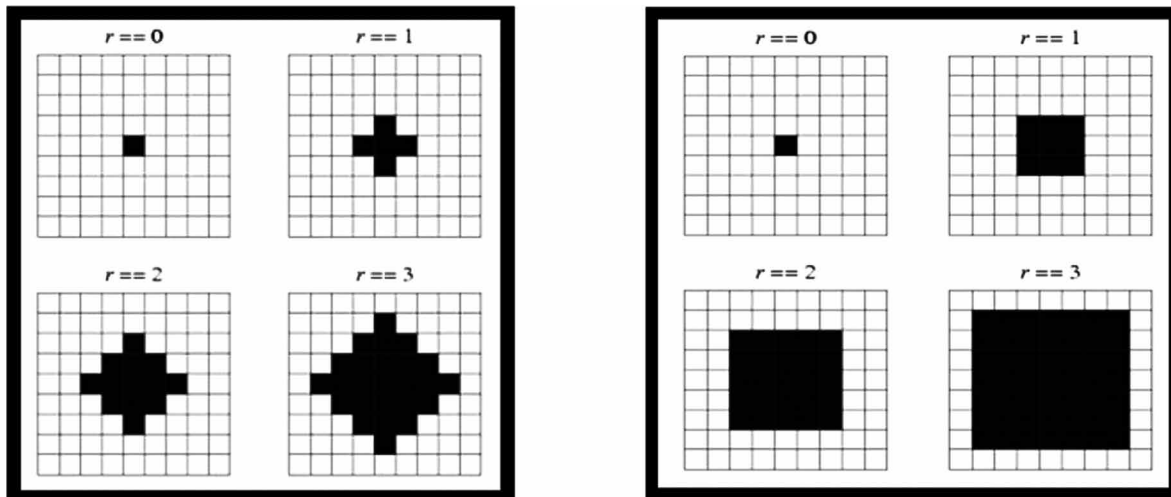
Cellular Automata

In a CA, space is defined as a grid of connected cells that evolve through discrete time steps according to a set of rules based on the states of neighboring cells. More precisely, a CA can be defined as a quadruple consisting of the following:

- **The dimensions of the grid:** 1D, 2D, or 3D;
- **A number of states:** On and off, gray level values, etc.;
- **Neighborhoods:** Von Neumann and Moore neighborhoods—see 7(1) and 7(2);
- **Rules:** Defining the automaton and the progress of the generations at each time $t+1$, where the initial state is given as $t = 0$.

Figure 7 shows the Von Neumann neighborhood and the more neighborhood.

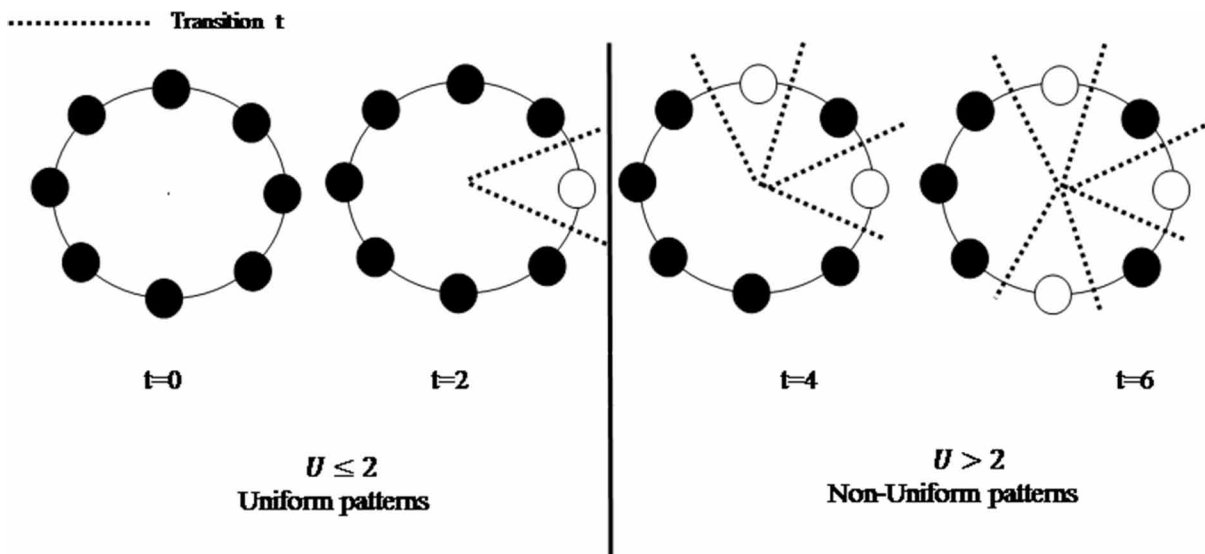
Figure 7. (1) Von Neumann neighborhood, (2) Moore neighborhood (Note: r denotes distance in (a) and (b))



Defining the Rule Set

Edge detection algorithms are usually applied to grayscale or color images, so designing a CA to be used as a practical edge detection application may be subject to one of the disadvantages of CAs, which is that the rule set for edges should be defined by laborious hand-generation, called the inverse problem. To explain this further, consider an MR image coded in 8 bits, which ends up with 8^{256} possible rules in the case of Moore neighborhoods. To train CAs, some previous works (Mofrad, Sadeghi, Rezvanian, & Meybodi, 2015; Uguz, Sahin, & Sahin, 2015) have used evolutionary approaches to select the edges. In this work, a simple model is used to train the CA to find the edge patterns for which the LBP is suitable for a CA; both are presented by a window characterized by a number of pixels ($N=8$) and a radius ($R=1$) along with the Moore neighborhood of the CA.

Figure 8. Representation of uniform and non-uniform LBP patterns



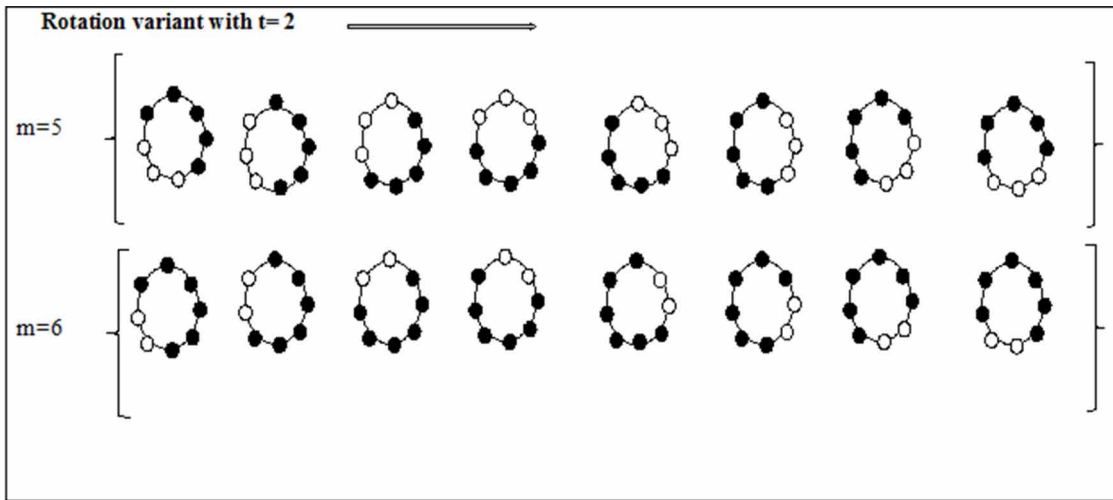
After calculating the QuLBP patterns for an input brain MR image, the question is: How can the edges be defined based on the obtained QuLBP patterns. The answer to this question is given as a second major step, using the CA.

The use of the QuLBP as a local descriptor reduces the rule search space to 2^8 possible rules presented by QuLBP patterns; only 0 and 1 are needed to express the obtained patterns, instead of the gray values. The possible space of edge rules is still a very vast range to search for the appropriate rules.

In (Ojala, Pietikainen, & Maenpaa, 2002) they have worked on what they call uniform patterns. They measured a uniformity called “U” by the number of bitwise transitions in the LBP pattern from 0 to 1 or vice versa, see (Figure 8). An LBP is called uniform if U is less than or equal to 2.

Based on the uniformity concept and the number of pixels with the value 1, as shown in (Figure 9), it has been empirically defined, with a limited number of tests, the possible patterns that represent the QuLBP edge patterns. Just the Uniform patterns are considered for this approach since the QuLBP model expressed well the MRI textures and separated the brain structures.

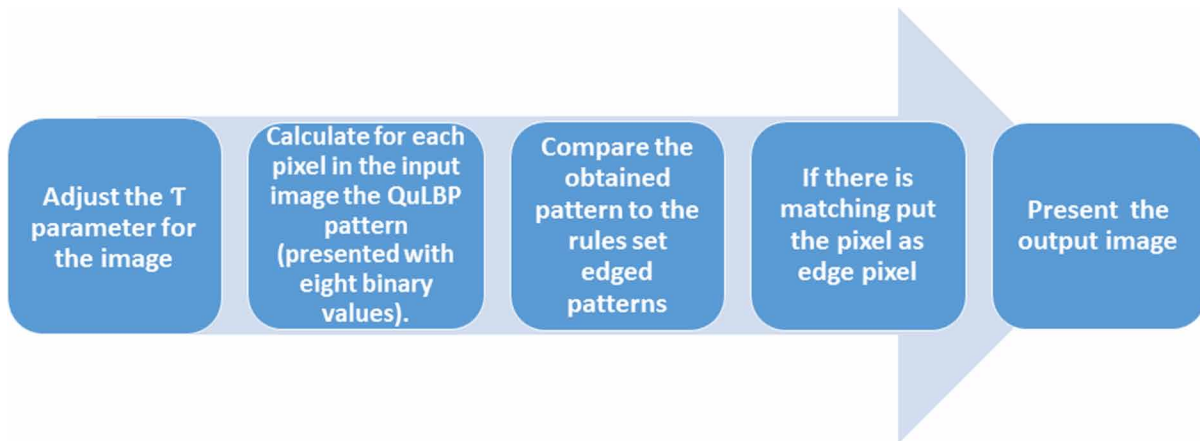
Figure 9. Representation of the obtained QuLBP edge patterns



The Pseudocode for the Approach

The CA edge detection algorithm is based on five main steps, as presented in (Figure 10).

Figure 10. Main steps of the proposed edge detection approach



Combination of Qulbp with Deriche-Canny Edge Detection for Salt and Pepper Noise Resistance

Deriche-Canny is an edge detection algorithm based on the Canny algorithm. Canny is known as one of the edge operators most resistant to noise in the classical methods. Deriche-Canny is based on the original Canny algorithm, which consists of four basic steps: Gaussian smoothing, gradient calculation, directional non-maximum suppression for gradient magnitudes, and hysteresis thresholding to determine

Quantum Local Binary Pattern for Medical Edge Detection

edge pixels. The difference is that the Deriche smoothing filter whose derivative is the exact solution to the Canny equation is extended to infinite support filters. The Deriche-Canny output can be adjusted through α scale parameter to filter out high frequency noise. Usually, the value of α is recommended to be around 1, as a small value of α (0.25 to 0.5) or a large value (around 2 to 3) will, given two choices, fail to exhibit good detection for the first or proper localization for the second. An edge detector must be precise and robust against noise and able to handle edge detection drawbacks, and although Deriche-Canny is a good candidate for such tasks it still has limitations with respect to noisy images, i.e., salt and pepper.

The basic idea behind the application is to combine the QuLBP model with the Deriche algorithm as the process immediately before the Deriche-Canny algorithm; this enhances the edges and presents a better localization in the presence of salt and pepper noise. In (Figure 11), it is obvious that the QuLBP preserves all edges and the obtained codes are not affected by the noisy pixels. The model also localizes the image boundaries with good performance.

Figure 11. Application of LBP and QuLBP, in the 2nd and 3rd columns, to a noisy (salt and pepper) T2 weighted MR image



EXPERIMENTAL RESULTS

To assess the strength of the proposed method, the proposed QuLBP had been tested through two different applications: CA edge detection and an edge filter. First the different datasets are described and the evaluation methods. Then the different experiments are described and ran for each of the models, evaluating and commenting upon these separately.

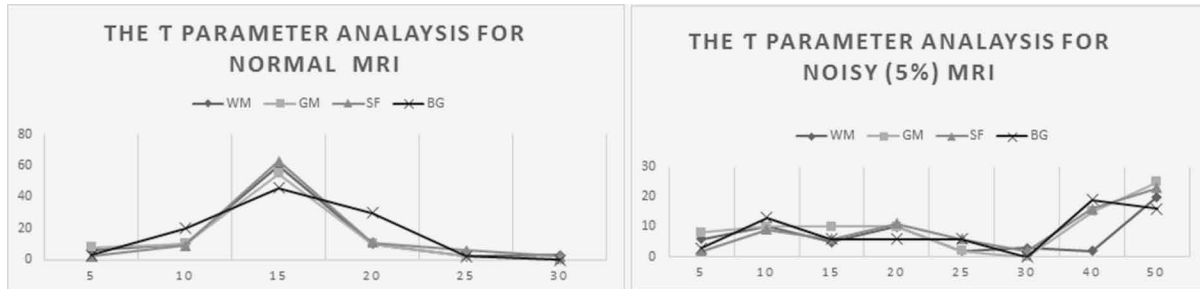
T Parameter Analysis

According to the algorithm description, T is considered as major parameter of QuLBP. It controls the performance of QuLBP as a local classifier. To adjust the threshold value T for each image in the experimental section, several patches of a (9*9) window were taken from the same region. Note that there are four main regions in an MR image: white matter (WM), grey matter (GM), spinal fluid (SF), and the background (BG)) in a variety of 20 of the training MR images, including normal and noisy ones.

First, the range of the T value is obtained from the histograms; specifically, the highest peak value and the next valley, as shown in (Figure 12).

Taking one image as an example, the best values of T are between 10 and 20 for normal MR images and 35 and 40 for noisy MR images.

Figure 12. T threshold adjustment for two patches taken from normal and noisy MR images



Description of Datasets

In this paper, two different datasets were used: real T1 and T2 brain MR images with 256x256 and 512x512 resolutions with 3% typical noise, and a synthetic MR image dataset presented in BrainWeb (1996). These are presented through six images to cover this diversity.

BrainWeb is an open access dataset that provides a full three-dimensional data volume of simulated MR images using T1 sequences with a variety of thicknesses, noise levels, and levels of intensity non-uniformity. The algorithm has been applied to the T1 MR sequence with a thickness of 1 mm, 1% noise, and an intensity inhomogeneity ranging from 0% to 40%.

Most of edge detection algorithms avoid one obstacle in the edge detection task by basing their evaluations on visual comparison only. To lay a foundation for the quantitative evaluation and offer a performance evaluation, Deriche-Canny algorithm provides the ground truth images, since it is known to be an optimal edge detector, then the blurred edges are manually corrected.

Evaluation Methods

The performance of the proposed approach had been evaluated by using three well-known assessment methods. The structural similarity index (SSIM) was utilized for the quantitative evaluation of the first application, and the root mean square error (RMSE) and peak signal to noise ratio (PSNR) were used to evaluate the second application's performance on noisy images.

The Structural Similarity Index

The SSIM is a method for measuring the similarity between two images, considering three independent channels: luminance, contrast, and structure.

The SSIM for two images x and y is calculated as:

Quantum Local Binary Pattern for Medical Edge Detection

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (9)$$

where c_1 and c_2 are small positive constants defined as $c_1 = (0.01 \times 2^n)^2$ and $c_2 = (0.03 \times 2^n)^2$, with n being the number of bits used to code the image ($n = 8$ in the case of an image coded in 8 bits). μ_x denotes the mean of x ; μ_y denotes the mean of y ; σ_x and σ_y are the variance of x and y , respectively; and σ_{xy} is the covariance of x and y .

Root Mean Square Error

The root mean square error (RMSE) is an image quality assessment metric. The RMSE calculates the root of the average difference between the original image and the edge-detected image such that a lower RMSE means less error between the two images. For the original image I and the edge-detected image J , the RMSE is calculated as in Equation (10):

$$RMSE = \sqrt{\frac{1}{m \times n} \sum_{i=1}^m \sum_{j=1}^n (I_{i,j} - J_{i,j})^2} \quad (10)$$

where m and n are the height and width of the images, respectively.

Peak Signal to Noise Ratio

The peak signal to noise ratio (PSNR) is the third image evaluation method the experiments used; it is usually expressed using the logarithmic decibel (dB) scale. A better quality image is characterized by a higher PSNR ratio between the original image and the distortion signal in an image. The PSNR is calculated as follows:

$$PSNR = 10 \log_{10} \left(\frac{R^2}{MSE} \right) \quad (11)$$

where $R = 255$ is the maximum variation for an input image with an 8-bit grayscale and MSE is calculated by (10) regardless of the root.

Cellular Automata Edge Detection

The edge detection results for real and synthetic MR Images are shown in (Figure 13) and (Figure 14), respectively. Two classical edge detectors were employed, i.e., Sobel and Canny, to extract edges with a standard threshold technique, and they are compared with the proposed approach. The T parameter was set in the model in the range [10...30] and the radius R to 1 for all experiments.

As can be seen in 13(2) and 14(2), not only does the Sobel operator fail to detect most of the MR images' meaningful edges, but in addition, the produced edges are discontinuous and thick. Canny's edges

in 13(3) and 14(3) are better than Sobel's in terms of their responsiveness to more of the images' edges. However, Canny misses some critical edge structures, which leads it to produce meaningless images.

The results reveal that the proposed approach successfully detected most of the edges. 13(4) and 14(4) show that the proposed approach detects the outlier edges of the brain textures and provides good localization of the small overlapping regions. The separation between different brain regions is presented with thin and connected edges. However, a double line marks the edges in some areas.

The quantitative accuracy of the results is shown in (Table 1). The images are given in the same order as in (Figure 13) and (Figure 14). For most of the results, the proposed approach has the best values for the evaluation metrics used; as an example, the SSIM value 0.69 is the best value that is achieved. The best values in the table are highlighted in boldface.

The results of the classical Canny and Sobel methods are not satisfactory. Sensitivity to each edge and its localization is more important in MR images than in other types of images, from the point of view of medical health.

The proposed method presented the MR images' edges with significantly more detail, which can be very useful for medical analysis, for example, in the presentation of certain anatomical textures such as tumors. Due to the high sensitivity of the proposed model to the images' boundaries. The choice of the T parameter in the QuLBP influences its sensitivity, and this choice can be understood as the crucial point for proper detection—which in some cases can produce double lines, although this may be rare.

Figure 13. Edge detection algorithms for real T1 and T2 weighted MR images: (1) MR test images, (2) Sobel algorithm, (3) Canny algorithm, (4) the proposed algorithm

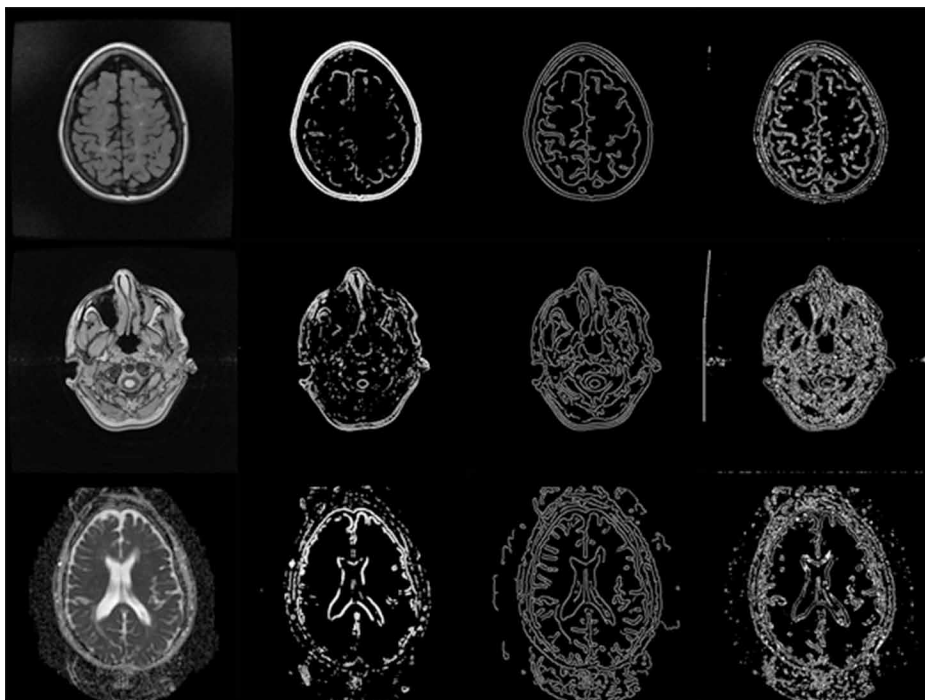


Figure 14. Edge detection for Brainweb T1 weighted MR images with 0% noise and 0 to 40% non-uniformity: (1) MR test image, (2) Sobel algorithm, (3) Canny algorithm, (4) The proposed algorithm

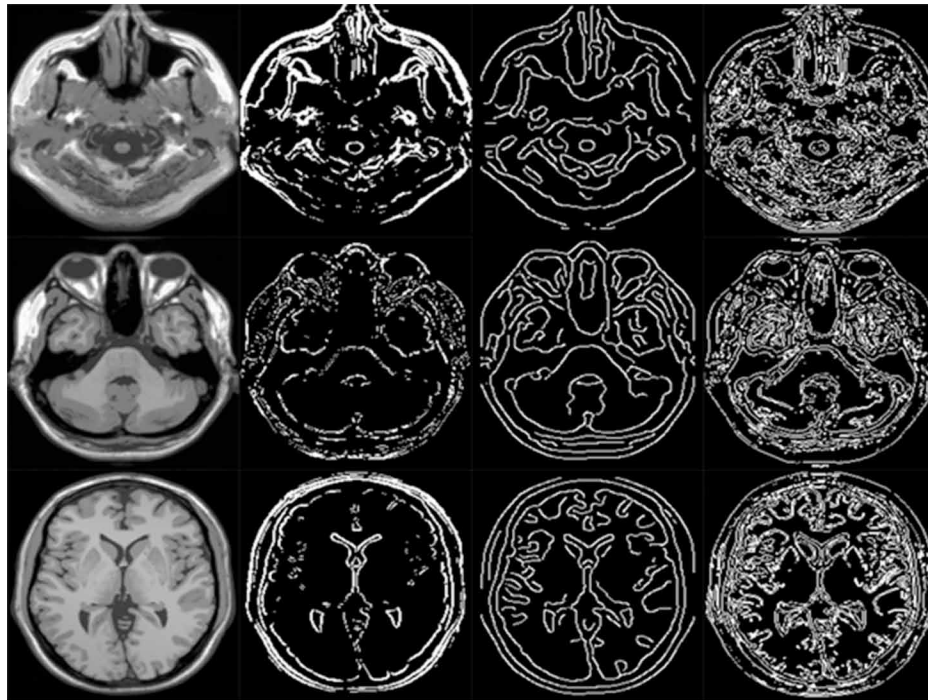


Table 1. Comparison of edge detection results

	Sobel	Canny	Proposed Approach
IM1	0.3976	0.4394	0.6924
IM2	0.5192	0.6064	0.6640
IM3	0.4023	0.5723	0.5886
IM4	0.4500	0.5054	0.6022
IM5	0.4395	0.4599	0.5491
IM6	0.2905	0.3532	0.4535

The Combination of Qulbp with Deriche-Canny Edge Detection for Salt and Pepper Noise Resistance

For the second application of the model, the same data was used as in the preceding test. The images are affected by salt and pepper noise, and for both applications α is set to 1, the two hysteresis thresholds are set to their best values with the best T parameter, and the radius R is 1.

15(1) shows the results for the Deriche-Canny algorithm, and 15(2) shows the results for the proposed approach. The Deriche-Canny algorithm produced more noisy pixels for the real MR images and missed most of the MR images' edges, producing a false discrimination of the brain regions. The proposed approach performs better with noisy pixels and eliminates a large range of these while preserving more

of the edged structures than the Deriche-Canny algorithm. However, some of the edges are lost due to the strong noise.

The results in (Table 2) confirm the qualitative results for at least five of the six MR images.

The application of the model to noisy images affected by salt and pepper noise preserves the boundaries of the MR images as shown previously in (Figure 15) and strengthens the edge pixels. Moreover, the effect of noise is reduced, and the approach provides a different edge map for the Deriche-Canny algorithm instead of the gray values of the original images, on that has less noisy pixels and stronger edge structures. In contrast, using the Deriche-Canny algorithm alone, the structure of edges is disfigured due to the strong effect of the noise and a false response to these noisy pixels.

Figure 15. Edge detection of (b) Deriche-Canny and (c) the proposed model on (a) real and synthetic MR images affected by salt and pepper noise

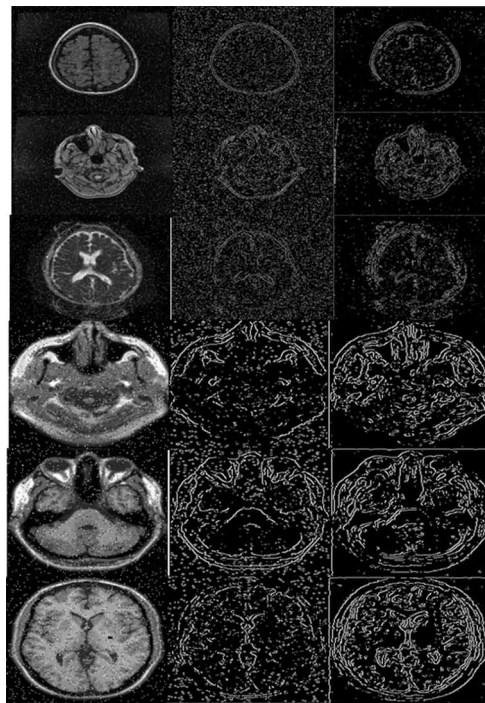


Table 2. Comparison of Deriche-Canny and the proposed approach

	Deriche-Canny		Proposed Approach	
	PSNR	RMSE	PSNR	RMSE
IM1	10.1369	79.3767	11.4908	67.9183
IM2	9.3414	86.9898	11.3508	69.0239
IM3	9.4388	86.0194	10.7173	74.2457
IM4	11.1846	70.3569	8.1243	100.0760
IM5	10.2101	78.7108	10.1252	79.4831
IM6	7.2939	86.4487	9.3957	110.1144

CONCLUSION

A novel model for MR image edge detection is presented. The QuLBP is designed as a local texture classifier, and the QuLBP model is investigated through two separate applications. The two applications, CA edge detection and QuLBP combined with Deriche-Canny for noise resistance, show good results compared to the classical methods. The main contributions of this paper can be summarized as follows:

- A new model that is an extension of the LBP model has been designed to deal with MR images with different in-homogeneities; the model successfully classifies local pixels while preserving the simplicity of the original model;
- The QuLBP patterns have been relaxed for the CA models and improved the performance of the edge detection with two rules that are empirically shown to provide an easy process without the need for evolutionary algorithms;
- As a second application, the effect of salt and pepper noise for the Deriche-Canny algorithm has been successfully reduced.

The QuLBP is designed to be investigated for specific applications and specific parameters, such as the type of data and its homogeneity in addition to the type of noise. To determine the generality of the model in medical analysis, future work should investigate a different type of noise for various medical imaging applications.

REFERENCES

- Brainweb: Simulated Brain Database. (1996). Retrieved from <http://brainweb.bic.mni.mcgill.ca/brainweb/>
- Canny, J. (1986). A Computational Approach to Edge Detection. *IEEE Transactions on Pattern Analysis and Machine Intelligence, PAMI-8*(6), 679–698. doi:10.1109/TPAMI.1986.4767851 PMID:21869365
- Deriche, R. (1987). Using Canny's criteria to derive a recursively implemented optimal edge detector. *International Journal of Computer Vision, 1*(2), 167–187. doi:10.1007/BF00123164
- Dyer, C. R., & Rosenfeld, A. (1981). Parallel image processing by memory augmented cellular automata. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 3*(1), 29–41. doi:10.1109/TPAMI.1981.4767048 PMID:21868917
- Ghose, S., Oliver, A., Marti, R., Llado, X., Freixenet, J., & Villanova, J. C., & Meriaudeau, F. (2011). Prostate segmentation with local binary patterns guided active appearance models. *Medical Imaging: Image Processing, 7962*, 8.
- Hernández, G., & Herrmann, H.J. (1996). Cellular automata for enhancement elementary image. *Graphical Models and Image Processing, 58*(1), 82–89. doi:10.1006/gmip.1996.0006
- Krishnamachari, S., & Chellapa, R. (1997). Multiresolution Gauss-Markov random field models for texture segmentation. *IEEE Transactions on Image Processing, 6*(2), 251–267. doi:10.1109/83.551696 PMID:18282921

- Lakovidis, D., Keramidis, E., & Maroulis, D. (2008). Fuzzy local binary patterns for ltrasound texture characterization. In *International conference image analysis and recognition* (pp. 750-759). Springer. 10.1007/978-3-540-69812-8_74
- Manjunath, B. S., & Ma, W.-Y. (1996). Texture features for browsing and retrieval of image data. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 18(8), 837–842. doi:10.1109/34.531803
- Massich, J., Meriaudeau, F., Sentís, M., Ganau, S., Pérez, E., Puig, D., ... Martí, J. (2014). Sift texture description for understanding breast ultrasound images. In *International Workshop on Digital Mammography*, (pp. 681-688). Cham: Springer. 10.1007/978-3-319-07887-8_94
- Mofrad, M., Sadeghi, S., Rezvanian, A., & Meybodi, M. R. (2015). Cellular edge detection: combining cellular automata and cellular learning automata. *AEÜ. International Journal of Electronics and Communications*, 69(9), 1282–1290. doi:10.1016/j.aeue.2015.05.010
- Narayanan, A. (1999). Quntaum computing for beginners. In *Proceedings of the 1999 Congress on Evolutionary Computation CEC 99* (pp. 2231-2238). IEEE.
- Narayanan, A., & Menneer, T. (2000). Quantum artificial neural network architectures and components. *Information Sciences*, 128(3), 231–255. doi:10.1016/S0020-0255(00)00055-4
- Ojala, T., Pietikäinen, M., & Harwood, D. (1996). A comparative study of texture measures with classification based on featured distributions. *Pattern Recognition*, 29(1), 51–59. doi:10.1016/0031-3203(95)00067-4
- Ojala, T., Pietikainen, M., & Maenpaa, T. (2002). Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 24(7), 971–987. doi:10.1109/TPAMI.2002.1017623
- Oliver, A., Lladó, X., Freixenet, J., & Martí, J. (2007). False positive reduction in mammographic mass detection using local binary patterns. *Medical Image Computing and Computer-Assisted Intervention–MICCAI, 2007*, 286–293. PMID:18051070
- Roberts, L. G. (1963). *Machine perception of three-dimensional solids* [Doctoral Dissertation]. Massachusetts Institute of Technology.
- Rosin, P. (2010). Image processing using 3-state cellular automata. *Computer Vision and Image Understanding*, 114(7), 790–802. doi:10.1016/j.cviu.2010.02.005
- Rosin, P. L. (2006). Training cellular automata for image processing. *IEEE Transactions on Image Processing*, 15(7), 2076–2087. doi:10.1109/TIP.2006.877040 PMID:16830925
- Rosin, P. L., & Sun, X. (2014). Edge detection using cellular automata. In *Cellular Automata in Image Processing and Geometry* (pp. 85–103). Springer International Publishing. doi:10.1007/978-3-319-06431-4_5
- Shen, P., Qin, W., Yang, J., Hu, W., Chen, S., Li, L., ... Gu, J. (2015). Segmenting multiple overlapping Nuclei in H & E Stained Breast Cancer Histopathology Images based on an improved watershed. In *IET International Conference on Biomedical Image and Signal Processing (ICBISP 2015)*, (p. 4). 10.1049/cp.2015.0779

Quantum Local Binary Pattern for Medical Edge Detection

Slatnia, S., Batouche, M., & Melkemi, K. (2007). Evolutionary cellular automata based approach for edge detection. In *Applications of Fuzzy Sets Theory* (pp. 404-411).

Sobel, I. (1970). Camera models and machine perception. Stanford University, Dept of Computer Science.

Uguz, S., Sahin, U., & Sahin, F. (2015). Edge detection with fuzzy cellular automata transition function optimized by PSO. *Computers & Electrical Engineering*, 43, 180–192. doi:10.1016/j.compeleceng.2015.01.017

Zhang, X., Li, X., & Feng, Y. (2015). A medical image segmentation algorithm based on bi-directional region growing. *Optik-International Journal for Light and Electron Optics*, 126(20), 2398–2404. doi:10.1016/j.ijleo.2015.06.011

This research was previously published in the Journal of Information Technology Research (JITR), 12(2); pages 36-52, copyright year 2019 by IGI Publishing (an imprint of IGI Global).

Index

A

ASEAN Exchange 411, 415
 authentication 128, 130, 132, 134, 143, 156-158, 160-162, 278, 289-301, 303, 325, 335-338, 354

B

back-propagation algorithm 435-438, 441, 443
 Bayesian inference 384, 402-403, 415
 brute-force attack 289, 313-314

C

cellular automaton (CA) 447
 classical cryptography 262-263, 289, 292, 299, 325-326, 357-358, 375
 cluster 164-165, 167-168, 174-175, 196, 206
 clustering 50, 91, 137, 160, 164-165, 167, 189, 194-196, 205-206, 225, 233, 244
 Code-based Cryptosystem 267
 combinatorial optimization 22, 24, 48-49, 51-52, 56, 88-90, 92, 158, 228-229, 233-235, 242-243
 context sensitive 197-199, 225
 Correlation Coefficient 164, 173
 cryptography 128, 137, 160, 247-252, 255, 262-268, 270, 273-275, 278, 284-292, 298-300, 325-332, 335-337, 339-344, 346-347, 353-354, 356-360, 374-376

D

digital image watermarking 127, 132, 143, 156, 158, 160
 diversity 1-2, 7, 18-19, 31, 58, 61-63, 71, 75-76, 229, 233, 458
 DNA sequence 228, 230-231, 238, 242-243, 245, 324
 Domain Knowledge Incorporation 51

E

E-Business 400-402, 408, 410, 415
 E-Commerce 247, 356, 400-402, 408, 410, 413, 415
 economic load dispatch 50, 91, 93-94, 107-110
 EEG 416-418, 421-422, 425-429, 432-433
 E-governance 247-248, 260-264
 empirical measures 173
 entanglement 164-165, 172, 201, 234, 247, 254-255, 258, 262, 267, 283-285, 287, 303, 323, 356, 372, 379-381, 383, 386, 390, 399, 438
 entity authentication 289-290, 292, 294-295, 298

F

FCM 164-167, 174-177, 183, 189-193, 196
 fragment assembly 228-230, 233-234, 240-245

G

genetic algorithm 50, 88-92, 94, 108, 110, 137, 164-168, 171, 174, 176, 189, 193-194, 196, 228-230, 233-234, 242, 244, 412
 global convergence 1, 10-11, 370
 Global Stress 378
 gray scale image 165, 197-201, 207, 213-214, 225-226, 447

H

handwritten character recognition 435-437, 442-445
 hardware 127-128, 131, 133, 135, 138, 144, 152, 154, 156, 253, 256, 273, 284, 286, 340-341
 hash 142, 277-278, 290, 302-304, 307-308, 310, 322, 325, 337-338, 344
 hash functions 278, 325, 338, 344
 hash-based cryptography 278
 Human Computer Interaction Evaluation Systems 416
 Hybrid Evolutionary Algorithm 22

Index

I

imperceptibility 127-128, 131-132, 141, 152-154, 156

J

Job Improvement 378

K

key distribution 247, 249, 253-255, 257, 262-263, 265-266, 282-283, 285, 325-326, 328-329, 331-332, 334, 336, 338-339, 341, 343-347, 349-357, 359-360, 362, 364-365, 367, 370, 374-375

L

local binary pattern (LBP) 448
local classifier 447, 450, 457
LSB replacement 127, 133, 142, 144, 156

M

magnetic resonance imaging (MRI) 447
Markowitz portfolio optimization 400, 403, 406, 411
Modern Portfolio Theory (MPT) 403, 415
multi-analytic processes 400-401, 410
Multi-layer Neural Network 435, 443
Multilevel Feedback Queue Scheduling 111-114, 120, 126
multiple knapsack problem 22-25, 27, 30, 35, 48-49, 51, 78, 80-81, 87-90
Multi-Tasking 111
multivariate cryptography 267, 275
MUSIG function 197, 209-210

N

NEQR 302-305, 309-310, 312, 322, 324
Network Security 137, 161, 226, 286, 289, 299
NeuroIS 416-417, 422-424, 428-433
noise reduction 447, 452
non-convex 93, 108-110

O

One-time Pad Technique 325
optimization 1-3, 5, 7, 9, 13, 17-22, 24, 48-49, 51-52, 56, 87-96, 102-103, 106-110, 158, 161, 165, 194-195, 198, 207, 226, 228-230, 232-235, 242-245, 355, 360-361, 363-364, 368, 370, 374-376, 400,

403, 406, 408-414, 444

organisational management 387, 392

OTP 289-290, 292-298

P

Parallel Algorithms 51
Photon Impulse 345
power dissipation 127-128, 131, 145, 156
Probabilistic cloning 283-284, 286
Probability Detection 345
Project management 387, 397
PSO algorithm 1-3, 5, 16, 167

Q

QIP 302
quantum behaved 1, 20-21
quantum bit 199, 203, 250, 254, 307, 438, 450
Quantum Brain 378, 380, 424, 432
quantum cloning 267-268, 280-288
quantum computers 52, 137, 249, 258, 267-268, 270, 273, 284, 289-290, 292, 298, 313, 323, 326, 340, 357, 359-360, 372
quantum computing 24, 52, 88, 95, 97, 106, 164-167, 171-172, 174-175, 195-196, 229, 234, 259, 264, 266-267, 284, 303, 325, 327, 340, 343, 355-357, 359-360, 375-376, 403, 416, 418, 435-436, 438, 445, 450
quantum consciousness models 416, 431
quantum cryptography 160, 247-251, 262-266, 286, 288, 292, 298, 325-327, 329-330, 332, 335-337, 339-344, 346-347, 353, 357-360, 374-376
Quantum Decision Science 387
quantum differential evolution 362, 372-373
Quantum Economy 387
quantum gates 172, 201, 254, 302, 304, 307, 357, 368, 445
quantum information 195, 244, 254-256, 281, 283-284, 303, 324, 342, 376, 378-380, 382-383, 419, 433, 440, 445, 448, 450-451
Quantum inspired evolutionary algorithm 51, 95, 167, 243
Quantum inspired Genetic algorithm 228-229, 234, 242
quantum key distribution 247, 249, 253, 255, 262-263, 265-266, 282-283, 285, 326, 331, 334, 336, 339, 343-347, 349-355, 357, 359-360, 367, 374-375
quantum machine learning 355, 360-361, 373-375, 418
quantum mechanics 165, 172, 196, 201, 225, 254, 262-263, 268, 283-284, 324-325, 327, 356, 368, 378-381, 383, 387-390, 393, 396, 398, 400-401,

403, 406, 411, 415, 417-418, 420, 425, 432-433, 436-439, 444, 450

Quantum Neural Network 355, 371, 418, 433, 436-437
quantum node 247, 253, 256

quantum reinforcement learning 355, 361, 368-369, 375
quantum repeater 247, 254-257, 266

Quantum resistant cryptography 325, 340

quantum secure 289-290, 292, 298

quantum superposition principle 197, 199

Quantum-Behaved Bat Algorithm 93, 95, 101

R

reply attack 289-290, 294, 297

reversible logic 127, 131, 136, 138-139, 141, 143-146, 148-151, 154, 156, 160-162, 323

robustness 57, 127-129, 131-133, 141, 143, 152-154, 156, 338, 403, 448

Round Robin 111-113, 126

S

scheduling algorithm 111-113, 115, 126

segmentation 143, 160, 164-167, 173-174, 176, 178-179, 181, 184-185, 187, 189-190, 193-201, 204-209, 212-213, 218, 221, 224-227, 324, 361, 447-448, 463, 465

self supervised 197-198, 203, 225

self-renewal mechanism 1-2, 19

spatial domain 127-128, 131-133, 143-144, 156, 158, 160

Statistical Measure 196

synchronization 249, 333, 345, 347, 349-352, 354

T

time quantum 111, 113-116, 118, 120, 126, 167

V

valve-point effect 93-96, 101-108, 110