Smart IoT System Construction of Security Mechanisms Based on Quantum Walks and Chaotic Systems

By

Ahmad Alanezi

A thesis submitted in partial fulfilment of the requirements of Liverpool John Moores University for the degree of Doctor of Philosophy

January 2024

Acknowledgements

In the name of Allah, the Beneficent, the Merciful

In the name of Allah, the Beneficent, the Merciful. First and foremost, I would like to thank ALLAH for the blessing and bounty. Thanks for ALLAH for the completion of this PhD's thesis. Only due to His blessings I could finish my thesis. Praise be to ALLAH on all HIS blessings. I am profoundly grateful to my parents, Dahwi and Badeiyah, for their unwavering support and encouragement throughout my academic journey. Their belief in me has been a constant source of strength and motivation. I extend my heartfelt thanks to all my family, and children, whose love and understanding have been my pillars of support. Their endless patience and encouragement have been instrumental in my success. Special thanks are due to my supervisor Dr. Hoshang Kolivand , and Prof. Ahmed A. Abd El-Latif, for their invaluable guidance, insightful feedback, and constant encouragement. Their expertise and mentorship have been crucial in shaping my research and academic growth. I would like to dedicate a special acknowledgment to my late brother, Najeeb. His support and belief in my abilities remained a source of inspiration, even in his absence. His memory continued to guide and motivate me throughout this journey. This thesis is not only a reflection of my effort but also the unwavering support and sacrifice of all those mentioned above, for which I am eternally grateful.

Ahmad Alanezi

List of Publications

The main results in this thesis are summarized in the following articles:

[1] **Ahmad Alanezi**, Bassem Abd-El-Atty, Hoshang Kolivand, Abd El-Latif, A. Ahmed, Abd El-Rahiem, Syam Sankar, and Hany S Khalifa. "Securing digital images through simple permutation-substitution mechanism in cloud-based smart city environment." Security and Communication Networks 2021 (2021).

[2] **Ahmad Alanezi**, Bassem Abd-El-Atty, Hoshang Kolivand, and Ahmed A. Abd El-Latif. "Quantum based encryption approach for secure images." In 2021 1st International Conference on Artificial Intelligence and Data Analytics (CAIDA), pp. 176-181. IEEE, 2021.

[3] **Ahmad Alanezi**, Ahmed A. Abd El-Latif , Hoshang Kolivand, and Bassem Abd-El-Atty. "Quantum walks-based simple authenticated quantum cryptography protocols for secure wireless sensor networks" New Journal of Physics 25, no. 12 (2023): 123041.

[4] Bassem Abd-El-Atty, Abdullah M Iliyasu, **Ahmad Alanezi**, Ahmed A Abd El-latif, "Optical image encryption based on quantum walks", Optics and Lasers in Engineering, 138, 106403..

[5] Alejandro Freyre-Echevarria, **Ahmad Alanezi**, Ismel Martinez-Diaz, Musheer Ahmad, Ahmed A. Abd El-Latif, Hoshang Kolivand, Abdul Razaq, "An External Parameter Independent Novel Cost Function for Evolving Bijective Substitution-Boxes", Symmetry 2020, 12(11), 1896.

[6] Dhinakaran Veeman, **Ahmad Alanezi**, Hayder Natiq, Sajad Jafari, Ahmed A. Abd El-Latif, "A Chaotic Quadratic Oscillator with Only Squared Terms: Multistability, Impulsive Control, and Circuit Design" Symmetry , 2022.

ABSTRACT

The integration of Internet of Things (IoT) into daily life, particularly in the context of fifth-generation (5G) networks, demands robust security mechanisms to protect sensitive information. Current encryption methods, especially concerning image transmission over 5G networks, face vulnerabilities. This thesis explores the innovative fusion of quantum walks and chaotic systems to fortify data security in IoT environments, addressing the inherent vulnerabilities in multimedia content security. The research introduces novel cryptographic mechanisms, leveraging chaotic systems for image encryption. A key novelty lies in the development of a novel image encryption approach for data transfer in cloud-based smart cities, cascading Logistic-Chebyshev and Logistic-Sine maps, demonstrating enhanced security and efficiency with lower encryption time compared to existing algorithms. An optical image cryptosystem, integrating quantum walks at two encryption stages - inner encryption and encoding by double random phase encoding, exhibits robustness and security against diverse attacks. Furthermore, a digital image cryptosystem utilizing quantum walks for image substitution surpasses state-of-the-art cryptosystems in performance. In response to the burgeoning field of quantum computation and chaotic dynamical systems, the thesis introduces three authenticated quantum cryptographic protocols based on quantum walks. Authenticated Quantum Key Distribution (AQKD), Authenticated Semi-Quantum Key Distribution (ASQKD), and Authenticated Semi-Quantum Key Distribution with limited quantum resources ensure security against well-known attacks while maintaining high efficiency. This study addresses the security concerns arising from the interaction between physical and virtual worlds in the 5G-IoT context. It emphasizes the vulnerabilities in multimedia data transmission and proposes cutting-edge technologies based on quantum and chaotic systems as robust defense mechanisms. The convergence of 5G and IoT, while transformative, introduces security challenges, and the proposed solutions aim to significantly improve data security in 5G networks, IoT, cloud computing, and applications in smart cities. The comprehensive evaluation of proposed solutions using various metrics underscores their robustness against a spectrum of attacks, positioning them as promising contributors to enhancing the security of multimedia data transmission in 5G networks and beyond.

Table of Contents

List of Tables

List of Figures

Figure **Page**

CHAPTER 1

INTRODUCTION

1.1 Introduction

In the modern era, the Internet of Things (IoT) has become an indispensable tool in our lives, extending beyond industrial and scientific applications to permeate all facets of our daily existence. IoT represents a rapidly expanding network of interconnected objects and devices equipped with sensors, allowing them to gather data and communicate this data through Internet networks (Atzori et al. (2017)). The boundless potential of IoT has led to its adoption in a wide range of domains, including smart cities, smart homes, smart vehicles, and telemedicine (Nair et al. (2022)). These interlinked devices are tasked with real-time data collection and integration with cloud resources, where the gathered data is stored and analyzed (Kumar and Agrawal (2023)). However, these processes have significant implications for the privacy and security of sensitive information. Thus, safeguarding this sensitive data from malicious attacks has become a critical concern in the realm of IoT (Iftikhar et al. (2023)).

Despite its futuristic connotations, IoT has already integrated into our daily lives. Internet networks serve as communication channels for data transfer and the deployment of new applications (Heidari et al. (2023)). With enhanced accessibility and cost-effectiveness, cloud computing has evolved into a fundamental computing platform that permeates various aspects of our daily routines (Al-Qerem et al. (2023)). Nevertheless, the secure transmission of data between IoT devices and cloud computing platforms remains a pressing challenge, particularly due to the lack of a standardized, secure data transfer medium. Consequently, many cloud users have experienced data breaches or loss on cloud platforms. This underscores the increasing urgency to develop advanced techniques for securing data accessible via IoT (Zhang et al. (2023)).

Chaotic systems play a crucial role in shaping security mechanisms (Yan et al. (2023)). Chaotic systems can be intuitively described as dynamical systems characterized by highly sensitive initial conditions and behavior so intricate that prediction becomes nearly impossible. While there is no universally accepted formal mathematical definition of a chaotic system, the following criteria are generally acknowledged as essential (Clemente-López et al. (2023)):

1. Sensitivity to initial conditions.
2. Topological mixing.
3. Dense periodic orbits.

Chaotic systems can exist in both continuous-time and discrete-time forms. In discrete systems, a more operational definition has been proposed: some discrete-time chaotic systems are characterized by nonlinear maps (Gan et al. (2018)).

Furthermore, the mappings that describe chaotic systems are both deterministic and highly sensitive to initial conditions. The deterministic nature of the equations defining chaotic systems implies the existence and uniqueness of solutions. However, it is crucial to note that determinism does not guarantee computability. In other words, even though solutions exist and are unique, they may be impossible to calculate exactly using a computer. Deterministic mappings of chaotic systems defined over the real number system are computationally unpredictable, primarily because their trajectories are non-computable. In contrast, deterministic mappings defined on finite sets are always predictable because their trajectories are eventually periodic.

Chaotic systems play a pivotal role in the design of cryptographic mechanisms for IoT devices (Zhang et al. (2023)), where cryptographic methods are used to ensure data security and confidentiality. Cryptographic techniques are employed to establish secure communication between two parties, even in the presence of potential eavesdroppers. Hash functions, pseudo-random number generators, and substitution boxes play a crucial role in the development of modern cryptographic applications, forming the backbone of many contemporary cryptographic systems. With the rapid advancement of quantum computation, many traditional cryptographic mechanisms may be vulnerable due to their reliance on mathematical computation. Thus, the development of hash functions, pseudo-random number generators, and substitution box mechanisms based on quantum technologies is a promising avenue for creating secure and reliable cryptographic applications (Srinivas et al. (2018)).

Quantum computation is a rapidly evolving field that has achieved numerous breakthroughs in recent decades (Ladd et al. (2010)). It has transitioned from an emerging scientific discipline to a mature research area in science and engineering. Quantum walks (QWs), the quantum counterpart of classical random walks, have emerged as a powerful tool for constructing quantum algorithms and have been recognized as a universal model of quantum computation. Additionally, QWs have the potential to be employed in the development of quantum cryptographic protocols and quantum networks. Quantum walks are now a well-established research area in quantum computation, offering a rich landscape of exciting challenges for physicists, computer scientists, and engineers (Kendon (2007)).

A discrete-time quantum walk can be represented as a nonlinear mapping, denoted as $Q : \mathscr{H} \mapsto \mathscr{P}$, where $\mathscr{H}$ represents the Hilbert space in which the quantum walker operates, and $\mathscr{P}$ is a set of probability distributions (Gu et al.

(2021)). Viewing discrete quantum walks as nonlinear mappings permits considering them as discrete-time and discrete-value chaotic systems. Further substantiating this perspective are the deterministic characteristics of evolution through unitary operators and the high sensitivity to initial conditions. Consequently, discrete quantum walks find applications in designing secure cryptographic mechanisms for IoT devices.

As a conclusion, this dissertation aims to tackle the critical challenge of insecure data communication. It proposes two innovative approaches: firstly, investigating the use of chaotic systems as a foundation for novel cryptographic mechanisms against conventional attacks. Secondly, it explores the potential of quantum walks in designing secure protocols for data transfer within communication framework, offering a solution to the potential vulnerabilities of traditional cryptographic methods posed by the advent of quantum computation.

1.2 Problem statement

The booming multimedia landscape, fueled by the Internet of Things and ubiquitous internet access, has propelled image and video sharing on 5G networks to new heights (Akpakwu et al. (2017)). Yet, this surge in multimedia exchange intensifies the vulnerability of sensitive content to malicious attacks during transmission. Applied cryptography emerges as a critical shield, safeguarding data security, particularly for images, a ubiquitous digital format. Cryptography researchers strive to develop robust techniques that effectively encrypt image information and thwart unauthorized access by adversaries(Wayner (2009)).

However, traditional encryption algorithms like DES and AES struggle with images due to the inherent correlation between neighboring pixels (Amin and EL-Latif (2010); Belazi et al. (2015)). Chaos-based cryptography has e-merged as a promising alternative, harnessing the unpredictable nature of chaotic systems to scramble image data (Gan et al. (2018)). Chaos maps like the Lorentz and Arnold-Tent maps serve as engines for generating random sequences, used to alter pixel values (substitution) and rearrange their positions (permutation) within the image matrix (Abd-El-Atty et al. (2019b); Ali and Khan (2019)). Researchers further enhance security by incorporating techniques like DNA sequence operations(Wang et al. (2015)), cellular automata (Zhang et al. (2014)), and substitution boxes (Abd-El-Atty et al. (2019b); Ali and Khan (2019)), weaving them into the chaotic encryption tapestry.

The permutation-substitution process lies at the heart of image encryption, dictating the obfuscation level achieved (Zhou et al. (2014a)). While traditional methods like sort-based and cyclic shift have limitations (Wang et al. (2019)), innovative approaches like Wang's combined cyclic shift-sorting Wang et al. (2019)) and Hua's "chaotic magic transform" (Hua et al. (2015)) offer faster processing and efficient pixel permutation. In the substitution stage, pixel values are scrambled primarily via XOR operations with chaotic sequences. Notably, researchers have flexibility in sequencing these steps, prioritizing reversibility, robust evaluation parameters, and swift processing.

Recent research has witnessed a surge in designing specialized chaotic systems for image encryption, both one-dimensional (1-D) and multi-dimensional (Wang et al. (2019); Zhou et al. (2014a); Li et al. (2017)). Each work aims to enhance specific security aspects. While 1-D maps offer simplicity and speed, their limitations like small key spaces and discontinuities necessitate exploration of cascading systems, leveraging the strengths of multiple 1-D maps while mitigating their drawbacks (Xian and Wang (2021); Gan et al. (2018); Chai et al. (2020a,b)).

Despite substantial efforts to design secure cryptosystems, the advent of quantum technologies presents new challenges. Many cryptographic mechanisms may become vulnerable due to the potential capabilities of quantum computers. Therefore, ensuring security and privacy in the transmitted data within the IoT environment is of utmost importance. New cryptographic mechanisms are required to withstand potential attacks not only from digital computers but also from quantum computers.

1.3 Research Questions

In this section, we will explore the following research questions:

- **What is the research impact of this study?**

  The potential impact of the dissertation is significant. The proposed image security solutions have the potential to significantly improve the security of multimedia data transmission in a variety of applications, including 5G networks, cloud computing, and smart cities. Specifically, the proposed image security solutions could have the following impacts:
  - Improved security for multimedia data transmission in 5G networks.
  - Enhanced security for cloud computing and smart cities.
  - New opportunities for research and innovations.

- **What is the research aims of this study?**

  The research aim of this dissertation is to develop new image security solutions, utilizing quantum and chaotic systems, to address the security challenges of multimedia data transmission in 5G networks and other applications.

- **What is the research gap in this study?**

  Previous image encryption algorithms suffer from one or more of the following drawbacks:

  Low efficiency: Some algorithms require a lot of time and computational resources to encrypt and decrypt images. This can be a problem for real-time applications.

  Lack of robustness against attacks: Some algorithms are vulnerable to common attacks, such as brute-force attacks, differential attacks, and statistical attacks.

Complex implementation: Some algorithms are difficult to implement, especially in hardware.

- **How can we evaluate the security and performance of image security solutions based on quantum and chaotic systems?**

  Using a variety of metrics, including correlation analysis, histogram analysis, Shannon entropy analysis, UACI and NPCR analyses, Key sensitivity analysis, and occlusion analysis.

- **What is the research scope?**

  The research scope of this dissertation is to develop new image security solutions, utilizing quantum and chaotic systems, to address the security challenges of multimedia data transmission in 5G networks and other applications. The specific research areas covered in this dissertation include:

  Chaotic image encryption.

  Quantum image encryption.

  Image security for 5G networks.

  Quantum authentication protocols for secure wireless communications.

- **Relationship to previous works?**

  The proposed security solutions in this dissertation are related to previous work in the following ways:

  The proposed image security solutions are novel, efficient, and secure, and they outperform previous works in terms of both security and efficiency.

  The proposed chaotic image encryption mechanism is based on cascading two chaotic maps, which is more efficient and secure than previous chaotic image encryption algorithms.

  The proposed quantum image cryptosystem uses quantum walks instead of QKD to generate and distribute encryption keys, which makes it more efficient and less vulnerable to attacks.

The proposed optical encryption approach for 5G networks can encrypt and decrypt images in real time, which is essential for 5G networks.

The proposed secure authenticated quantum cryptography protocols for wireless sensor networks are more efficient and secure than previous protocols for image encryption and authentication in wireless sensor networks.

- **What are the key methodological steps used in this dissertation?**

  The proposed image security solutions were designed based on the unique properties of quantum and chaotic systems.

  The proposed solutions were implemented using MATLAB.

  The proposed solutions were evaluated using a variety of metrics, including correlation analysis, histogram analysis, Shannon entropy analysis, UACI and NPCR analyses, Key sensitivity analysis, and occlusion analysis.

1.4 Project Aims

The primary objective of this project is to propose new cryptographic algorithms based on quantum walks/chaotic systems for IoT platforms. These algorithms aim to enhance data security in IoT environments and protect data from potential threats in the quantum era. The designed cryptographic mechanisms will contribute to the security of IoT devices and facilitate advanced detection without compromising the efficiency of exclusion protocols. They will be employed to ensure the safety and privacy of data within IoT network environments.

1.5 Objectives

To achieve the project's aim, the following objectives have been identified:

- Conduct a comprehensive literature review and construct a meta-analysis framework to explore various aspects of quantum physics as applied to IoT. The proposed cryptographic systems based on quantum walks will be grounded in robust research, enhancing the structural topologies and functions of IoT.

- Develop new quantum key distribution protocols based on quantum walks for IoT applications, securing critical infrastructures (e.g., the Smart Grid), financial institutions, and national defense. Create a new secure data transmission protocol based on quantum walks/chaotic maps for IoT-based smart systems.

- Design and implement a novel visual cryptographic protocol based on quantum walks/chaotic maps for IoT-based smart systems.

- Develop a new secret sharing protocol using quantum walks/chaotic maps for IoT scenarios.

- Create new cryptographic mechanisms based on quantum walks/chaotic maps for IoT applications.

- Simulate and experiment with an actual QW-enabled protocol-based network environment. This simulation will study and enhance the behavior of crawler software designed to discover discrete objects like devices and data sources commonly encountered in an IoT environment. The proposed protocol will be tested alongside complex exclusion protocols, which are integral components of advanced crawler architecture.

1.6 Novelties

Quantum computation and chaotic dynamical systems represent rapidly growing fields with numerous breakthroughs in recent decades. Both quantum walks and chaotic systems have emerged as powerful tools with applications in quantum computation, cryptography, and universal computation modeling.

This dissertation introduces the following significant contributions:

- A novel image encryption approach for data transfer in cloud-based smart cities, leveraging the cascading of two integrated 1-D chaotic systems: the Logistic-Chebyshev map and the Logistic-Sine map. This approach ensures security and efficiency, exhibiting lower encryption time compared to related algorithms. (Alanezi et al. (2021))

- An optical image cryptosystem that incorporates quantum walks at two encryption stages: inner encryption and encoding by double random phase encoding. The system demonstrates robustness and security against a variety of attacks. (Alanezi et al. (2021))

- A digital image cryptosystem that utilizes quantum walks to substitute the original image before encrypting the substituted image. This system outperforms several robust state-of-the-art cryptosystems. (Alanezi et al. (2021))

- Three authenticated quantum cryptographic protocols based on quantum walks: Authenticated Quantum Key Distribution (AQKD), Authenticated Semi-Quantum Key Distribution (ASQKD) where one of the two participants has limited quantum capabilities, and Authenticated Semi-Quantum Key Distribution with both legitimate users possessing limited quantum resources. These protocols ensure security against various well-known attacks and exhibit high efficiency. (Alanezi et al. (2023))

1.7 Scope

This thesis is dedicated to the essential and timely research domain of information security, particularly focusing on quantum and classical cryptography.

Specifically, it explores the potential of quantum walks and chaotic systems, with a detailed examination of discrete-time quantum walks, as valuable resources for designing secure cryptographic applications. These applications encompass the creation of hash functions, pseudo-random number generators, substitution boxes, as well as the development of quantum and classical image encryption protocols and authentication protocols. With this perspective, the thesis provides a comprehensive approach to the design and implementation of security solutions suitable for modern and future networks (e.g., 5G, 6G), environments (e.g., Internet of Things), and applications (e.g., digital image encryption and steganography).

1.8 Structure of the Thesis

The thesis comprises six chapters, each contributing to the comprehensive exploration of the subject:

Chapter 1: Introduction - This chapter provides an introductory overview of the thesis topic. It elaborates on the rationale, motivation, and research problem while highlighting the main contributions. Additionally, the chapter outlines the structure of the dissertation.

Chapter 2: Fundamental Concepts - This chapter delves into the fundamental concepts that serve as the basis for the thesis, namely, quantum walks and chaotic maps. It explores their applications in cryptography, including pseudo-random number generators, quantum hash functions, and image cryptosystems.

Chapter 3: Methodology - In this chapter, the methodology employed in the study is presented, organized into four distinct phases.

Chapter 4: Proposed Methods - The fourth chapter introduces the novel methods developed in this study. It begins with a proposal for a cipher image mechanism based on chaotic systems, designed for secure data transfer in cloud-based smart cities. Subsequently, a multimedia cryptosystem built on quantum walks is presented, offering resilience against potential attacks from both quantum and classical computers. Additionally, a multimedia cryptosystem that incorporates quantum walks into optical image encryption frameworks is discussed. The chapter concludes with the introduction of three authenticated quantum cryptography protocols based on quantum walks, designed to ensure secure wireless sensor communications.

Chapter 5: Performance Evaluation - This chapter is dedicated to the evaluation of the performance of the cryptosystems presented in Chapter 4.

Chapter 6: Conclusion and Future Work - The final chapter offers a conclusion of the work conducted in the thesis and outlines potential areas for future research.

CHAPTER 2

MATHEMATICAL BACKGROUND

Quantum walks are generalizations of random walks that have extensive applications in various fields including cryptography, quantum algorithms, and quantum networking. Discrete-time quantum walks can be seen as nonlinear mappings between quantum states and position probability distributions, and this mathematical property may be thought of as an imprint of chaotic behavior, consequently used to generate encryption keys. In this chapter, the fundamental concepts for quantum random walks, besides its cryptographic applications, are discussed.

2.1 Quantum walks

Since classical random walks have been successfully adopted in developing classical algorithms, and one of the key issues in quantum computation is to design quantum algorithms that are faster than their classical analogs, there has been a tremendous interest in understanding the characteristics of quantum walks over the last few years (Venegas-Andraca (2012a)). Quantum walks constitute a generalization of random walks in the quantum world. Originally devised as models of physical phenomena as well as advanced tools for building quantum algorithms (Nayak and Vishwanath (2000); Aharonov et al. (1993, 2001)), quantum walks have been proved to constitute a universal model of quantum computation (Venegas-Andraca (2012a); Lovett et al. (2010); Childs (2009)). These properties, together with the appealing idea of defining the notion of an algorithm based on scattering theory (Feldman and Hillery (2007)), have made quantum walks a popular field of research.

Quantum walks can be either continuous or discrete models of computation, depending on how time is measured ($t \in \mathscr{R}^+ \cup \{0\}$ for the continuous case and $t \in \mathscr{N} \cup \{0\}$ for the discrete case). Continuous-time quantum walks evolve via the Schrödinger equation, while discrete-time quantum walks evolve via Unitary operators (Venegas-Andraca (2012a); Wong (2016); Tregenna et al. (2003); Luo et al. (2015); Konno et al. (2016); Carson et al. (2015)). In both cases and so far, the mathematical and computational properties of quantum walks have been studied on graphs. In this thesis, discrete-time quantum walks (QWs) are utilized as a key component of the presented quantum/classical cryptographic protocols.

The basic components of a coined discrete quantum walk are a coin, a walker, evolution operators, and a set of observables. A walker is a quantum system living in a Hilbert space H_p with $\#(H_p) = \aleph_0$ if the quantum walk runs on an unlimited line or $\#(H_p) = N$ if it runs on a circle of N vertices. The coin is typically a quantum system living in a two-dimensional Hilbert space $H_c = \alpha|0\rangle + \beta|1\rangle$. Then, the total state of a discrete quantum walk lives in $|\psi\rangle_{t_0} = H_p \otimes H_c$.

The total evolution operator $\hat{U}$ for a discrete quantum walk is given by Eq. (2.1):

$$\hat{U} = \hat{S}(\hat{C} \otimes \hat{I}) \tag{2.1}$$

where $\hat{C}$ and $\hat{S}$ are the coin operator and the shift operator, respectively.

An elementary step of a coined classical random walk consists of tossing a coin and, depending on the outcome of the coin toss, the walker would walk one step either to the left or the right. The dynamics of a coined discrete quantum walk resemble that of a coined classical random walk.

An elementary step of a coined discrete quantum walk consists of applying, to the total quantum system (walker and coin), an evolution operator to the coin state followed by a conditional shift operator. The coin operator transforms the coin state into a superposition, and the shift operator spreads the walker state over the graph upon which the quantum walk is run (for example, over $\mathscr{Z}$ if it is an unrestricted quantum walk on a line.)

In general, an r-step discrete quantum walk can be written as

$$|\psi\rangle_{t_r} = \hat{U}^r |\psi\rangle_{t_0} \tag{2.2}$$

or, equivalently, as

$$|\psi\rangle_{t_r} = \sum_k [a_k |0\rangle_c + b_k |1\rangle_c] |k\rangle_p \tag{2.3}$$

where $|\psi\rangle$ is the total quantum state, t_r is the step number, and $\hat{U}^r$ represents the unitary operator applied on the entire quantum state $|\psi\rangle_{t_0}$ t_r times. The general matrix representation of a 2-dimensional coin operator is given by Eq. (2.4) (Venegas-Andraca (2012a); Tregenna et al. (2003)):

$$\hat{C} = \begin{pmatrix} \sqrt{\rho} & \sqrt{1-\rho}\, e^{i\omega} \\ \sqrt{1-\rho}\, e^{i\omega} & -\sqrt{\rho}\, e^{i(\omega+\phi)} \end{pmatrix} \tag{2.4}$$

Where $0 \le \rho \le 1$ and the arbitrary angles $0 \le \omega, \phi \le \pi$. If coin operators defined over $\mathscr{R}^2$, the general matrix representation of a 2-dimensional coin operator is given by Eq. (2.5), where $\theta \in \mathscr{R}$ (Li et al. (2018a); Yang et al. (2015, 2016a)):

$$\hat{C} = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix} \tag{2.5}$$

2.1.1 Single-particle quantum walks on a line

The structure of the shift operator $\hat{S}$ depends on the graph the quantum walk is running on. For instance, a shift operator for a coined discrete quantum walk on an unrestricted line is given by Eq. (2.6):

$$\hat{S} = \sum_x (|x+1,0\rangle\langle x,0| + |x-1,1\rangle\langle x,1|) \tag{2.6}$$

Quantum walks can be thought of as non-linear mappings $Q : H \mapsto P$ where H is a Hilbert space in which the quantum walker lives and P is a set of probability distributions. This property, together with high sensitivity and other characteristics, allows us to think of quantum walks as chaotic systems. The probability $P(x,r)$ of finding the particle at position x after r steps can be stated as follows:

$$P(x,r) = \sum_{c\in\{0,1\}} |\langle x,c|\left(\hat{U}\right)^r|\psi\rangle_{t_0}|^2 \tag{2.7}$$

An illustrated example for the probability distributions of running quantum walks on a line for r-steps is given in Figs. 2.1, 2.2, 2.3, and 2.4, where the initial position state is $|0\rangle_p$, and the initial coin operator constructed by $\theta = \pi/4$ as stated in Eq. (2.5). It is obvious from Figs. 2.1, 2.2, 2.3, and 2.4 that the characteristic of quantum walks on a line is the skewness of their probability distributions and dependent on the coin initial state. In addition, noticing a quasi-uniform behavior in the central region of probability distributions, approximately in the period [−39, 39] in the case of running quantum walks on a line for 50 steps. Eventually, regarding the skewness of probability distributions covers the same number of positions. If the quantum walk performed an even number of times, then only even positions could have a non-zero probability, and odd positions have zero probability, also if the quantum walk performed an odd number of times, then only odd position sites could have non-zero probability, and even positions have zero probability.

2.1.2 Single-particle quantum walks on a circle

The shift operator suitable for being used on one-dimensional quantum walks on an N-circle, i.e. a circle with N nodes, is given by Eq. (2.8):

$$\hat{S} = \begin{cases} |2,0\rangle\langle 1,0| + |N,1\rangle\langle 1,1| & when\ x = 1 \\ |1,0\rangle\langle N,0| + |N-1,1\rangle\langle N,1| & when\ x = N \\ |x+1,0\rangle\langle x,0| + |x-1,1\rangle\langle x,1| & when\ x \neq 1,N \end{cases} \tag{2.8}$$

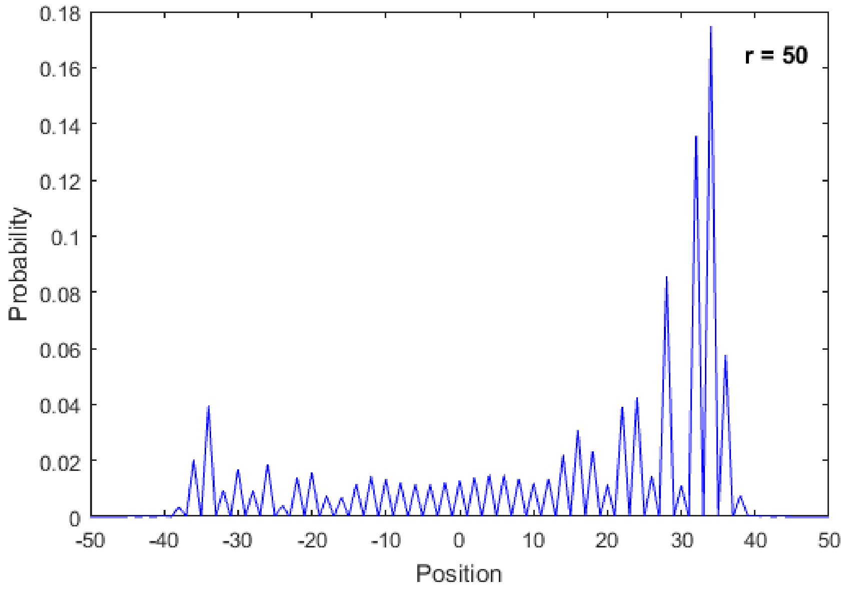


Figure 2.1: the probability distribution of running quantum walks on a line for 50 steps, where the initial coin particle is $H_c = |0\rangle$. It is obvious that the probability at the even positions have non-zero probability, while the odd positions have zero probability in the period $[-39, 39]$ (Venegas-Andraca (2012a)).

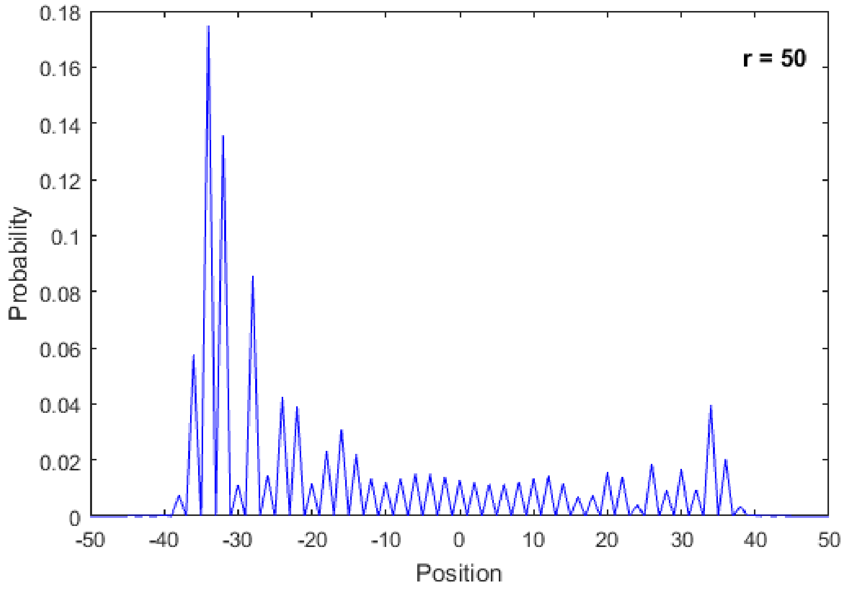


Figure 2.2: the probability distribution of running quantum walks on a line for 50 steps, where the initial coin particle is $H_c = |1\rangle$. It is obvious that the probability at the even positions have non-zero probability, while the odd positions have zero probability in the period $[-39, 39]$ (Venegas-Andraca (2012a)).

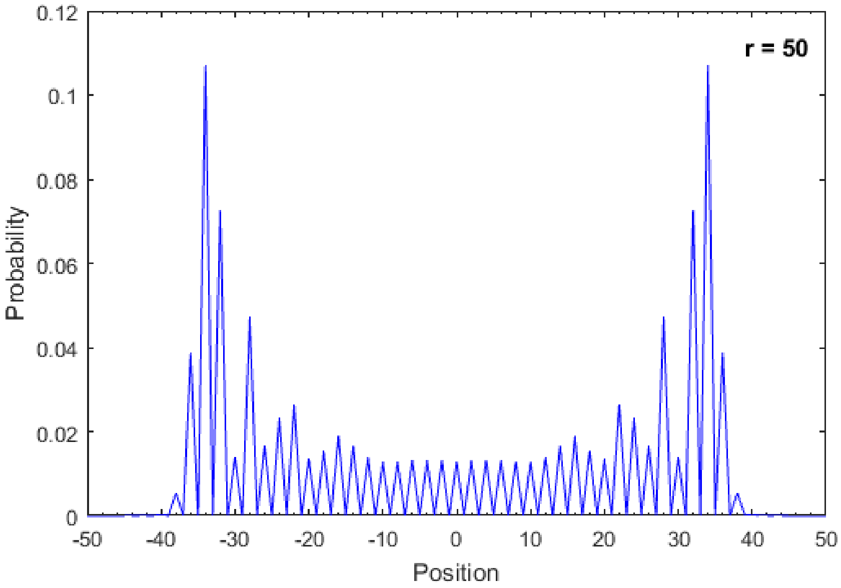


Figure 2.3: the probability distribution of running quantum walks on a line for 50 steps, where the initial coin particle is $H_c = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. It is obvious that the probability at the even positions have non-zero probability, while the odd positions have zero probability in the period $[-39, 39]$ (Venegas-Andraca (2012a)).

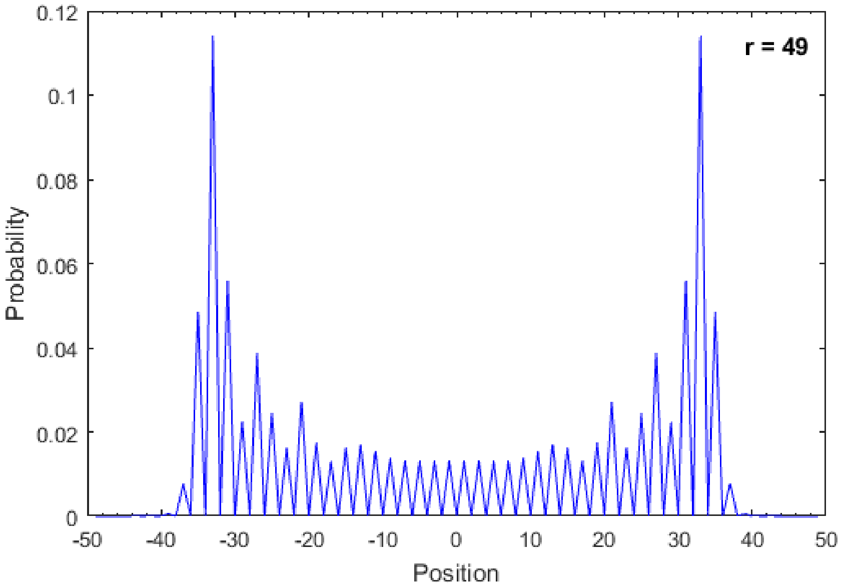


Figure 2.4: the probability distribution of running quantum walks on a line for 49 steps, where the initial coin particle is $H_c = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. It is obvious that the probability at the odd positions have non-zero probability, while the even positions have zero probability in the period $[-38, 38]$ (Venegas-Andraca (2012a)).

Since Eq. (2.1) defines a Unitary (hence reversible) operator, the position probability distribution produced by a walker on an N-circle never reaches a uniform distribution (Tregenna et al. (2003)). Moreover, please note that for a circle with only odd N nodes, the probability $P(x,r)$ is nonzero in any position if the number of steps r is greater than or equal to the number of nodes N (Nayak and Vishwanath (2000); Li et al. (2013a); Yang and Zhao (2016)).

An illustrated example for the probability distributions of running one-dimensional one-particle quantum walks on a circle with 99 vertices is given in Figs. 2.5 and 2.6, where the initial position is $|0\rangle_p$ and the initial coin operator $\hat{C}$ is constructed by $\theta = \pi/4$. It is obvious that for a circle with only N nodes, the probability $P(x,r)$ is nonzero in any position if the number of steps r is greater than or equal to the number of nodes N.

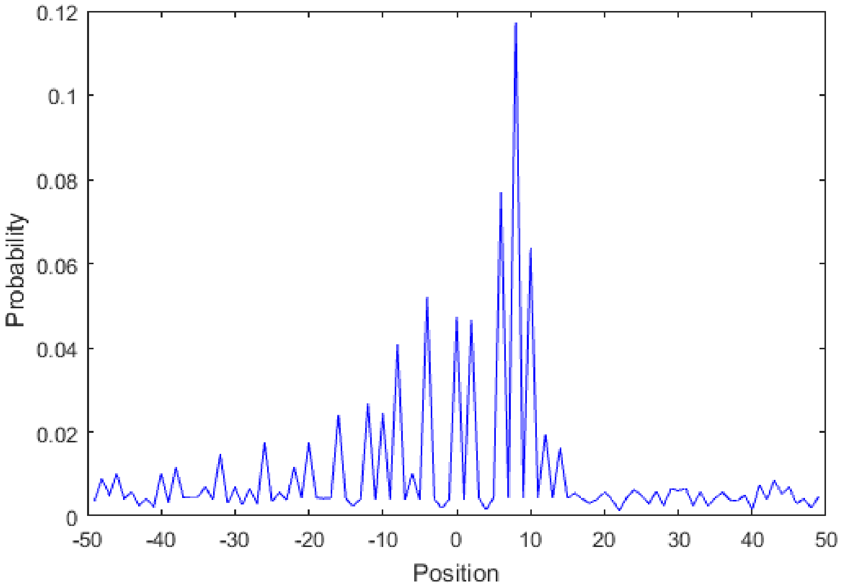


Figure 2.5: the probability distribution of running quantum walks on a circle with 99 vertices for 155 steps, where the initial coin particle is $H_c = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. It is obvious that for a circle with only odd N nodes, the probability $P(x,r)$ is nonzero in any position if the number of steps r is greater than the number of nodes N (EL-Latif et al. (2020a)).

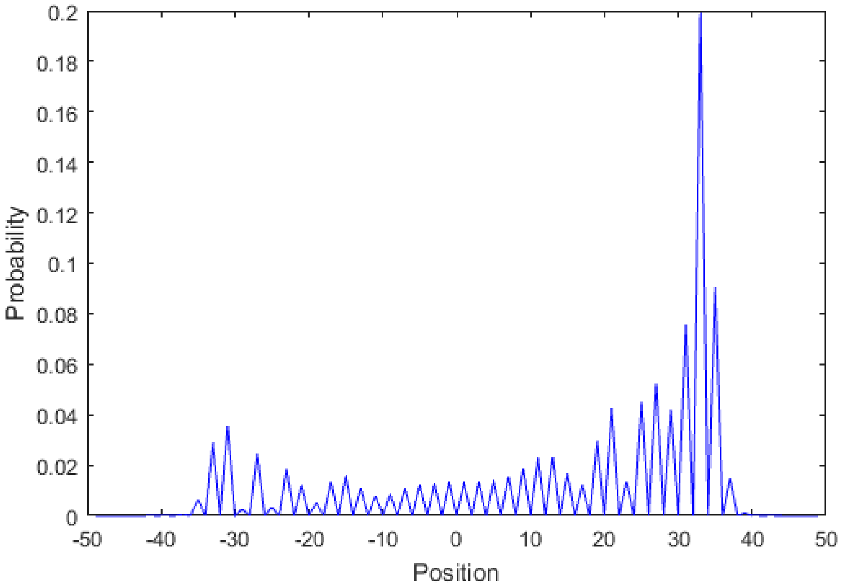


Figure 2.6: the probability distribution of running quantum walks on a circle with 99 vertices for 49 steps, where the initial coin particle is $H_c = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. It is obvious that for a circle with only odd N nodes, the probability $P(x,r)$ have zero in some positions if the number of steps r is less than the number of nodes N (EL-Latif et al. (2020a)).

2.1.3 Two-particle quantum walks on a circle

One of the attractive characteristics of multi-walker quantum random walks is that the dimension of the probability increases exponentially with the number of walkers. In addition to the entanglement between interacting particles. Consequently, it is promising running two-particle quantum walks on a circle is more powerful than running single-particle quantum walks (Li et al. (2013a)).

In this model of quantum walk, two coins $|coin\rangle_1, |coin\rangle_2$ and two walkers $|walker\rangle_1, |walker\rangle_2$ are used. The total shift operator for the system is $\hat{S} = \hat{S}_1 \otimes \hat{S}_2$ (Yang et al. (2015, 2016a); Li et al. (2013a)), where $\hat{S}_1$ and $\hat{S}_2$ are shift operators for $|walker\rangle_1$ and $|walker\rangle_2$, respectively. Following the same rationale, two coin operators shall be use, one for each coin $|coin\rangle_1, |coin\rangle_2$. The total coin operator is a Unitary operator that can be written as an order 4 matrix (Yang et al. (2015, 2016a); Li et al. (2013a)). In this thesis, the coin matrices presented in Eq. (2.9) is utilized.

$$\hat{C} = \left[\begin{pmatrix} \cos(\theta_1) & \sin(\theta_1) \\ \sin(\theta_1) & -\cos(\theta_1) \end{pmatrix} \otimes \begin{pmatrix} \cos(\theta_2) & \sin(\theta_2) \\ \sin(\theta_2) & -\cos(\theta_2) \end{pmatrix} \right] \tag{2.9}$$

An illustrated example for the probability distributions of running one-dimensional two-particle quantum walks on a circle with 25 vertices is given in Figs. 2.7 and 2.8, where the initial position is $|0\rangle_p$ and the initial coin operator $\hat{C}$ constructed by $\theta_1 = \pi/4$ and $\theta_2 = \pi/3$ as stated in Eq. (2.9). It is obvious that for a circle with only odd N nodes, the probability is nonzero in any position if the number of steps r is greater than or equal to the number of nodes N.

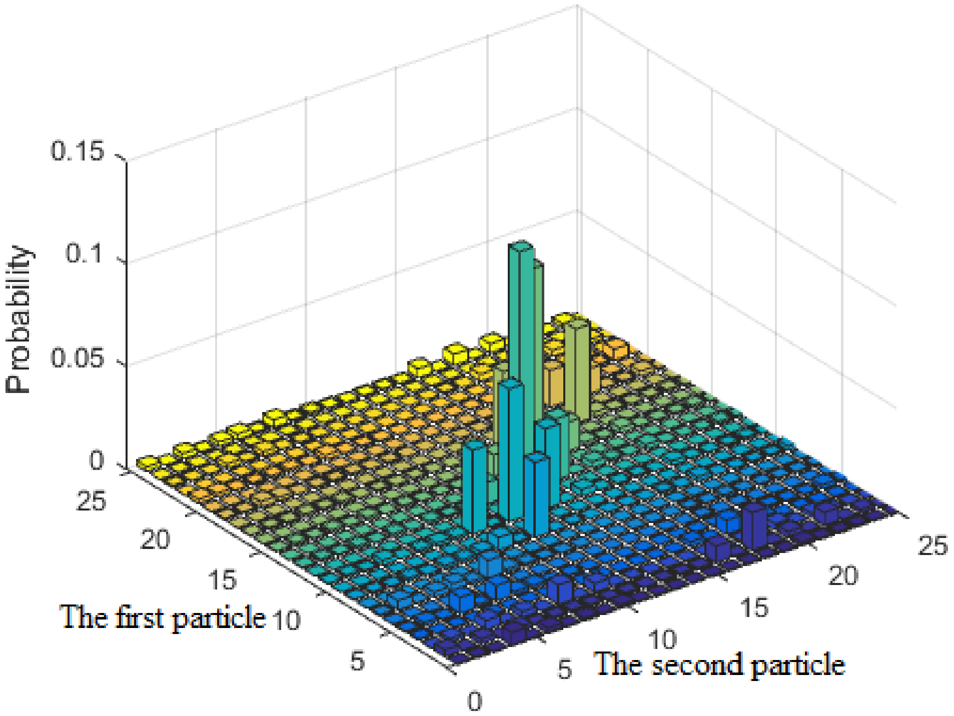


Figure 2.7: the probability distribution of running one-dimensional two-particle quantum walks on a circle with 25 vertices for 30 steps, where the initial coin particles are $H_{c_1} = |0\rangle$ and $H_{c_2} = |1\rangle$. It is obvious that for a circle with only odd N nodes, the probability has nonzero in any position if the number of steps r is greater than the number of nodes N (EL-Latif et al. (2020a)).

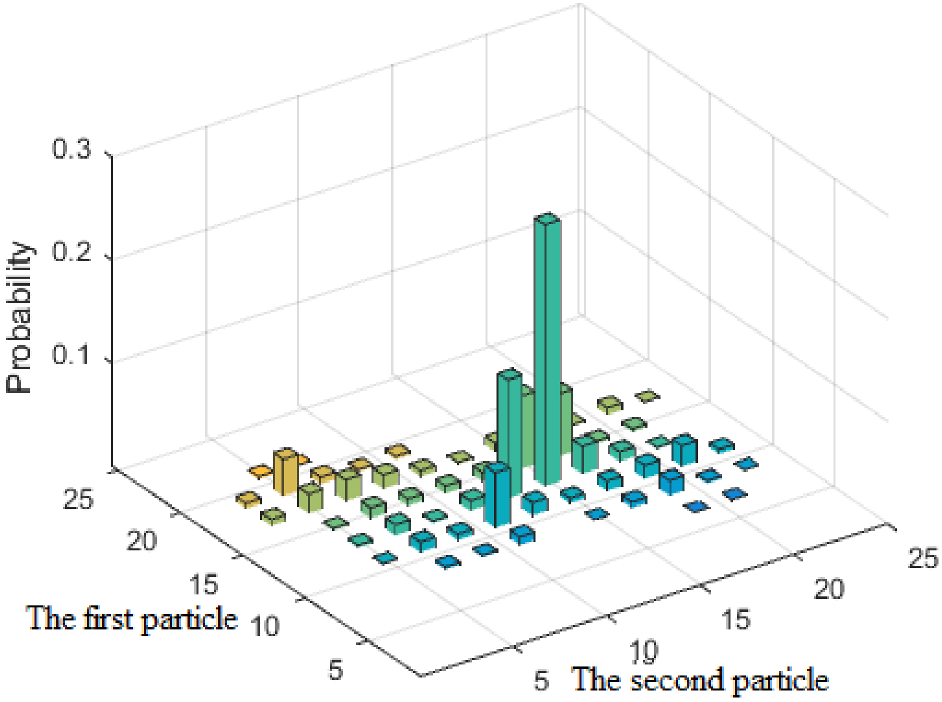


Figure 2.8: the probability distribution of running one-dimensional two-particle quantum walks on a circle with 25 vertices for 12 steps, where the initial coin particles are $H_{c_1} = |0\rangle$ and $H_{c_2} = |1\rangle$. It is obvious that for a circle with only odd N nodes, the probability has zero in some positions if the number of steps r is less than the number of nodes N (EL-Latif et al. (2020a)).

2.1.4 Alternate single-particle quantum walks on a circle

In this model of quantum walk, the evolution operator $\hat{U}$ can be expresed as stated in Eq. (2.10)

$$\hat{U} = \hat{S}_y(\hat{I} \otimes \hat{C})\hat{S}_x(\hat{I} \otimes \hat{C}) \tag{2.10}$$

Here, $\hat{S}_y$ refers to the shift operator running on y dimensional and can be defined as follows.

$$\hat{S}_y = \sum_{x,y}^{N} (|x,(y+1)\ mod\ N,0\rangle\langle x,y,0| + |x,(y-1)\ mod\ N,1\rangle\langle x,y,1|) \tag{2.11}$$

Also $\hat{S}_x$ can be defined as $\hat{S}_y$, which is running on x dimensional.

The probability of finding the particle at position *(x, y)* after r steps stated as follows

$$P(x,y,r) = \sum_{c\in\{0,1\}} |\langle x,y,c| \left(\hat{U}\right)^r |\psi\rangle_0|^2 \tag{2.12}$$

An illustrated example of the probability distributions for running alternating one-particle quantum walks on a circle with 25 vertices is provided in Figs. 2.9 and 2.10, where the initial position is $|00\rangle_p$, and the initial coin operator $\hat{C}$ is constructed with $\theta = \frac{\pi}{4}$. It is evident that for a circle with only odd N nodes, the probability $P(x, y, r)$ is nonzero in any position if the number of steps r is greater than or equal to the number of nodes N.

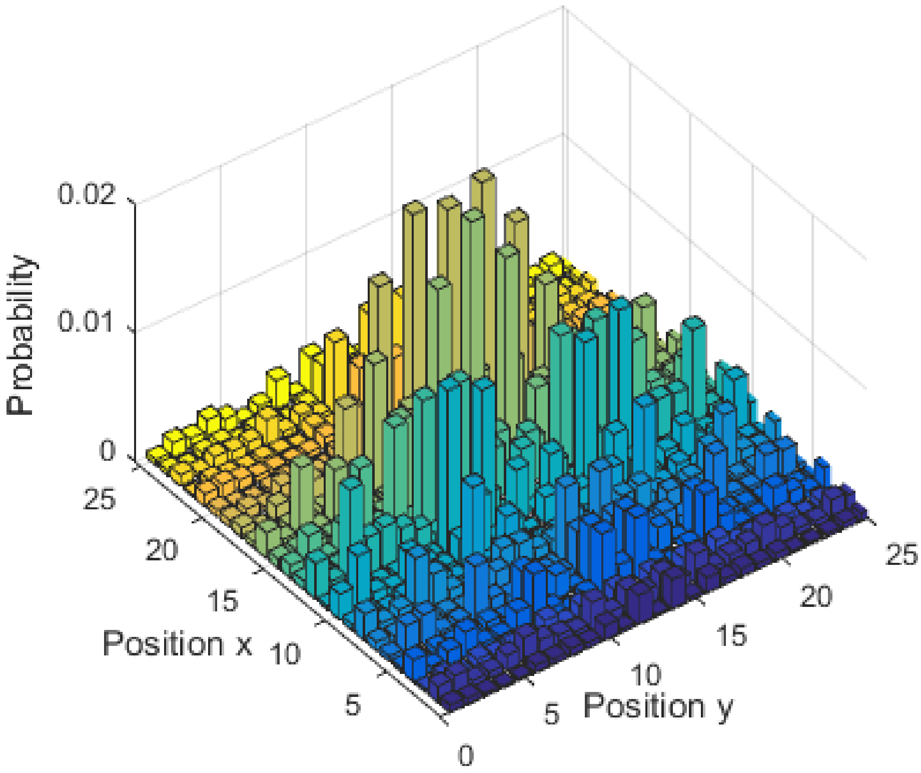


Figure 2.9: the probability distribution of running alternate quantum walks on a circle with 25 vertices for 30 steps, where the initial coin particle is $H_c = |0\rangle$. It is obvious that for a circle with only odd N nodes, the probability $P(x, y, r)$ has nonzero in any position if the number of steps r is greater than the number of nodes N (EL-Latif et al. (2020a)).

2.2 Cryptographic Applications of Quantum Walks

Quantum walks (QWs) are a computational paradigm in quantum computation, serving as the quantum mechanical counterpart to classical random walks. They have proven to be a powerful tool for developing quantum algorithms and

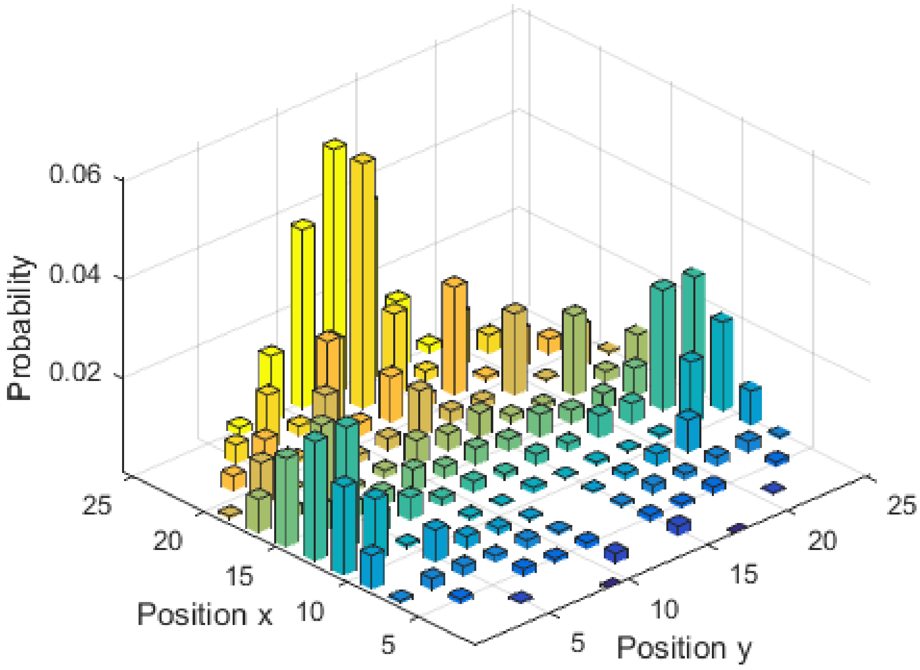


Figure 2.10: the probability distribution of running alternate quantum walks on a circle with 25 vertices for 12 steps, where the initial coin particle is $H_c = |0\rangle$. It is obvious that for a circle with only odd N nodes, the probability $P(x, y, r)$ has zero in some positions if the number of steps r is less than the number of nodes N (EL-Latif et al. (2020a)).

have recently been recognized as a universal model of quantum computation. Quantum walks find extensive applications in various domains, including cryptography, quantum algorithms, and quantum networking, among others (Li et al. (2013a); Yang et al. (2015); Yang and Zhao (2016); Yang et al. (2016a); Li et al. (2018a); Carson et al. (2015); Wong (2016); Konno et al. (2016)).

Discrete quantum walks have gained attention as a valuable resource for chaos-based encryption algorithms. Calculating the position probability distributions of quantum walkers involves squaring quantum amplitudes, i.e., squaring the norms of complex numbers. Consequently, discrete quantum walks can be seen as nonlinear mappings, where $\mathscr{H}$ represents the Hilbert space in which quantum walkers reside, and $\mathscr{P}$ denotes a set of probability distributions. This nonlinear behavior, along with the deterministic nature of quantum evolution and the high sensitivity to initial conditions (the position probability distributions of quantum walks depend on various factors, including the initial quantum state of walkers and coins), allows us to view discrete quantum walks as discrete-time and discrete-value chaotic systems (Yang et al. (2015); Alvarez and Li (2006)).

As a result, quantum walks offer significant potential as resources for designing secure cryptographic applications, including the creation of quantum hash functions, pseudo-random number generators, construction of substitution boxes, and image encryption mechanisms.

2.2.1 Pseudo-random number generator schemes

Pseudo-random number generators (PRNGs) play a vital role in the design of modern cryptographic mechanisms and are considered the backbone of many contemporary cryptographic applications. They are responsible for generating long keystreams of numbers with desired randomness properties, making the generated numbers crucial for designing robust cryptographic applications. Consequently, they have garnered significant attention from engineers and cryptographers. A well-designed PRNG mechanism should exhibit the robustness required of cryptographic primitives to ensure that attackers cannot regenerate or predict the secret data. There are various methods to design PRNG mechanisms, including the use of chaotic maps, cellular automata, and more (Vlassopoulos and Girau (2014); Lui et al. (2013); Akhshani et al. (2014); Francois et al. (2013); Hu et al. (2013); François et al. (2014); Özkaynak and Yavuz (2013); Li et al. (2019)).

However, with the accelerated progress of quantum computation, it has become apparent that many existing PRNG mechanisms may be vulnerable due to the potential power of quantum computation (Li et al. (2013a); Kiktenko et al. (2018)).

Discrete quantum walks have recently been recognized as a valuable resource for chaos-based cryptographic applications. This is because the computation of position probability distributions of quantum walkers involves squaring quantum amplitudes. Consequently, discrete quantum walks can be viewed as nonlinear mappings, where $\mathscr{H} \mapsto \mathscr{P}$. This non-linear behavior, combined with the deterministic nature of quantum evolution and the high sensitivity of quantum walks to initial conditions, allows us to consider discrete quantum walks as discrete-time and discrete-value chaotic systems (Yang et al. (2015); Alvarez and Li (2006)). As a result, quantum walks hold the potential to serve as resources for pseudo-random number generators.

There are various PRNG mechanisms based on quantum walks that have been suggested in prior works (Yang and Zhao (2016); Yang et al. (2016a)). Yang and Zhao (2016) introduced the first PRNG mechanism, which relies on one-dimensional one-particle quantum walks on a circle with V vertices. In the same year, Yang et al. (2016a) developed a quantum hash function and demonstrated its application for generating pseudo-random numbers using controlled one-dimensional two-particle quantum walks on a circle. However, it's important to note that running two-particle quantum walks requires more computational resources compared to one-particle quantum walks. Additionally, performing quantum walks on a one-dimensional structure results in a probability distribution with a dimension of V, whereas two-dimensional quantum walks produce probability distributions of dimension $V \times V$, making them more resilient against predictable collision attacks (Li et al. (2018a)). Addressing these limitations, EL-Latif et al. (2020a) designed a novel PRNG mechanism that combines the advantages of both PRNG methods proposed in (Yang and Zhao (2016); Yang et al. (2016a)) while avoiding the mentioned shortcomings. As physical quantum computing devices are not yet widely available, quantum-inspired frameworks provide a platform for simulating quantum algorithms. Within the constraints of digital computers, these quantum-inspired frameworks can partially replicate some of the quantum mechanical properties associated with the potential of quantum computation. Building on this concept, El-Latif et al. (2020a) introduced a new method for designing PRNG mechanisms based on cascaded quantum-inspired quantum walks and chaotic maps.

2.2.2 Quantum hash function schemes

Quantum walks can be thought of as non-linear mappings $Q : \mathscr{H} \mapsto \mathscr{P}$ where $\mathscr{H}$ is a Hilbert space in which the quantum walker lives and $\mathscr{P}$ is a set of probability distributions. This property, together with high sensitivity and other characteristics, allows us to consider quantum walks as chaotic systems. Consequently, quantum walks can be used for producing quantum hash functions (QHFs) (Li et al. (2013a); Yang et al. (2016a); Li et al. (2018a)). Li et al. (2013a) presented the first QHF based on one-dimensional two-particle quantum walks, and Yang *et al.* Yang et al. (2016a) utilized this QHF (Li et al. (2013a)) to present some applications in pseudo-random number generation, privacy amplification processes in quantum key distribution, and image encryption.

One of the main advantages of QHFs based on QWs is that the length of the hash value changes with respect to the number of vertices N in the circle. However, if the length of the bit string of the message is less than the number of nodes N, the system may be inefficient as some positions have zero probabilities. Quantum walk-based QHFs presented in (Li et al. (2013a); Yang et al. (2016a); Li et al. (2018a)) exhibit this limitation. To address this constraint, El-Latif et al. (2020d) developed two new QHFs to overcome this limitation and presented their applications in fifth-generation networks.

2.2.3 Image Encryption Schemes

Images are a widely used source of information for humans. As raw digital images can be maliciously manipulated and altered, safeguarding image data from unauthorized access has become a crucial issue studied by experts and researchers (Patel and Belani (2011)). Image encryption is a widely employed technique for protecting images, involving the transformation of an image from an understandable form into an unidentifiable form (El-Latif et al. (2014)).

Several quantum and classical image encryption techniques are based on quantum walk systems. Gong et al. (2016) introduced a quantum image encryption algorithm based on quantum controlled-NOT (C-NOT) operations controlled by Chen's hyper-chaotic system. Additionally, Liang et al. (2016) presented a quantum encryption algorithm based on generalized affine transforms and quantum C-NOT operations controlled by the logistic map. Tan et al. (2016) also presented a quantum color image encryption scheme based on similar ideas to Gong et al. (2016). Zhou et al. (2017) proposed a quantum image encryption algorithm that utilizes a 4-dimensional hyper-chaotic system and iterative Arnold transforms.

Furthermore, a variety of quantum and classical image encryption techniques based on quantum walks have been suggested in (Yang et al. (2015, 2016a)). Yang et al. (2015) introduced a classical image encryption approach based on two-particle quantum walks on a circle. Yang et al. (2016a) developed a quantum hash function and demonstrated its application in classical image encryption, which relies on the idea of controlled quantum walks from (Li et al. (2013a)). Abd-El-Atty et al. (2019a) presented a new quantum grayscale image encryption method based on quantum walks. EL-Latif et al. (2020a) designed a new pseudo-random number generator mechanism and applied it to color image encryption. Subsequently, several image encryption algorithms based on quantum walks were designed to provide enhanced security mechanisms (EL-Latif et al. (2020); El-Latif et al. (2020a)).

2.3 Chaotic Maps

In the digital era of processing multimedia data by nearly all electronic devices, technologists, researchers, and scientists are actively engaged in designing and developing robust cryptosystems. With images being a ubiquitous source of digital data in today's world, cryptosystem developers are increasingly focused on techniques that secure the actual image information in a way that makes it impossible for adversaries to unveil. In more concrete terms, images can be viewed as matrices of numbers. An encryption algorithm, through a series of reversible operations, obscures the actual pixel values. To achieve enhanced security, four main parameters should be emphasized: the design of efficient confusion and diffusion strategies, the reduction of pixel correlation, increased entropy of encrypted images, and a large key space.

It is observed that due to the high correlation among image pixels, widely-used encryption mechanisms like Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are not effectively suitable for image encryption. The active area of research in designing encryption algorithms for images is chaos-based cryptography (Amin and EL-Latif (2010); Belazi et al. (2015)). It primarily involves the processing of images with a sequence of random numbers generated by a chaotic system. Chaotic systems are mathematical functions with a property of sensitivity to primary parameter values. The values of parameters or constants in chaotic maps act as keys in the cryptosystem. Various researchers employ maps such as the Lorentz map, Arnold-Tent map, Cat map, etc., to generate random numbers used to modify original pixel values (substitution or diffusion) and alter the positions of actual pixel values (permutation or confusion). To enhance security on all levels, researchers incorporate concepts such as DNA sequence operations (Wang et al. (2015)), Cellular Automata (Zhang et al. (2014)), substitution-boxes (Abd-El-Atty et al. (2019b); Ali and Khan (2019)), finite-state machines (Waseem and Khan (2019)), fractal sorting matrices (Xian and Wang (2021)), bit-level permutations (Gan et al. (2018)), compressive sensing (Chai et al. (2020a,b)), etc., in combination with chaos-based cryptography.

As previously explained, the permutation-substitution process determines the level of security achieved by the final ciphered image. It is considered the two fundamental encryption steps. Most researchers primarily focus on developing an efficient permutation strategy by devising a separate shifting algorithm to effectively conceal the original image information. Traditional image permutation mechanisms like sort-based, Arnold-based, Baker-based, cyclic shift-based, etc., have disadvantages, such as weak permutation and high time complexity (Wang et al. (2019)). Addressing these limitations, Wang et al. (2019) introduced a new permutation method to achieve low time complexity by combining cyclic shift with sorting. Additionally, Hua et al. (2015) presented a new permutation mechanism called the "chaotic magic transform," using a two-dimensional chaotic system to achieve low time complexity and efficient permutation of image pixels. In the substitution step, pixel values are altered, primarily through the XOR operation between random sequences generated by chaotic maps and the image matrix. Researchers have maximum flexibility in choosing the steps in the encryption algorithm. The choice between permutation and substitution is influenced by three factors: the step must be reversible, produce improved evaluation parameters, and run at high speed.

In their recent work, researchers have been concentrating on the design of one-dimensional (1-D) chaotic systems (Wang et al. (2019); Zhou et al. (2014a); Li et al. (2017)) and multi-dimensional chaotic maps (Xian and Wang (2021); Gan et al. (2018); Chai et al. (2020a,b)) with exclusive applications in image encryption. Each work aims to enhance various aspects of security analysis. One-dimensional chaotic systems offer benefits such as ease of design, low computational complexity, high-speed processing, and a simple structure. However, 1-D maps are vulnerable to multiple attacks due to their small key-space and chaotic discontinuous ranges (Zhou et al. (2014a)).

Chaotic systems play a crucial role in modern cryptosystem design. In the following subsections, we provide details of the chaotic systems utilized.

2.3.1 Logistic-Chebyshev map

Logistic-Chebyshev map is an integration of two common 1-D chaotic systems: Logistic and Chebyshev. It can be expressed as given in Eq. (2.13) (Abd-El-Atty et al. (2019b)).

$$LC_{i+1} = \left[\alpha \times LC_i(1-LC_i) + \frac{(4-\alpha)\cos(A \times \arccos(LC_i))}{4}\right] mod 1 \tag{2.13}$$

where $\alpha \in (0,4)$ is the control parameter, $LC_0 \in (0,1)$ is the primary value of the system, and $A \in N$ is the degree of the chaotic map.

2.3.2 Logistic-Sine map

The logistic-Sine map is an integration of two 1-D chaotic maps: The logistic map and the Sine map, which can be expressed as given in Eq. (2.14) (Zhou et al. (2014a)).

$$LS_{i+1} = \left(\beta(LS_i - LS_i^2) + (4-\beta)\sin(\pi \times LS_i)/4\right) mod\ 1 \tag{2.14}$$

here$\beta \in (0,4)$is the control parameter and$LS_0 \in (0,1)$is the original value.

2.4 Conclusion

This chapter has presented the fundamental concepts of quantum walks. Quantum walks are generalizations of random walks with extensive applications in various fields, including cryptography, quantum algorithms, and quantum networking. Quantum walks can be either continuous or discrete models of computation, depending on how time is measured ($t \in \mathscr{R}^+ \cup \{0\}$ for the continuous case and $t \in \mathscr{N} \cup \{0\}$ for the discrete case). Continuous-time quantum walks evolve via the Schrödinger equation, while discrete-time quantum walks evolve via Unitary operators. In both cases, quantum walks have been studied mathematically and computationally on graphs.

Discrete quantum walks have recently been recognized as valuable resources for chaos-based encryption algorithms. This recognition stems from the computation of position probability distributions of quantum walkers, which involves squaring quantum amplitudes or, in other words, squaring norms of complex numbers. As a result, discrete quantum walks can be regarded as nonlinear mappings $Q : \mathscr{H} \mapsto \mathscr{P}$, where $\mathscr{H}$ represents the Hilbert space in which quantum walkers exist, and $\mathscr{P}$ represents a set of probability distributions (Nayak and Vishwanath (2000); Aharonov et al. (1993, 2001)). The combination of this non-linear behavior with the deterministic nature of quantum evolution and the heightened sensitivity of quantum walks to initial conditions, including the initial quantum state of walkers and coins, allows us to perceive discrete quantum walks as discrete-time and discrete-value chaotic systems. Consequently, quantum walks offer promising resources for designing secure cryptographic applications, such as the development of quantum hash functions, pseudo-random number generators, construction of substitution boxes, and image encryption mechanisms.

Additionally, this chapter has provided background information on the chaotic systems used. Chaotic systems are mathematical functions with the property of sensitivity to primary parameter values. Recent research has focused on designing one-dimensional (1-D) chaotic systems and multi-dimensional chaotic maps for image encryption, with a primary goal of enhancing various aspects of security analysis. 1-D chaotic systems offer significant advantages, including ease of design, low computational complexity, high-speed processing, and simple structures. However, 1-D maps are susceptible to certain attacks due to their initial values having a small key space and chaotic discontinuous ranges.

CHAPTER 3

METHODOLOGY

3.1 Introduction

Data security is of paramount importance in the context of data transfer within IoT-based smart cities. Cryptographic mechanisms serve as the linchpin for ensuring the confidentiality of data security, enabling secure communication between two parties while safeguarding against potential third-party eavesdroppers. Modern cryptographic applications heavily rely on essential components such as hash functions, pseudo-random number generators, and substitution boxes.

Chaotic maps have emerged as a common foundation in the development of modern cryptographic applications. Within this domain, one-dimensional chaotic systems are frequently employed due to their straightforward design and low computational complexity. Nevertheless, one-dimensional chaotic maps are susceptible to various forms of attacks, primarily stemming from their limited key space and chaotic, non-continuous characteristics. To harness the advantages of one-dimensional chaotic maps while mitigating their vulnerabilities, the approach of cascading two integrated one-dimensional chaotic systems is adopted.

As quantum computing continues to advance rapidly, the foundations of many modern cryptographic mechanisms face the risk of being compromised due to their reliance on mathematical computations. Consequently, the exploration of cryptographic mechanisms rooted in quantum technologies offers a promising path to designing secure and reliable cryptographic applications tailored to IoT-based smart systems.

3.2 Research Framework

Smart cities are enhanced urban infrastructures that aim to provide citizens with a high quality of life by efficiently delivering various services, such as transportation, e-governance, waste management, healthcare, education, and water supply. These cities leverage information and communication technologies to achieve the desired level of service delivery. The smart city environment involves collecting data from various sensors, devices, and people, which is then processed to make informed decisions. A significant volume of data is generated daily through various smart city applications. To efficiently store and manage this data, cloud servers are deployed. Cloud computing enables access to various services hosted remotely.

Within the context of smart cities, data security, authenticity, and integrity policies are paramount, as smooth data transmission and storage are essential. Ensuring the privacy of digital contents is of utmost importance (Shahzadi, 2020; Awan, 2020).

In this research framework, we aim to harness the power of quantum computation and quantum walks to address data security challenges in the IoT-based smart city environment. Our objectives include:

- Developing new secure data transmission protocols based on quantum walks/chaotic maps for IoT-based smart systems.

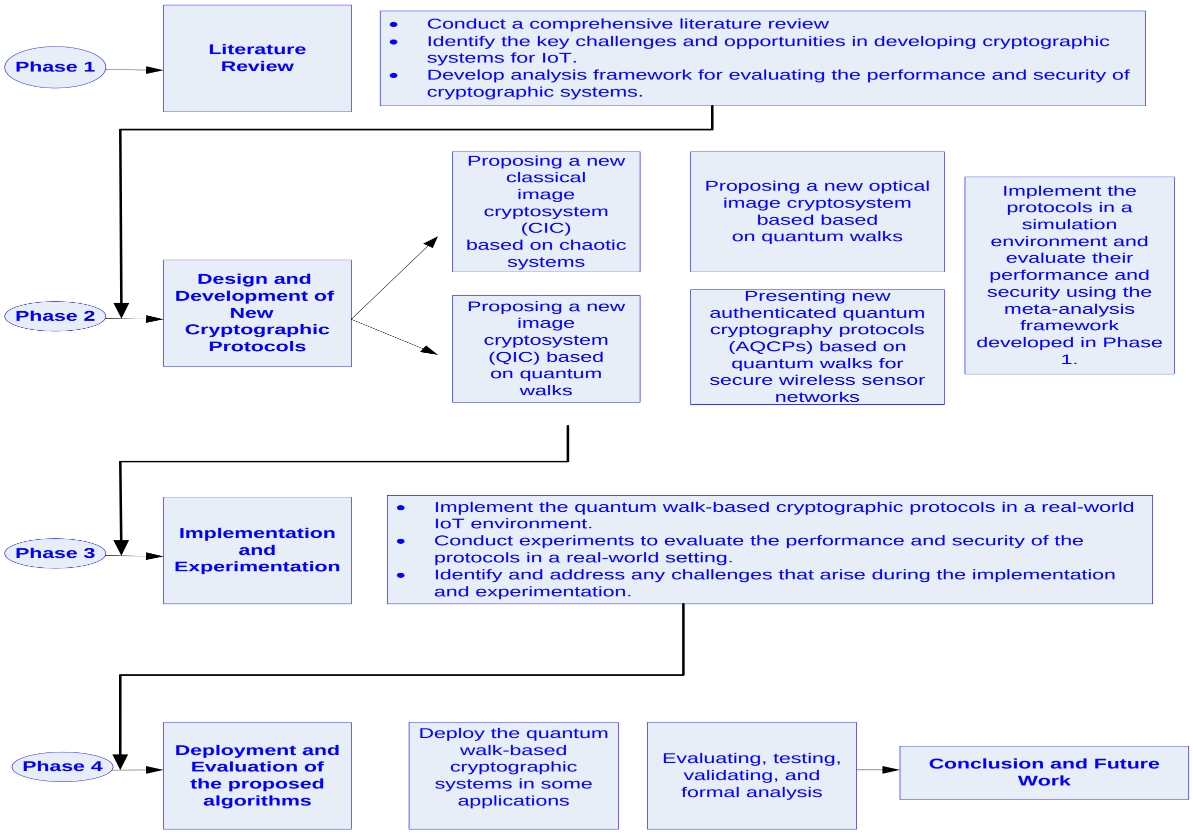

Phase 1
Literature Review
Conduct a comprehensive literature review
Identify the key challenges and opportunities in developing cryptographic systems for IoT.
Develop analysis framework for evaluating the performance and security of cryptographic systems.
Phase 2
Design and Development of New Cryptographic Protocols
Proposing a new classical image cryptosystem (CIC) based on chaotic systems
Proposing a new image cryptosystem (QIC) based on quantum walks
Proposing a new optical image cryptosystem based based on quantum walks
Presenting new authenticated quantum cryptography protocols (AQCPs) based on quantum walks for secure wireless sensor networks
Implement the protocols in a simulation environment and evaluate their performance and security using the meta-analysis framework developed in Phase 1.
Phase 3
Implementation and Experimentation
Implement the quantum walk-based cryptographic protocols in a real-world IoT environment.
Conduct experiments to evaluate the performance and security of the protocols in a real-world setting.
Identify and address any challenges that arise during the implementation and experimentation.
Phase 4
Deployment and Evaluation of the proposed algorithms
Deploy the quantum walk-based cryptographic systems in some applications
Evaluating, testing, validating, and formal analysis
Conclusion and Future Work

Figure 3.1: Research Framework

- Designing new visual cryptographic protocols based on quantum walks/chaotic maps for IoT-based smart systems.

The proposed cryptosystem will encrypt digital image data captured in the smart city environment, which may include medical information, real-time traffic data, weather conditions, and security-related information. The encrypted image data can then be securely transferred and stored in interconnected cloud servers. Users at the receiving end can utilize the image data after applying the decryption mechanism. By storing the data in an encrypted form on cloud servers, unauthorized individuals will not be able to access and interpret the information.

Figure 3.1 displays the proposed framework for secure data transfer in an

IoT-based smart city. The image data might represent medical information of patients, live traffic blocks and violations, climatic conditions, suspicious individuals, etc. The encrypted image can be transferred and stored in interconnected cloud servers. Users at the other end can utilize the image data after applying the decryption mechanism. Since the data is stored in an encrypted form on cloud servers, opponents must not be able to view and interpret it.

Phase 1: The study of security analysis of multimedia data, including attacks on cryptographic systems, is essential for the design and implementation of new schemes. By addressing the drawbacks of existing cryptosystems, we can avoid them in future ones. Conducting a state-of-the-art review of chaos-based cryptosystems should be performed, classifying them based on the type of chaotic system used, the type of encryption method (stream cipher or block cipher), and the targeted application. A comprehensive analysis of these schemes will be carried out to identify their common drawbacks.

Phase 2: Investigation of new multimedia security based on chaotic systems/quantum walks. Chaotic maps are commonly used in designing modern cryptographic applications, with one-dimensional (1D) chaotic systems being widely used due to their simple design and low computational complexity. However, 1D chaotic maps are vulnerable to various attacks due to their chaotic discontinuous ranges and small key space. To combine the advantages of 1D chaotic maps and avoid their drawbacks, we have utilized the cascading of two integrated 1D chaotic systems. In this phase, we present an image cryptosystem for data transfer in cloud-based smart cities using the cascading of Logistic-Chebyshev and Logistic-Sine maps. Logistic-Sine map is employed to permute the plain image, and Logistic-Chebyshev map is used to substitute the permuted image, while the cascading of both integrated maps is used to perform an XOR procedure on the substituted image. Traditional cryptosystems may be vulnerable with the growth of quantum resources. Therefore, new cryptosystems based on quantum concepts are needed. In this phase, we propose a novel image cryptosystem using quantum walks. The image data might represent medical information of patients, live traffic blocks and violations, climatic conditions, suspicious individuals, etc. The encrypted image data can be transferred and stored in interconnected cloud servers. Users at the other end can utilize the image data after applying the decryption mechanism. Since the data is stored in an encrypted form on cloud servers, opponents should not be able to view or interpret it.

Phase 3: Design of partial encryption protocols based on quantum walks for IoT-based smart systems. In potential applications for quantum cryptographic protocols in IoT, we anticipate that there will be a need to employ quantum cryptographic protocols (QKD, AQKD, QHF, S-boxes, or PRNG) to encrypt and share data stored in cloud servers in the near future. A demonstration of the envisioned QIoT framework is presented in Fig. 3.2. In this approach, all communication takes place via one of the quantum cryptographic protocols. By incorporating quantum mechanics into all aspects of key management, access control, decryption, and encryption, an additional layer of tamper-proof data security will be provided. This integration not only prevents unauthorized access to data but also prepares for the ubiquity of soon-to-be-realized quantum hardware with minimal upgrades. Such QIoT frameworks will consist of connected devices that can communicate with each other using quantum-authenticated protocols to transmit secret information and share secure keys. It is expected that such a network will facilitate the storage and sharing of data by using a quantum cryptographic protocol to encrypt the data before uploading it to the cloud.

QKD protocols are investigated to enable two participants with fully quantum capabilities to share a random secret key, while SQKD protocols are designed to perform the same task using fewer quantum resources to make quantum communications more achievable and practical. Quantum walks play an essential role in quantum computing, which is a universal quantum computational paradigm. In this work, we leverage the advantages of quantum walks to design three authenticated quantum cryptographic protocols based

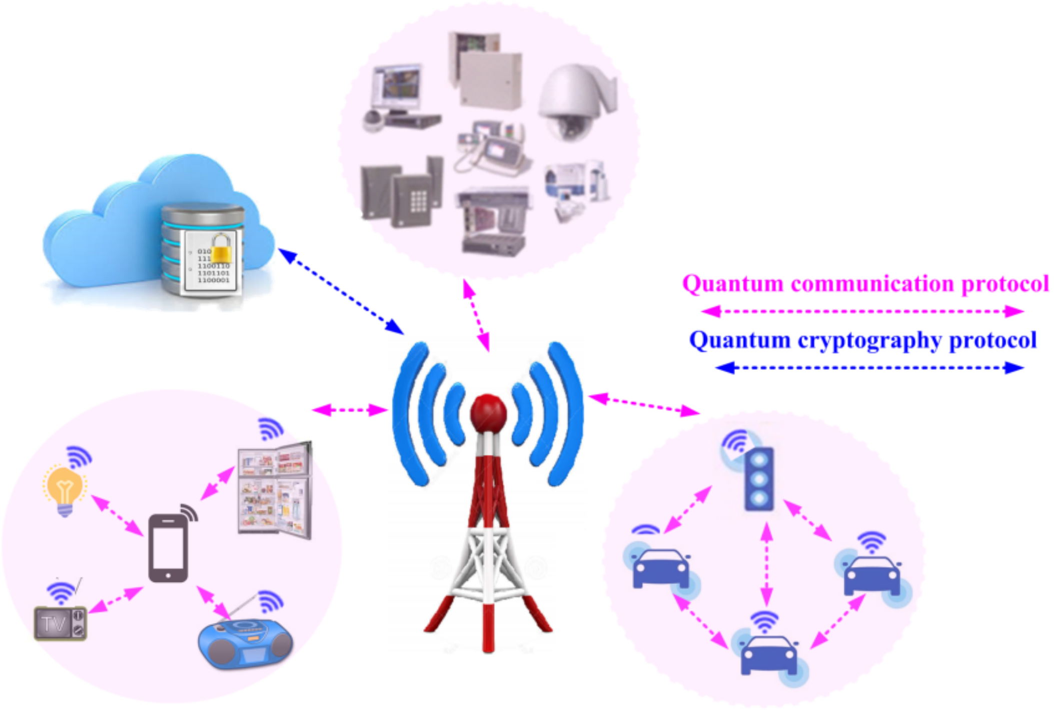


Figure 3.2: Framework for viable quantum Internet of things

on quantum walks: the first one is AQKD, the second one is ASQKD with one of the two participants having limited quantum capabilities, and the last one is authenticated semi-quantum key distribution, with both legitimate users possessing limited quantum resources. The advantages of the proposed protocols are that the partners can exchange several different keys with the same exchanged qubits, and the presented protocols rely on a one-way quantum communication channel. In contrast, all previously designed SQKD protocols relied on two-way quantum communication. Security analyses confirm that the presented protocols are secure against various well-known attacks and highly efficient.

Also, in this phase, we propose a new optical encryption approach based on quantum walks and the double random phase encoding technique. Quantum walks have been proven to be an excellent tool for designing modern cryptographic mechanisms due to their ability to resist potential attacks from both digital and quantum computers. In the proposed approach, we use alternate quantum walks (AQW) at two encryption stages. First, inner encryption and encoding by double random phase encoding (DRPE) are executed using permutation followed by substitution. Furthermore, AQW is adapted to generate two random masks for the DRPE process.

Wireless Sensor Networks (WSNs) have become a fundamental technological component for intelligent communities due to their potential benefits. The applications of WSNs extend from body area networks to local and home area networks, and further to a wide variety of services in smart cities Akerele et al. (2019). However, applications of WSNs lack stringent privacy and security protection due to the involvement of human life.

The architecture of WSNs and the limited nature of the node's resources make it vulnerable and susceptible to numerous attacks. In addition, an adversary can intercept and subsequently fabricate sensitive data to be transmitted as the original data. Moreover, an attacker can pass incorrect data and even impersonate a sensor itself and modify the collected data. If the communication of sensor nodes is not secure, then a malicious entity can extract the transmitted data and the code associated with that node, leading to many security threats and challenges.

Also, with the development of quantum technologies, many cryptographic mechanisms may be vulnerable due to the promising capabilities of quantum computers. Therefore, security and privacy are significant challenges for WSNs that require new cryptographic mechanisms to withstand potential attacks from digital computers and quantum computers. For these reasons, the goal of this paper is to design new authentication protocols for secure wireless communication based on quantum technologies and open the door for integrating quantum technologies with wireless sensor networks and various Internet of Things devices to achieve high security and efficiency. The suggested scenario for wireless sensor communications in the quantum scenario is presented in Fig. 3.3.

Phase 4: Investigate new solutions for interoperability between copyright protection and encryption for various applications: To address the security

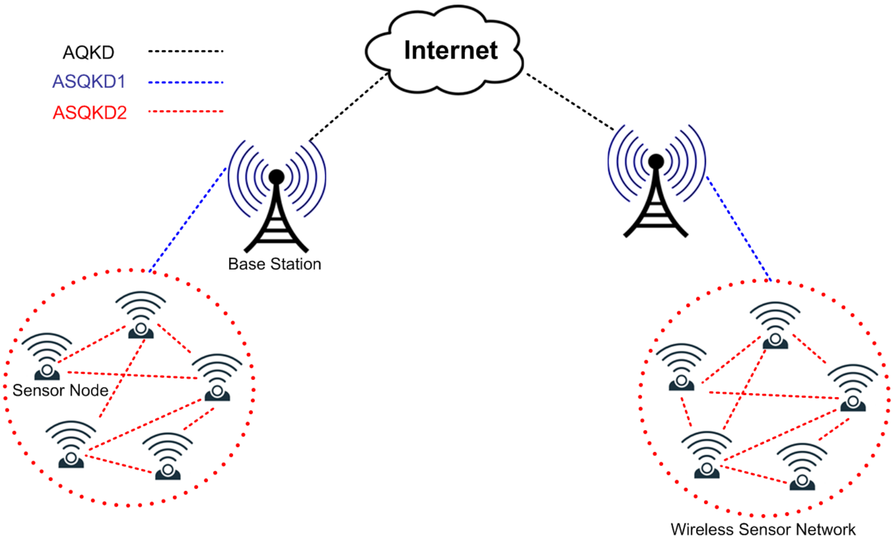


Figure 3.3: The suggested scenario for wireless sensor communications in quantum scenario

vulnerabilities we have identified, our goal is to intelligently integrate watermarking, encryption, and compression.

3.3 Conclusion

In this Chapter, we have investigated nonlinear dynamical systems, discrete chaotic systems, and quantum walks and have adapted them to enhance existing approaches and/or design new approaches for securing multimedia data transmitted in smart IoT systems.

In this project, the plan for designing secure quantum cryptographic protocols for IoT devices includes:

1. Identifying the advantages and limitations of these protocols. This will involve evaluating the various quantum cryptographic protocols that are available and identifying their strengths and weaknesses.

2. Developing new quantum communication protocols based on quantum walks to enhance the security of IoT-based smart systems and enable implementation in both classical and quantum environments. This will involve designing new quantum protocols that are specifically tailored to

the needs of IoT environments. The protocols should be efficient, secure, and implementable in both classical and quantum environments.

3. Simulating the proposed quantum protocol. This will involve developing a simulator for the proposed quantum protocol and using it to evaluate its performance and security under different conditions.

4. Analyzing the results of the proposed protocol and comparing it with other related protocols. This will involve comparing the proposed protocol to other state-of-the-art quantum cryptographic protocols in terms of its efficiency, security, and feasibility of implementation in IoT environments.

CHAPTER 4

PROPOSED METHODS

4.1 Introduction

In smart city environments, the data generated from various sources (smart city applications) are usually kept inside a cloud server and is manipulated by the concerned government officials and citizens of the city (Huang et al. (2017); Zhang et al. (2017)). The data of citizens include healthcare information, purchase behavior, weather conditions, environmental changes, transport information, etc. The majority of the data take the form of images. Image data concerning the day to day activities of people are very sensitive and critical. In order to save the data from exploitation by third parties, designing efficient encryption mechanisms are needed so that it can be integrated with the cloud system for secure storage.

The objective of this chapter is to design new security and privacy mechanisms for cloud/fog-assisted IoT applications.

4.2 Classical image cryptosystem (CIC)

Cascading systems are the solution to possess the benefits of iterating 1-D chaotic maps and avoiding their drawbacks. In the literature, Zhou et al.

(2014b) proposed a new cascaded system of two 1-D systems (Tent, Sine, Logistic) and presented its application in image encryption. In this study, a new image cryptosystem is reported, named as CIC, using the cascading of two integrated 1-D chaotic systems (Logistic-Chebyshev, Logistic-Sine). In the suggested cipher approach, Logistic-Sine system is utilized to permutated the plain image and Logistic-Chebyshev map, in Zhou et al. (2014b), is used for substituting the permuted image, while the cascading of both integrated maps is utilized in performing XOR process on the substituted image. The architecture of the proposed approach is provided in Figure 4.1, whereas the encryption processes are provided in Algorithm 1.

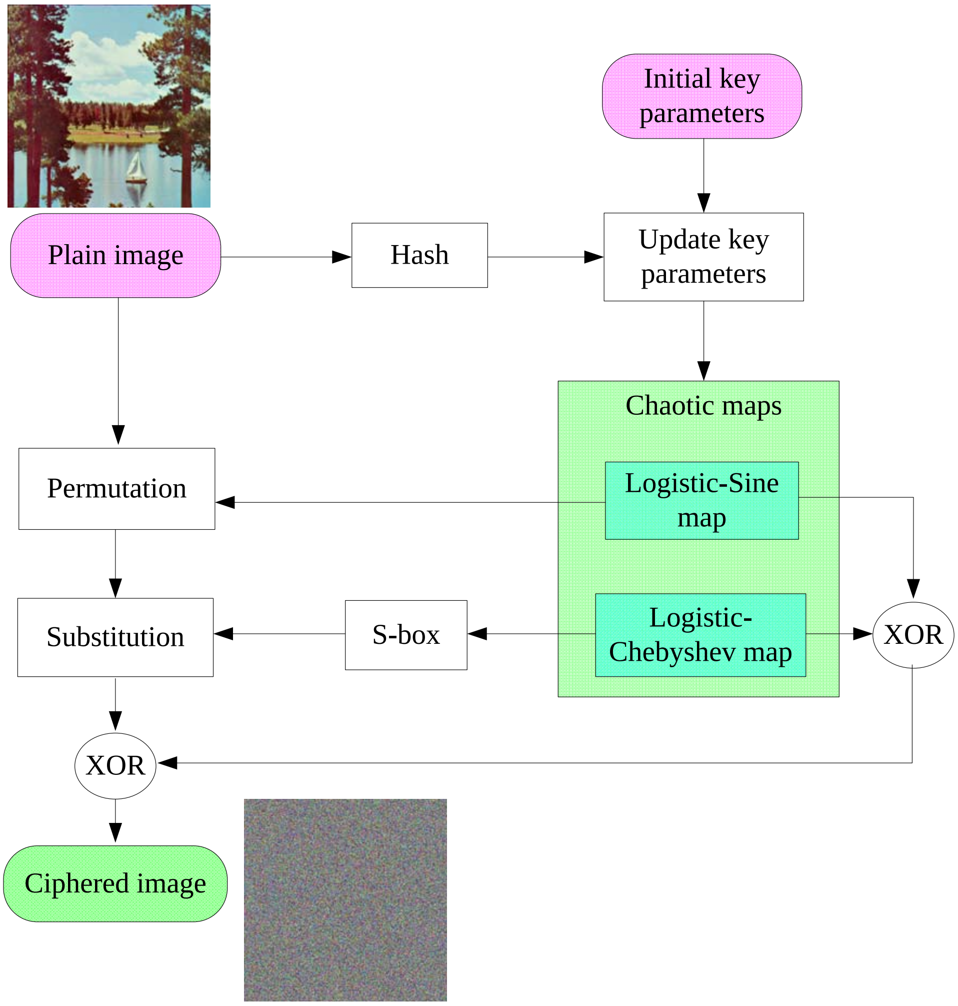


Figure 4.1: The architecture of the proposed image cryptosystem

Algorithm 1: Encryption algorithm

```
Parameters:$LS_0$, $\beta$, $LC_0$, $\alpha$, $A$ // Used for iterating chaotic maps.
Input: Plain image ($P$)
Output: Cipher image ($C$) and decimal values ($H_1$, $H_2$, $H_3$, and $H_4$)
$[m\, n\, c] \leftarrow size(p)$// Get image dimension
$Hb \leftarrow hash(P)$// Compute the hash value $Hb$ for image $P$ using SHA-256 algorithm.
$H \leftarrow uint8(Hb)$// Convert the 256-bit hash value to 32 integer values $h_1$, $h_2$, ..., $h_{32}$, where each integer composed of 8-bit.
$H_1 \leftarrow (h_1 \oplus h_2 \oplus \cdots \oplus h_8)/256$;
$H_2 \leftarrow (h_9 \oplus h_{10} \oplus \cdots \oplus h_{16})/128$;
$H_3 \leftarrow (h_{17} \oplus h_{18} \oplus \cdots \oplus h_{24})/256$;
$H_4 \leftarrow (h_{25} \oplus h_{26} \oplus \cdots \oplus h_{32})/128$;
// Update initial key parameters ($LS_0$, $\beta$, $LC_0$, $\alpha$) using $H_1$, $H_2$, $H_3$, and $H_4$
$LC_0 \leftarrow (LC_0 + H_1)/2$;
$\alpha \leftarrow \alpha/2 + H_2$;
$LS_0 \leftarrow (LS_0 + H_3)/2$;
$\beta \leftarrow \beta/2 + H_4$;
$LC \leftarrow Logistic-Chebyshev(LC_0, \alpha, A, m \times n \times c)$// Using the updated key parameters ($LC_0$, $\alpha$, $A$), operate Logistic-Chebyshev map for $m \times n \times c$ times to generate sequence $LC$, wherever the size of $P$ is $m \times n$ and $c$ denotes the number of color channels.
$LS \leftarrow Logistic-Sine(LS_0, \beta, m \times n \times c)$// Using the updated key parameters ($LS_0$, $\beta$), operate Logistic-Sine system for $m \times n \times c$ times to create sequence $\{LS\}$.
$KC \leftarrow fix\left(LC_i \times 10^{12} mod\ 256\right)$// Convert sequence $LC$ into integer values.
$KS \leftarrow fix\left(LS_i \times 10^{12} mod\ 256\right)$;
$PerIm \leftarrow permutation(P, KS)$// Permute the input image ($P$) using the sequence $KS$ and chaotic magic transform method presented in (Hua et al. (2015)).
$Sbox \leftarrow unique(KC)$// Collect the first 256 unequal elements in the sequence $\{KC\}$ to construct the substitution box (S-box).
// Substitution process.
for $i \leftarrow 1 to m$ do
    for $j \leftarrow 1 to n$ do
        for $k \leftarrow 1 to c$ do
            $Sim(i,j,k) \leftarrow Sbox(PerIm(i,j,k) + 1)$;
$Key \leftarrow KS \oplus KC$// Cascade both sequences ($KC$ and $KS$) to generate the key sequence $Key$.
$C \leftarrow Sim \oplus key$// Cipher image
End of the algorithm
```

4.3 Quantum Image Cryptosystem (QIC)

With the rapid development of quantum resources, many existing cryptographic mechanisms are now susceptible to attacks (EL-Latif et al. (2019b,a)). Consequently, there is a need for quantum technology to be employed in designing secure image encryption systems. Quantum walks (QWs) are a quantum tool used in designing quantum algorithms and possess robust characteristics such as non-periodicity, stability, and theoretically infinite key space to resist various attacks (Abd-El-Atty et al. (2019a)).

Leveraging the power of QWs, several researchers have developed novel quantum/classical cryptosystems based on QWs (Abd-El-Atty et al. (2019a); El-Latif et al. (2020d); EL-Latif et al. (2020); El-Latif et al. (2020c); Yan and Li (2021); Yang et al. (2015, 2016a); Abd-El-Atty et al. (2020); El-Latif et al. (2020a); EL-Latif et al. (2020a); Alanezi et al. (2021); El-Latif et al. (2020)) to withstand attacks from quantum and classical computers. For instance, Abd-El-Atty et al. (2019a) introduced the first quantum image encryption using one-walker QWs, and El-Latif et al. (2020d) harnessed the power of QWs to construct substitution boxes, which were subsequently used in designing video and file cryptosystems. EL-Latif et al. (2020) designed a new image cryptosystem using QWs to preserve privacy in the context of the Internet of Things, and Alanezi et al. (2021) utilized the benefits of QWs in designing an optical image cryptosystem. However, the current quantum resources available are insufficient for realizing full-scale QWs. Therefore, authors in (Abd-El-Atty et al. (2020); El-Latif et al. (2020a); Abd El-Latif et al. (2021)) have designed new cryptosystems using quantum-inspired QWs to be applicable in digital device environments and to withstand quantum attacks during and after the transition to the quantum realm.

In this section, we introduce a novel image cryptosystem called QIC, which employs quantum-inspired QWs for confidential data transmission in the form of images. In this encryption approach, QWs are used to substitute the original image and then acquire certain information about the substituted image. This information is then utilized to perform QWs again and encrypt the substituted image. The encryption procedures of this proposed approach are illustrated in Figure 4.2, and the detailed steps are outlined in Algorithm 2.

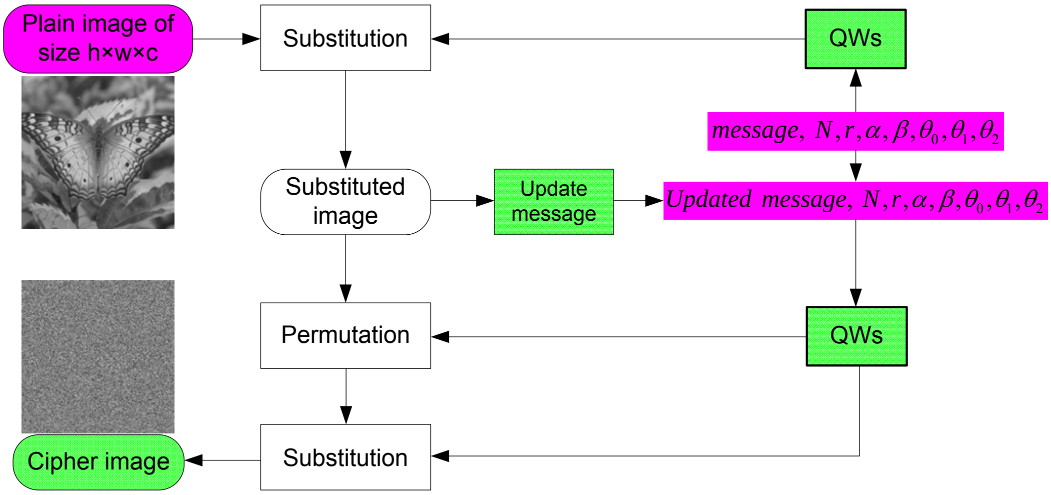

Plain image of size h×w×c
Substitution
QWs
message, $N, r, \alpha, \beta, \theta_0, \theta_1, \theta_2$
Substituted image
Update message
Updated message, $N, r, \alpha, \beta, \theta_0, \theta_1, \theta_2$
Permutation
QWs
Cipher image
Substitution

Figure 4.2: An illustration of the encryption technique for the presented encryption approach

4.4 Optical Image Cryptosystem (OIC)

Optical information processing, with its parallel capabilities, is heavily integrated into our daily lives. However, the advancements in optical information technology have given rise to new security and privacy concerns, particularly in the context of optical data storage and transmission (Kumar and Bhaduri (2017); Azoug and Bouguezel (2016)). One common approach to securing optical data is optical image encryption. Among the earliest techniques for image encryption is the double random phase encoding (DRPE) method (Refregier and Javidi (1995)). This technique employs two random phase masks, where the first mask operates in the spatial domain and the other mask in the Fourier domain to encode optical images.

Various transforms have been explored as alternatives to the Fourier transform to enhance the security of optical cryptographic systems based on DRPE (Nakano and Suzuki (2020); Su et al. (2020); Dou et al. (2019); Chen et al.

Algorithm 2: Encryption algorithm

```
Parameters: message, N, r, $\alpha$, $\beta$, $\theta_0$, $\theta_1$, $\theta_2$ // Used for operating
    QWs on a cycle of N-node for r-step and controlled by
    the binary string message.
Input: Plain image (PnImg)
Output: Cipher image (EncImg) and $SumPix$
$[h\ w\ c] \leftarrow size(PnImg)$// Get image dimension
$P1 \leftarrow QWs(message, N, r, \alpha, \beta, \theta_0, \theta_1, \theta_2)$;
$RP1 \leftarrow resize(P1, [1 h \times w \times c])$// Resize P1 to the size of the
    plain image PnImg
$Key1 \leftarrow fix(RP1 \times 10^{12} mod 256)$// convert $RP1$ into integers.
$Key1 \leftarrow reshape(Key1, h, w, c)$;
$SubImg1 \leftarrow PnImg \oplus Key1$// Perform Bit-XORed process.
// Update the binary string.
$SumPix \leftarrow \sum_i^h \sum_j^w \sum_k^c SubImg1(i, j, k)$;
$Updatedmessage \leftarrow dec2bin(SumPix)$
$P2 \leftarrow QWs(Updatedmessage, N, r, \alpha, \beta, \theta_0, \theta_1, \theta_2)$;
// Create two permutation boxes for shuffling the
    substituted image SubImg1, where the first box is acting
    to shuffle rows and the other one is acting to shuffle
    columns.
$RH \leftarrow resize(P2, [1\ h])$// Resize P2 to the number of rows ($h$)
$SH \leftarrow sort(RH)$// Arranging the elements in ascending order.
$PrH \leftarrow index(SH, RH)$;
$RW \leftarrow resize(P2, [1\ w])$;
$SW \leftarrow sort(RW)$;
$PrW \leftarrow index(SW, RW)$;
// Permutate SubImg1 using permutation boxes PrH and PrW.
for $i \leftarrow 1 to\ h$ do
    for $j \leftarrow 1 to\ w$ do
        $PrImg(i, j, :) \leftarrow SubImg1(PrH(i), PrW(j), :)$;
// Construct a substitution box of 256 elements.
$RSb \leftarrow resize(P2, [1\ 256])$;
$SB \leftarrow sort(RSb)$;
$Sbox \leftarrow index(SB, RSb)$;
// Substitute PrImg using the constructed Sbox.
for $i \leftarrow 1 to\ h$ do
    for $j \leftarrow 1 to\ w$ do
        for $j \leftarrow 1 to\ c$ do
            $SbImg(i, j, k) \leftarrow Sbox(PrImg(i, j, k) + 1)$;
$RP2 \leftarrow resize(P2, [1\ h \times w \times c])$;
$Key2 \leftarrow fix(RP2 \times 10^{12} \mod 256)$;
$Key2 \leftarrow reshape(Key2, h, w, c)$;
$EncImg \leftarrow SbImg \oplus Key2$// Cipher image
End of the algorithm
```

(2019); Liansheng et al. (2019); Farah et al. (2020)). However, despite their advantages, directly incorporating these transforms into DRPE may not always be beneficial from a security perspective, making them vulnerable to certain attacks (Qin and Peng (2009)). Therefore, hybrid optical-digital encryption approaches have garnered respect as they provide increased security for optical information systems (Azoug and Bouguezel (2016)). Furthermore, with the rapid progress in quantum technologies, most conventional optical cryptographic systems can be compromised using the power of quantum computers (EL-Latif et al. (2019b)). Consequently, new optical cryptosystems based on quantum mechanics are required. The discrete-time quantum walks (Venegas-Andraca (2012a)) offer chaotic dynamical behavior that serves as an attractive tool for designing quantum/classical cryptographic applications.

In this section, we present a new method for optical image encryption called OIC, which employs alternate quantum walks (AQW). This approach ensures the security of the proposed optical mechanism through quantum mechanics and initial key parameters. The AQW's role is to permute and diffuse the original image and then generate two random masks for the DRPE process. Simulation results confirm that this optical image encryption approach is efficient and highly secure.

The encryption procedures for this method are outlined in Figure 4.3 and detailed in Algorithm 3:

The decryption procedures are like to the encryption procedures but they necessity to be performed in the reverse direction. The decryption procedures of the presented method are outlined in Fig. 4.4, and explained in Algorithm 4.

Algorithm 3: Encryption algorithm

```
Parameters: $N_1, T_1, \alpha_1, \beta_1, N_2, T_2, \alpha_2, \beta_2$ // Used for acting AQWs.
Input: Plain image ($I$)
Output: Cipher image ($E$)
$[m\,n] \leftarrow size(I)$// Get image dimension
$P1 \leftarrow AQWs(N_1, T_1, \alpha_1, \beta_1)$// Operate AQWs on a cycle of $N_1$
    vertices ($N_1$ is odd) for $T_1$ steps to produce a
    probability distribution $P_1$ of dimension $N_1 \times N_1$ where
    the primary state of the walker is $H_c = \cos\alpha_1|0\rangle + \sin\alpha_1|1\rangle$.
    Hence, $\beta_1$ is the key parameter used to design the coin
    operator $\hat{C}$ and $\alpha_1, \beta_1 \in [0, \pi/2]$.
$ReP_1 \leftarrow resize(P_1, [1 m \times n])$// Resize $P_1$ to the size of the
    plain image $I$ $(m \times n)$
$V \leftarrow sort(ReP_1)$// Sort the elements of $ReP_1$ in ascending
    order.
$PerV \leftarrow index(ReP_1, V)$// Obtain the index of every element of
    $ReP_1$ in $V$ as a vector $PerV$.
$ImV \leftarrow reshap(I, m \times n, 1)$// Reshape the original image $I$ to a
    vector.
// Permutate the vector image $ImV$ using the constructed
    vector $PerV$
for $i \leftarrow 1$ to $m \times n$ do
    $PerImV(i) \leftarrow ImV(PerV(i))$;
$PerIm \leftarrow reshap(PerImV, m, n)$;
$P2 \leftarrow AQWs(N_2, T_2, \alpha_2, \beta_2)$// Operate AQWs on a cycle of $N_2$
    vertices
$ReP_2 \leftarrow resize(P_2, [1\, m \times n])$;
$K \leftarrow fix(ReP_2 \times 10^{12}) \mod 256$// Convert $ReP_2$ to integer values
$SIm \leftarrow K \oplus PerIm$// Perform bitwise XOR operation
$R_1 \leftarrow ReP_1 \times 10^{12} \mod 2\pi$// Convert $ReP_1$ into values in
    interval $[0, 2\pi]$.
$RPM_1 \leftarrow \exp[i * R_1]$// Random phase mask.
$R_2 \leftarrow ReP_2 \times 10^{12} \mod 2\pi$;
$RPM_2 \leftarrow \exp[i * R_2]$;
$E \leftarrow IFT\{FT\{SIm \otimes RPM_1\} \otimes RPM_2\}$// Perform DRPE process in
    Fourier transform for constructing the encoded image $E$,
    where FT{.} donates Fourier transform, IFT{.} donates
    invers Fourier transform, and $\otimes$ represents
    element-by-element multiplication.
End of the algorithm
```

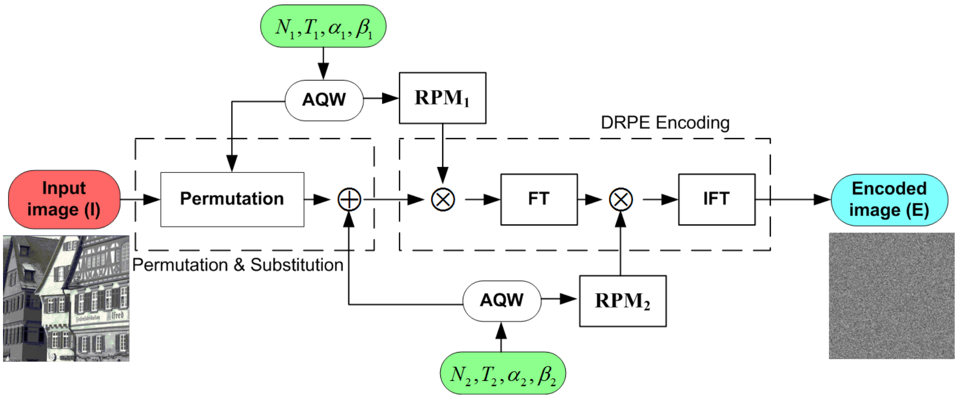

$N_1, T_1, \alpha_1, \beta_1$
AQW
RPM$_1$
DRPE Encoding
Input image (I)
Permutation
FT
IFT
Encoded image (E)
Permutation & Substitution
AQW
RPM$_2$
$N_2, T_2, \alpha_2, \beta_2$

Figure 4.3: Diagram of encryption procedures for the proposed approach, in which AQW is used to permutations and diffuses the original image then generates two random masks for the DRPE process.

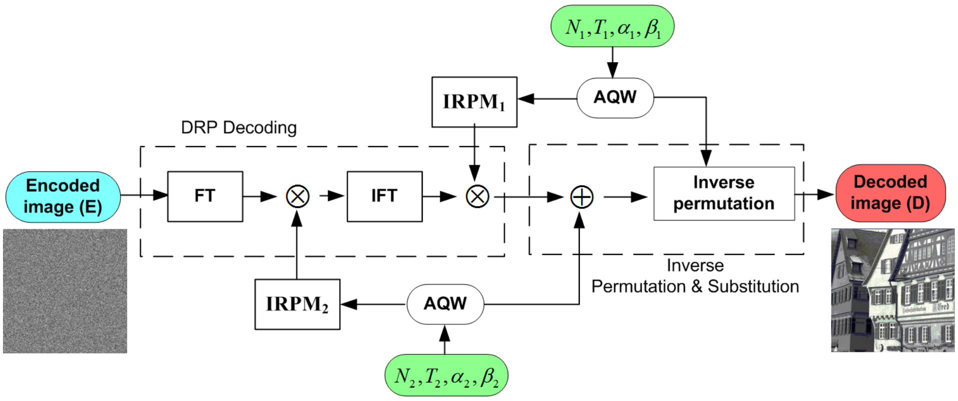

$N_1, T_1, \alpha_1, \beta_1$
IRPM$_1$
AQW
DRP Decoding
Encoded image (E)
FT
IFT
Inverse permutation
Decoded image (D)
Inverse Permutation & Substitution
IRPM$_2$
AQW
$N_2, T_2, \alpha_2, \beta_2$

Figure 4.4: Diagram of decryption procedures for the proposed approach.

4.5 Simple Authenticated Quantum Cryptography Protocols (AQCPs)

Wireless sensor networks, which have become an integral part of modern society, offer versatile communication platforms suitable for numerous applications, including monitoring, logistics, surveillance, smart homes, and healthcare, among many others (Baghezza et al. (2021); Anitha et al. (2021); Al-Saedi et al. (2022)). These applications often require a high level of security (Ahmad et al. (2021); Alturki et al. (2021)). However, with the advent of quantum technologies, many conventional security mechanisms are at risk due to the promising capabilities of quantum computation (Abd-El-Atty (2023, 2022); Abd-El-Atty et al. (2022)). As a result, the security and privacy of wireless sensor networks

Algorithm 4: Decryption algorithm

```
Parameters: $N_1, T_1, \alpha_1, \beta_1, N_2, T_2, \alpha_2, \beta_2$ // Used for acting AQWs.
Input: Cipher image ($E$)
Output: Decrypted image ($D$)
$[m\, n] \leftarrow size(E)$ // Get image dimension
$P1 \leftarrow AQWs(N_1, T_1, \alpha_1, \beta_1)$ // Operate AQWs on a cycle of $N_1$
    vertices ($N_1$ is odd) for $T_1$ steps to produce a
    probability distribution $P_1$ of dimension $N_1 \times N_1$ where
    the primary state of the walker is $H_c = \cos\alpha_1|0\rangle + \sin\alpha_1|1\rangle$.
    Hence, $\beta_1$ is the key parameter used to design the coin
    operator $\hat{C}$ and $\alpha_1, \beta_1 \in [0, \pi/2]$.
$ReP_1 \leftarrow resize(P_1, [1m \times n])$;
$P2 \leftarrow AQWs(N_2, T_2, \alpha_2, \beta_2)$ // Operate AQWs on a cycle of $N_2$
    vertices
$ReP_2 \leftarrow resize(P_2, [1m \times n])$;
$R_1 \leftarrow ReP_1 \times 10^{12} \mod 2\pi$;
$IRPM_1 \leftarrow \exp[-i * R_1]$;
$R_2 \leftarrow ReP_2 \times 10^{12} \mod 2\pi$;
$IRPM_2 \leftarrow \exp[-i * R_2]$;
$DR \leftarrow IFT\{FT\{E\} \otimes IRPM_2\} \otimes IRPM_1$ // Perform DRP decoding
    process in Fourier transform for constructing the decoded
    image DR
$K \leftarrow fix(ReP_2 \times 10^{12}) \mod 256$;
$SIm \leftarrow K \oplus DR$ // Perform bitwise XOR operation
$V \leftarrow sort(ReP_1)$;
$PerV \leftarrow index(ReP_1, V)$;
$SV \leftarrow reshap(SIm, m \times n, 1)$;
// Inverse permutation process
for $i \leftarrow 1$ to $m \times n$ do
    $PerImV(PerV(i)) \leftarrow SV(i)$;
$D \leftarrow reshap(PerImV, m, n)$ // Decrypted image
End of the algorithm
```

necessitate new cryptographic mechanisms based on quantum principles to withstand potential threats from both digital computers and quantum computers.

Quantum information and quantum computation are two rapidly advancing fields of scientific research that are transitioning from the laboratory to practical applications. The compelling results and potential advantages of quantum information and quantum computation have drawn mathematicians, computer scientists, physicists, and engineers into these fields, fostering new trends and innovations in information theory, communication, computation, and cryptography.

Quantum Key Distribution (QKD) is a well-established quantum cryptography technology that generates private keys for use in both symmetric and asymmetric cryptographic protocols. The first QKD protocol, BB84 (Bennett and Brassard (1984)), enabled two parties to establish a random secret key using quantum states prepared in different bases. Today, in addition to QKD, quantum cryptography encompasses various branches of quantum technology, including quantum secret sharing and quantum authentication protocols, among others (Abd-El-Atty et al. (2018)).

In QKD techniques, legitimate participants require full access to quantum resources to distribute a random secret key, including the ability to prepare and measure qubits in different bases and perform unitary operations on qubits. A pertinent question arises: Is it possible to generate private keys with partial access to quantum resources, combining classical and quantum resources? Boyer et al. (2007) (BKM07) introduced the first Semi-Quantum Key Distribution (SQKD) protocol using four quantum states, in which quantum Alice can share a random secret key with classical Bob. Since then, several SQKD protocols have been developed (Boyer et al. (2009); Zou et al. (2009); Zhang et al. (2009); Wang et al. (2011); Krawec (2016); Li et al. (2016b); Zhu et al. (2018)). For example, Boyer et al. (2009) proposed two SQKD protocols similar to BKM07, one based on randomization and the other on measure-resend. Zou et al. (2009) demonstrated that the BKM07 protocol could be implemented with fewer than four quantum states and introduced several SQKD protocols using fewer than four quantum states. Zhang et al. (2009) designed a multi-user SQKD protocol with an m-classical receiver, and Wang et al. (2011) presented an SQKD protocol based on quantum entangled states.

Without authentication, communicating parties are vulnerable to eavesdroppers performing active attacks, such as man-in-the-middle and impersonation attacks, if they do not verify each other's identity. Authentication is crucial for ensuring data integrity and is a vital component of information security. As a result, authentication is a crucial element in various quantum cryptography protocols (Arul et al. (2018)).

Most quantum cryptographic protocols rely on classical channels, which play a vital role in detecting eavesdropping. The effectiveness of these classical channels is closely linked to the existence of authentication protocols. Without this feature, quantum protocols would be vulnerable to active attacks by undetected eavesdroppers (Li et al. (2016b); Yang et al. (2013); Lin et al. (2013a)). To create secure quantum cryptography protocols without authenticated classical channels, various authenticated quantum protocols have been developed (Zeng and Zhang (2000); Lin et al. (2013b); Huang et al. (2016); Xin et al. (2016); Yuan et al. (2014); Guan et al. (2014)). These protocols incorporate authentication with a pre-shared secret key and communication over public classical channels. For example, Zeng and Zhang (2000) designed an authenticated quantum key distribution (AQKD) protocol based on Bell states. Zeng *et al.*'s protocol relies on a trusted information center during the initial phase to help legitimate participants establish the secret key. Lin et al. (2013b) proposed a multi-user Authenticated QKD (AQKD) protocol with a star network topology, utilizing a keyed hash function to confirm participants' identities. In 2014, Yu et al. (2014) developed two Authenticated Semi-Quantum Key Distribution (ASQKD) protocols using Bell states, requiring a pre-shared master key. Meslouhi and Hassouni (2017) identified a man-in-the-middle attack in the protocol presented by Yu et al. (2014). Yuan et al. (2014) introduced a quantum authentication protocol based on the ping-pong method, which can verify the identity of legitimate participants and update the initial authentication key for reuse. Guan et al. (2014) presented a three-party AQKD protocol for sharing a random secret key between two parties with the assistance of a trusted center. However, Luo et al. (2017) pointed out that the protocol proposed by Guan et al. (2014) suffers from information leakage and intercept-measure attacks. In 2016, Huang et al. (2016) introduced two AQKD protocols based on single photons and collective detection. The first protocol is a two-party AQKD, and the other is a multiparty AQKD with a star network topology. In both protocols, legitimate participants pre-share an *m-bit* secret key. Li et al. (2016a) presented two ASQKD protocols that operate without classical channels.

With the rise of quantum computers and quantum algorithms, some traditional cryptographic methods are under threat (Li et al. (2013b)). Simultaneously, several novel proposals involving quantum systems to enhance classical cryptographic protocols have emerged, such as using quantum walks (QW), a universal quantum computational model (Venegas-Andraca (2012b)). Quantum walks can be employed to create hash functions (Li et al. (2013b); Yang et al. (2016b); Li et al. (2018b); Yang et al. (2018a,b); EL-Latif et al. (2019c)) due to their nonlinear chaotic dynamical behavior. Quantum walks offer high sensitivity to initial states, non-periodicity, stability, and the ability to generate extremely large keyspaces capable of withstanding various attacks (Abd-El-Atty et al. (2019a); El-Latif et al. (2020b,e)).

Hash functions have numerous applications in cryptographic tasks, making them a crucial component of modern cryptographic systems (Lindell and Katz (2014)). Classical hash functions are widely used in quantum authentication protocols to ensure the security of established quantum channels (Huang et al. (2016); Xin et al. (2016); Li et al. (2016a)). To enhance the security of quantum cryptographic protocols, three authenticated quantum cryptography protocols have been investigated based on quantum hash functions constructed using quantum walks. The first protocol is AQKD, and the other two are ASQKD.

Any SQKD protocol relies on a two-way quantum communication, where qubits travel from the sender to the receiver and back to the sender, with quantum Alice sending a quantum state to classical Bob (Zhang et al. (2018)). Classical Bob is limited to performing specific operations, including measuring the received particles in the computational basis (Z-basis), preparing fresh qubits in the computational basis, reflecting qubits, and reordering qubits.

To minimize the quantum resources required to establish a random secret key between two parties, Krawec (2015) and Liu and Hwang (2018) introduced a SQKD protocol that leverages a mediated server with quantum capabilities to enable two classical participants to share a random secret key. In all the aforementioned SQKD and ASQKD protocols, users are essentially semi-classical users, as they require some quantum resources for preparing qubits on a computational basis or maintaining quantum memory to reorder qubits (Li et al. (2016b)). In this study, two ASQKD protocols that reduce the quantum resources required to establish a random secret key for sensor node participants are presented. In the first protocol, the receiver node (Bob) has access only to the quantum resources necessary for executing quantum walks and measuring qubits on a computational basis. In the second protocol, both legitimate participant nodes are semi-classical. The sender node (Alice) has access to the quantum resources needed for running quantum walks, preparing and sending qubits in the computational basis $\{|0\rangle,|1\rangle\}$, while the receiver node has access to the quantum resources needed to measure qubits in the computational basis and perform quantum walks. To distinguish between the proposed ASQKD protocols, the first is named ASQKD1 (with one semi-classical user), and the second is ASQKD2 (where both users are semi-classical).

Some key properties of the proposed quantum cryptography protocols are as follows:

1. The pre-shared control parameters are numerical values and can be reused several times.

2. Authenticated members can establish different secret keys using the same set of qubits.

3. The number of bits in the shared secret key may exceed the number of shared qubits multiple times.

4. To reduce the cost of quantum resources in practical implementations, the proposed ASQKD protocols utilize a one-way quantum communication

channel, whereas previously presented ASQKD and SQKD protocols relied on two-way quantum communication.

4.5.1 Quantum Walks Based Quantum Hash Function (QHF)

A coined discrete quantum walk is composed of the following elements: a walker, a coin, evolution operators for both the coin and walker, and a set of observables. The walker is a quantum system $|\psi\rangle_p$ that exists in a Hilbert space $\mathcal{H}_p$ of dimension d where $d = N$ for a quantum walk run on an N-node circle. The coin is typically a quantum system existing in a two-dimensional Hilbert space $|\psi\rangle_c \in \mathcal{H}_c$. In each step t of acting Quantum Walks (QWs), a Unitary operator $\hat{U}$ is applied to the entire quantum state $|\varphi\rangle$.

$$\hat{U} = \hat{S}(\hat{I} \otimes \hat{C}) \tag{4.1}$$

Here, $\hat{C}$ is a Unitary operator applied to the coin state, $\hat{I}$ is the identity operator, and $\hat{S}$ is the Shift operator, which diffuses the quantum particle over the topology on which the quantum walk is performed. If the quantum walk is run on an N-node circle, then the shift operator $\hat{S}$ can be expressed as shown in Eq. (4.2).

$$\begin{aligned} \hat{S} = &\textstyle\sum_{x \notin \{1,N\}} |x+1,0\rangle \langle x,0| + |x-1,1\rangle \langle x,1| \\ &+ \textstyle\sum_{x \in \{1\}} |2,0\rangle \langle 1,0| + |N,1\rangle \langle 1,1| \\ &+ \textstyle\sum_{x \in \{N\}} |1,0\rangle \langle N,0| + |N-1,1\rangle \langle N,1| \end{aligned} \tag{4.2}$$

The coin operator $\hat{C}$ can be written in matrix for as in Eq.(4.3).

$$\begin{pmatrix} \cos\,\theta & \sin\,\theta \\ \sin\,\theta & -\cos\,\theta \end{pmatrix}, where\ \theta \in [0, \pi] \tag{4.3}$$

The final state $|\varphi\rangle_{final}$ of the quantum state after t steps is provided by Eq.(4.4).

$$|\varphi\rangle_{final} = \left(\hat{U}\right)^t |\varphi\rangle_0 \tag{4.4}$$

The probability $P(x,t)$ of locating the walker at location x after t steps can be represented as in Eq.(4.5).

$$P(x,t) = \sum_{i=0}^{1} \left| \langle x,i| \left(\hat{U}\right)^t |\psi\rangle_0 \right|^2 \tag{4.5}$$

In 2013, Li et al. (2013b) proposed the first Quantum Hash Function (QHF) based on 1-D two-walker Quantum Walks (QWs) on a circle controlled by a bit string. After that, numerous QHFs based on QWs have been constructed (Yang et al. (2016b, 2018a,b)). Furthermore, it's important to note that the probability $P(x,t)$ is nonzero at any location x if the number of steps t is greater than or equal to the number of vertices N (EL-Latif et al. (2019c, 2020b)). All constructed QHFs based on QWs (EL-Latif et al. (2019c)) overcome this issue. To address this concern, an improved QHF (Yang et al. (2018b)) is achieved by introducing an additional coin operator.

Yang et al. (2018b) built a QHF for a binary *m-bit* based on one-walker QWs on a circle with N nodes. Unitary operators $\hat{U}_0$ and $\hat{U}_1$ are applied when the t^{th} bit of m is *"0"* and *"1"*, respectively. In the modified QHF, three coins $\hat{C}_0$, $\hat{C}_1$ and $\hat{C}_2$ are used to construct the three evolution operators $\hat{U}_0$, $\hat{U}_1$ and $\hat{U}_2$, respectively. Where the evolution operator $\hat{U}_0$ ($\hat{U}_1$) is performed when the t^{th} bit of m is *"0"* (*"1"*), and the evolution operator $\hat{U}_2$ is applied when the t^{th} step exceeds to the size of m and does not reach N. As an example, if m is *"101"* and $N = 25$, the final state can be given as in Eq.(4.6).

$$|\varphi\rangle_{final} = \left(\prod_{t=4}^{25} \hat{U}_2^t\right) \hat{U}_1\hat{U}_0\hat{U}_1|\varphi\rangle_0 \tag{4.6}$$

According to QHF presented in (Yang et al. (2018b)), the final state can be written as in Eq.(4.7).

$$|\varphi\rangle_{final} = \hat{U}_1\hat{U}_0\hat{U}_1|\varphi\rangle_0 \tag{4.7}$$

where the probability P is equal to zero in some locations. For a better illustration, the hash values constructed by the two Quantum Hash Functions (QHFs), the modified QHF and Yang et al. (2018b)'s QHF, using the same parameters for the message m = "101" and $N = 25$, are provided in Fig. 4.5 in binary format and hexadecimal format as follows:

- Modified QHF: *9581 D3E3 0E6A 2956 2FB6 E3F7 5298 7609 8C31 A6E3 3B8F B2F4 53*
- Yang et al. (2018b)'s QHF: *0000 0000 0000 0000 003F 003F 003F 003F 0000 0000 0000 0000 00*

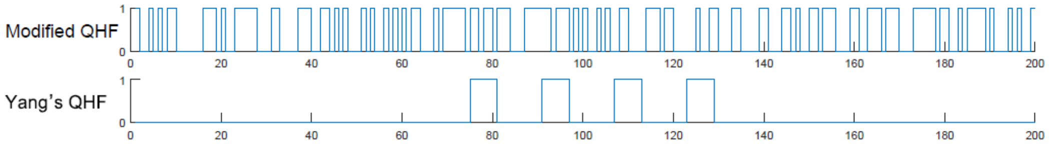


Figure 4.5: Plots of 200-bit hash value constructed by the two QHFs (modified QHF and Yang et al. (2018b)'s QHF) using the same parameters for message *"101"* and N is *25*.

The modified QHF is outlined in the following steps.

1. Select initial parameters $(N, m, \omega, \theta_0, \theta_1, \theta_2)$ for operating one-particle QWs on a circle of N vertices governed by m-*bit* to generate a probability distribution P of size N. Here θ_0, θ_1 and θ_2 are parameters for the coin operators $\hat{C}_0$, $\hat{C}_1$ and $\hat{C}_2$, respectively. The coin initial state is prepared as $|\psi\rangle_c = \cos(\omega)|0\rangle + \sin(\omega)|1\rangle$.

2. Construct the hash value for m string by transforming P to a binary values as in Eq.(4.8):

$$hash = dec2bin(fix(P_i \times 10^{12})\, mod\ 2^8, 8) \tag{4.8}$$

where *8*×N is the length of binary hash value.

4.5.2 The proposed quantum authentication protocols

This section presents three variants of quantum authentication protocols designed to establish random secret keys based on quantum walks. The first protocol is AQKD, and the others are ASQKD. The proposed protocols require pre-shared master key parameters $(\omega, \theta_0, \theta_1, \theta_2)$ for operating one-particle Quantum Walks (QWs) on a circle with an odd number of nodes, denoted as N

(for instance, this can be prepared in advance within a closed environment). Furthermore, the quantum communication environment is based on single photons, and the quantum channel is assumed to be lossless and noiseless.

4.5.2.1 The AQKD protocol

The procedure of AQKD protocol is illustrated in Fig. 4.6 and the detailed steps are given in Algorithm 5.

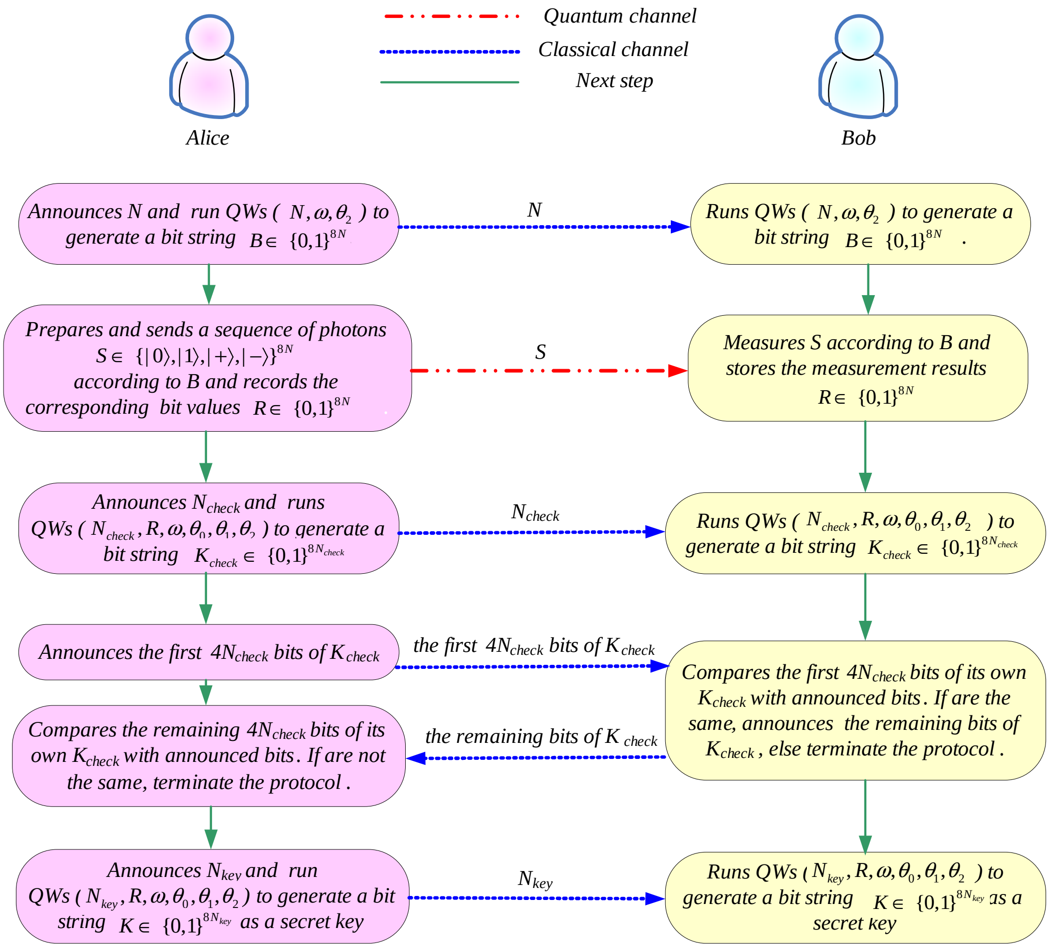

Quantum channel
Classical channel
Next step
Alice
Bob
Announces N and run QWs (N,ω,θ_2) to generate a bit string $B\in\{0,1\}^{8N}$
N
Runs QWs (N,ω,θ_2) to generate a bit string $B\in\{0,1\}^{8N}$.
Prepares and sends a sequence of photons $S\in\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}^{8N}$ according to B and records the corresponding bit values $R\in\{0,1\}^{8N}$
S
Measures S according to B and stores the measurement results $R\in\{0,1\}^{8N}$
Announces N_{check} and runs QWs ($N_{check},R,\omega,\theta_0,\theta_1,\theta_2$) to generate a bit string $K_{check}\in\{0,1\}^{8N_{check}}$
N_{check}
Runs QWs ($N_{check},R,\omega,\theta_0,\theta_1,\theta_2$) to generate a bit string $K_{check}\in\{0,1\}^{8N_{check}}$
Announces the first $4N_{check}$ bits of K_{check}
the first $4N_{check}$ bits of K_{check}
Compares the first $4N_{check}$ bits of its own K_{check} with announced bits. If are the same, announces the remaining bits of K_{check}, else terminate the protocol.
the remaining bits of K_{check}
Compares the remaining $4N_{check}$ bits of its own K_{check} with announced bits. If are not the same, terminate the protocol.
Announces N_{key} and run QWs ($N_{key},R,\omega,\theta_0,\theta_1,\theta_2$) to generate a bit string $K\in\{0,1\}^{8N_{key}}$ as a secret key
N_{key}
Runs QWs ($N_{key},R,\omega,\theta_0,\theta_1,\theta_2$) to generate a bit string $K\in\{0,1\}^{8N_{key}}$ as a secret key

Figure 4.6: The proposed AQKD protocol, which both the legitimate users have fully quantum capabilities and the size of the exchanged final key is dependent on the stated N_{key} only and not on the number of shared qubits

From the data sent through the classical channel containing the hash value, it is impossible for anyone to obtain any information regarding the master key $(\omega,\theta_0,\theta_1,\theta_2)$ or the final secret key K. Consequently, the master key can be reused several times later. For a clearer illustration, refer to the example

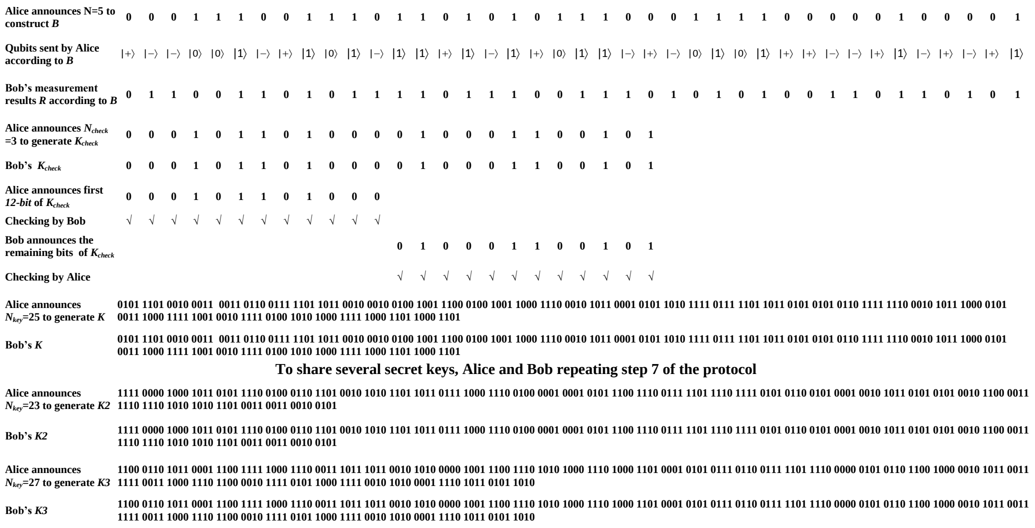
Algorithm 5: Procedure of AQKD protocol

```
1 The sender (Alice) informs the receiver (Bob) publicly an odd number $N$,
  for performing QHF $(N, \omega, \theta_2)$ to produce a hash value $B \in \{0,1\}^{8N}$ of
  length $8 \times N$. ;
2 Alice prepares a stream of single photons $S \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}^{8N}$
  according to $B$ sequence as follows and records its corresponding classical
  values $R \in \{0,1\}^{8N}$. $B$ decides the encoding bases. If the $i^{th}$ bit of $B$ is "1"
  then Alice randomly prepares the qubit $S_i$ in computational basis
  (Z-basis) as $|0\rangle$ or $|1\rangle$. Moreover, if the $i^{th}$ bit of $B$ is "0" then Alice
  randomly prepares the qubit $S_i$ in Hadamard basis (X-basis) as $|+\rangle$ or
  $|-\rangle$. ;
3 Alice transmits the photon stream $S$ to Bob through an ideal quantum
  channel. ;
4 As Bob receives the photon sequence $S$, he measures the qubits with
  correct bases according to the bit string $B$. If the $i^{th}$ bit of $B$ is "1" then
  Bob measures the qubit $S_i$ in the computational basis. Furthermore, if
  the $i^{th}$ bit of $B$ is "0" then Bob measures qubit $S_i$ in Hadamard basis.
  Thereby, Bob obtains the measurement results $R \in \{0,1\}^{8N}$. ;
5 Alice publicly agrees with Bob an odd number $N_{check}$, to perform QHF
  $(N_{check}, R, \omega, \theta_0, \theta_1, \theta_2)$ for creating a bit string $K_{check} \in \{0,1\}^{8N_{check}}$ with
  length $8 \times N_{check}$. ;
6 For detecting an eavesdropper, Alice informs Bob the first $4 \times N_{check}$-bit of
  $K_{check}$ sequence. If the comparing outcomes are identical, then Bob
  declares the remaining bits of $K_{check}$ to be reviewed by Alice. Thereby,
  both partners authenticate each other. If there is any mistake, both
  members end the protocol. ;
7 Eventually, Alice informs Bob an odd number $N_{key}$, to operates QWs
  $(N_{key}, R, \omega, \theta_0, \theta_1, \theta_2)$ for constructing the hash value $K \in \{0,1\}^{8N_{key}}$ as a
  secret key of length $8 \times N_{key}$ bits. ;
8 End of the algorithm
```

provided in Fig. 4.7, where both authorized partners can establish various secret keys using the same transmitted qubits by repeating step 7 multiple times, each time generating another N_{key}.

4.5.2.2 The ASQKD1 protocol

In any SQKD protocol, Alice with fully quantum capabilities communicates with the classical receiver (Bob) to establish a random secret key via a two-way quantum communication channel. The main contribution of presenting this class of protocols is to reduce the quantum capabilities to make quantum communications more realizable and practical. Therefore, the proposed ASQKD1



Alice announces N=5 to construct *B*	0 0 0 1 1 1 0 0 1 1 1 0 1 1 0 1 0 1 0 1 1 1 0 0 0 1 1 1 1 0 0 0 0 0 1 0 0 0 0 1
Qubits sent by Alice according to *B*	$\|+\rangle$ $\|-\rangle$ $\|-\rangle$ $\|0\rangle$ $\|0\rangle$ $\|1\rangle$ $\|-\rangle$ $\|+\rangle$ $\|1\rangle$ $\|0\rangle$ $\|1\rangle$ $\|-\rangle$ $\|1\rangle$ $\|1\rangle$ $\|+\rangle$ $\|1\rangle$ $\|-\rangle$ $\|1\rangle$ $\|+\rangle$ $\|0\rangle$ $\|1\rangle$ $\|1\rangle$ $\|-\rangle$ $\|+\rangle$ $\|-\rangle$ $\|0\rangle$ $\|1\rangle$ $\|0\rangle$ $\|1\rangle$ $\|+\rangle$ $\|+\rangle$ $\|-\rangle$ $\|-\rangle$ $\|+\rangle$ $\|1\rangle$ $\|-\rangle$ $\|+\rangle$ $\|-\rangle$ $\|+\rangle$ $\|1\rangle$
Bob's measurement results *R* according to *B*	0 1 1 0 0 1 1 0 1 0 1 1 1 1 0 1 1 1 0 0 1 1 1 0 1 0 1 0 1 0 0 1 1 0 1 1 0 1 0 1
Alice announces N_{check} =3 to generate K_{check}	0 0 0 1 0 1 1 0 1 0 0 0 0 1 0 0 0 1 1 0 0 1 0 1
Bob's K_{check}	0 0 0 1 0 1 1 0 1 0 0 0 0 1 0 0 0 1 1 0 0 1 0 1
Alice announces first *12-bit* of K_{check}	0 0 0 1 0 1 1 0 1 0 0 0
Checking by Bob	√ √ √ √ √ √ √ √ √ √ √ √
Bob announces the remaining bits of K_{check}	0 1 0 0 0 1 1 0 0 1 0 1
Checking by Alice	√ √ √ √ √ √ √ √ √ √ √ √
Alice announces N_{key}=25 to generate *K*	0101 1101 0010 0011 0011 0110 0111 1101 1011 0010 0010 0100 1001 1100 0100 1001 1000 1110 0010 1011 0001 0101 1010 1111 0111 1101 1011 0101 0101 0110 1111 1110 0010 1011 1000 0101 0011 1000 1111 1001 0010 1111 0100 1010 1000 1111 1000 1101 1000 1101
Bob's *K*	0101 1101 0010 0011 0011 0110 0111 1101 1011 0010 0010 0100 1001 1100 0100 1001 1000 1110 0010 1011 0001 0101 1010 1111 0111 1101 1011 0101 0101 0110 1111 1110 0010 1011 1000 0101 0011 1000 1111 1001 0010 1111 0100 1010 1000 1111 1000 1101 1000 1101
	To share several secret keys, Alice and Bob repeating step 7 of the protocol
Alice announces N_{key}=23 to generate *K2*	1111 0000 1000 1011 0101 1110 0100 0110 1101 0010 1010 1101 1011 0111 1000 1110 0100 0001 0001 0101 1100 1110 0111 1101 1110 1111 0101 0110 0101 0001 0010 1011 0101 0101 0010 1100 0011 1110 1110 1010 1010 1101 0011 0011 0010 0101
Bob's *K2*	1111 0000 1000 1011 0101 1110 0100 0110 1101 0010 1010 1101 1011 0111 1000 1110 0100 0001 0001 0101 1100 1110 0111 1101 1110 1111 0101 0110 0101 0001 0010 1011 0101 0101 0010 1100 0011 1110 1110 1010 1010 1101 0011 0011 0010 0101
Alice announces N_{key}=27 to generate *K3*	1100 0110 1011 0001 1100 1111 1000 1110 0011 1011 1011 0010 1010 0000 1001 1100 1110 1010 1000 1110 1000 1101 0001 0101 0111 0110 0111 1101 1110 0000 0101 0110 1100 1000 0010 1011 0011 1111 0011 1000 1110 1100 0010 1111 0101 1000 1111 0010 1010 0001 1110 1011 0101 1010
Bob's *K3*	1100 0110 1011 0001 1100 1111 1000 1110 0011 1011 1011 0010 1010 0000 1001 1100 1110 1010 1000 1110 1000 1101 0001 0101 0111 0110 0111 1101 1110 0000 0101 0110 1100 1000 0010 1011 0011 1111 0011 1000 1110 1100 0010 1111 0101 1000 1111 0010 1010 0001 1110 1011 0101 1010

Figure 4.7: An illustrated paradigm for the presented AQKD protocol, in the case of the pre-established master key is $\omega = 0, \theta_0 = 60, \theta_1 = 45$, and $\theta_2 = 36$

protocol relies on one-way quantum communication, and Bob has limited quantum capabilities to execute the following operations: (1) receive and measure qubits with the computational basis, and (2) run one-walker quantum walks on a circle. The procedures of the ASQKD1 protocol are given in Fig. 4.8 and described in Algorithm 6. Fig. 4.9 illustrates the presented ASQKD1 protocol.

Algorithm 6: Procedure of ASQKD1 protocol

```
1 Perform step 1 as in the presented AQKD protocol (Algorithm 5). ;
2 Alice prepares a stream of single photons $S \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}^{8N}$
  according to $B$ sequence as follows: Let $B$ decides the encoding bases. If
  the $i^{th}$ bit of $B$ is "1", then Alice randomly prepares the qubit $S_i$ in
  computational basis as $|0\rangle$ or $|1\rangle$, and records the corresponding classical
  bit value of $i^{th}$ qubit as $R \in \{0,1\}^x$. Otherwise, Alice randomly prepares
  the qubit $S_i$ with diagonal basis as $|+\rangle$ or $|-\rangle$. ;
3 Perform step 3 as in the presented AQKD protocol (Algorithm 5). ;
4 As Bob receives a photon stream $S$, he performs quantum measurements
  in computational basis on each incoming qubit and stores the
  corresponding measurement results of $i^{th}$ qubit when $i^{th}$ bit of $B$ is "1" to
  get the classical bit string $R \in \{0,1\}^x$.;
5 Performing steps 5, 6, and 7 in the proposed AQKD protocol (Algorithm
  5). ;
6 End of the algorithm
```

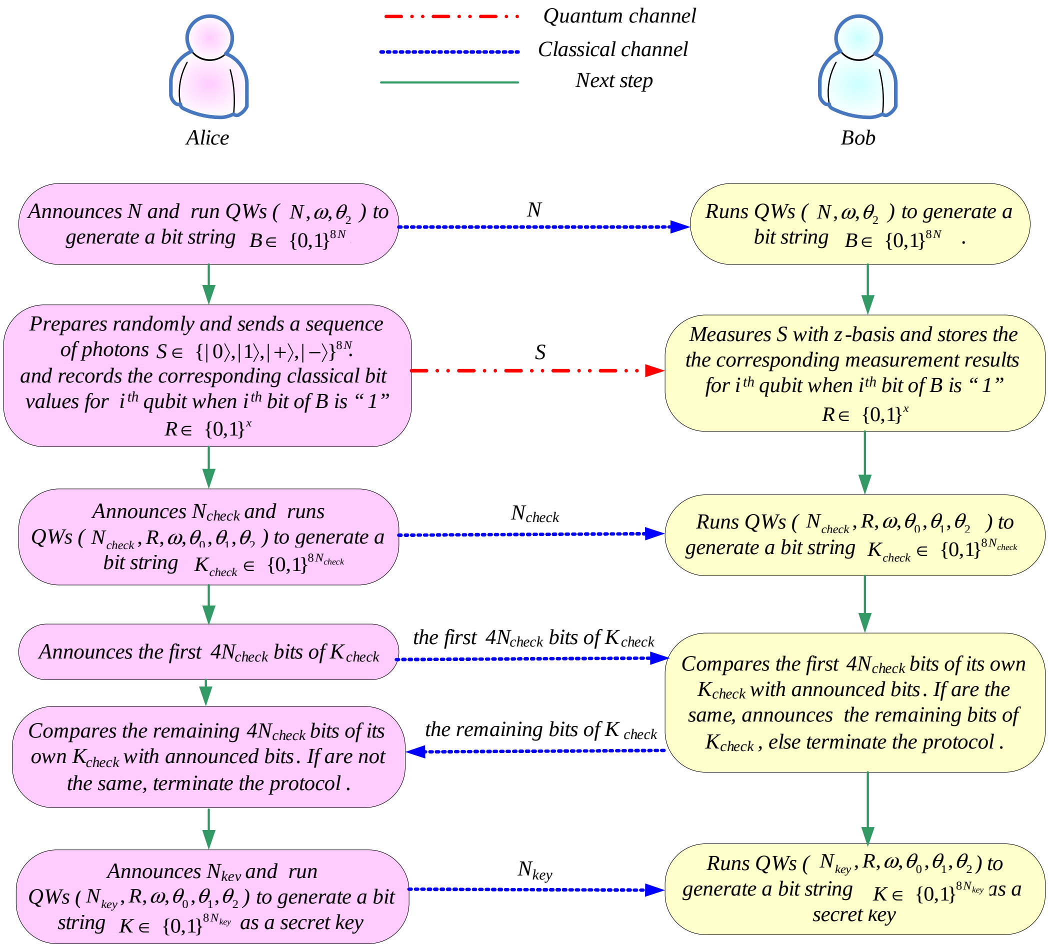
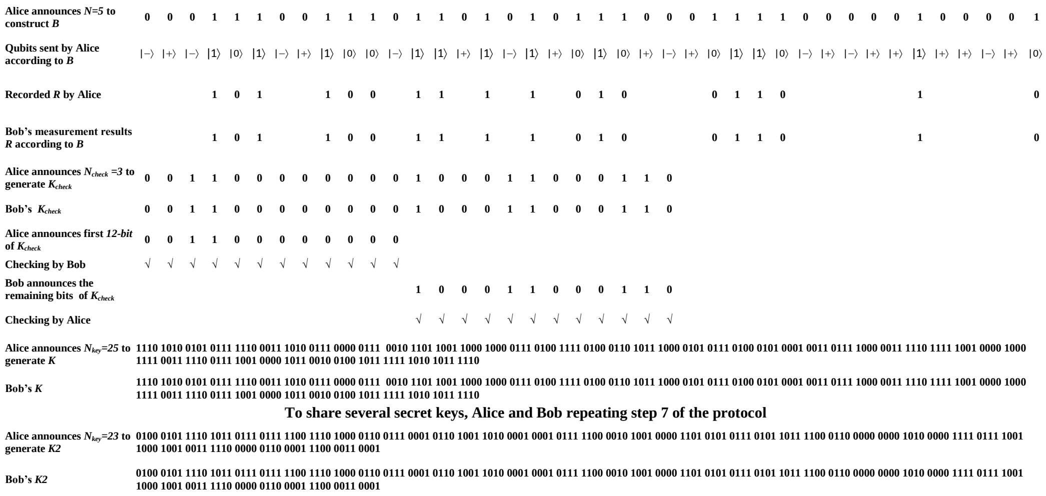

Quantum channel
Classical channel
Next step
Alice
Bob
Announces N and run QWs (N,ω,θ_2) to generate a bit string $B\in\{0,1\}^{8N}$
N
Runs QWs (N,ω,θ_2) to generate a bit string $B\in\{0,1\}^{8N}$.
Prepares randomly and sends a sequence of photons $S\in\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}^{8N}$. and records the corresponding classical bit values for i^{th} qubit when i^{th} bit of B is "1" $R\in\{0,1\}^x$
S
Measures S with z-basis and stores the the corresponding measurement results for i^{th} qubit when i^{th} bit of B is "1" $R\in\{0,1\}^x$
Announces N_{check} and runs QWs ($N_{check},R,\omega,\theta_0,\theta_1,\theta_2$) to generate a bit string $K_{check}\in\{0,1\}^{8N_{check}}$
N_{check}
Runs QWs ($N_{check},R,\omega,\theta_0,\theta_1,\theta_2$) to generate a bit string $K_{check}\in\{0,1\}^{8N_{check}}$
Announces the first $4N_{check}$ bits of K_{check}
the first $4N_{check}$ bits of K_{check}
Compares the first $4N_{check}$ bits of its own K_{check} with announced bits. If are the same, announces the remaining bits of K_{check}, else terminate the protocol.
the remaining bits of K_{check}
Compares the remaining $4N_{check}$ bits of its own K_{check} with announced bits. If are not the same, terminate the protocol.
Announces N_{key} and run QWs ($N_{key},R,\omega,\theta_0,\theta_1,\theta_2$) to generate a bit string $K\in\{0,1\}^{8N_{key}}$ as a secret key
N_{key}
Runs QWs ($N_{key},R,\omega,\theta_0,\theta_1,\theta_2$) to generate a bit string $K\in\{0,1\}^{8N_{key}}$ as a secret key

Figure 4.8: The proposed ASQKD1 protocol, in which Alice has full quantum capabilities and Bob is limited to measures qubits with computational basis, besides running quantum walks

4.5.2.3 The ASQKD2 Protocol

The main contribution of SQKD protocols is to establish a random secret key between two legitimate users while consuming fewer quantum resources: one of the participants has full quantum capabilities, and the other has limited quantum resources to carry out the following procedures: (1) receive and resend quantum states via a quantum channel, (2) perform measurements using the computational basis, (3) prepare quantum states in the computational basis, (4) reflect quantum states, and (5) reorder quantum states (which requires quantum memory) (Li et al. (2016b)).

In the presented ASQKD2 protocol, both legitimate participants have access to both classical and quantum resources: Alice has access only to those quantum



Alice announces *N=5* to construct *B*	0	0	0	1	1	1	0	0	1	1	1	0	1	1	0	1	0	1	0	1	1	1	0	0	0	1	1	1	1	0	0	0	0	0	1	0	0	0	0	1
Qubits sent by Alice according to *B*	$\lvert -\rangle$	$\lvert +\rangle$	$\lvert -\rangle$	$\lvert 1\rangle$	$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert -\rangle$	$\lvert +\rangle$	$\lvert 1\rangle$	$\lvert 0\rangle$	$\lvert 0\rangle$	$\lvert -\rangle$	$\lvert 1\rangle$	$\lvert 1\rangle$	$\lvert +\rangle$	$\lvert 1\rangle$	$\lvert -\rangle$	$\lvert 1\rangle$	$\lvert +\rangle$	$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert 0\rangle$	$\lvert +\rangle$	$\lvert -\rangle$	$\lvert +\rangle$	$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert 1\rangle$	$\lvert 0\rangle$	$\lvert -\rangle$	$\lvert +\rangle$	$\lvert -\rangle$	$\lvert +\rangle$	$\lvert +\rangle$	$\lvert 1\rangle$	$\lvert +\rangle$	$\lvert +\rangle$	$\lvert -\rangle$	$\lvert +\rangle$	$\lvert 0\rangle$
Recorded *R* by Alice				1	0	1			1	0	0		1	1		1		1		0	1	0				0	1	1	0						1					0
Bob's measurement results *R* according to *B*				1	0	1			1	0	0		1	1		1		1		0	1	0				0	1	1	0						1					0
Alice announces N_{check} =3 to generate K_{check}	0	0	1	1	0	0	0	0	0	0	0	0	1	0	0	0	1	1	0	0	0	1	1	0																
Bob's K_{check}	0	0	1	1	0	0	0	0	0	0	0	0	1	0	0	0	1	1	0	0	0	1	1	0																
Alice announces first *12-bit* of K_{check}	0	0	1	1	0	0	0	0	0	0	0	0																												
Checking by Bob	√	√	√	√	√	√	√	√	√	√	√	√																												
Bob announces the remaining bits of K_{check}													1	0	0	0	1	1	0	0	0	1	1	0																
Checking by Alice													√	√	√	√	√	√	√	√	√	√	√	√																
Alice announces N_{key}=25 to generate *K*	1110 1010 0101 0111 1110 0011 1010 0111 0000 0111 0010 1101 1001 1000 1000 0111 0100 1111 0100 0110 1011 1000 0101 0111 0100 0101 0001 0011 0111 1000 0011 1110 1111 1001 0000 1000 1111 0011 1110 0111 1001 0000 1011 0010 0100 1011 1111 1010 1011 1110																																							
Bob's *K*	1110 1010 0101 0111 1110 0011 1010 0111 0000 0111 0010 1101 1001 1000 1000 0111 0100 1111 0100 0110 1011 1000 0101 0111 0100 0101 0001 0011 0111 1000 0011 1110 1111 1001 0000 1000 1111 0011 1110 0111 1001 0000 1011 0010 0100 1011 1111 1010 1011 1110																																							
	To share several secret keys, Alice and Bob repeating step 7 of the protocol																																							
Alice announces N_{key}=23 to generate *K2*	0100 0101 1110 1011 0111 0111 1100 1110 1000 0110 0111 0001 0110 1001 1010 0001 0001 0111 1100 0010 1001 0000 1101 0101 0111 0101 1011 1100 0110 0000 0000 1010 0000 1111 0111 1001 1000 1001 0011 1110 0000 0110 0001 1100 0011 0001																																							
Bob's *K2*	0100 0101 1110 1011 0111 0111 1100 1110 1000 0110 0111 0001 0110 1001 1010 0001 0001 0111 1100 0010 1001 0000 1101 0101 0111 0101 1011 1100 0110 0000 0000 1010 0000 1111 0111 1001 1000 1001 0011 1110 0000 0110 0001 1100 0011 0001																																							

Figure 4.9: An illustrated paradigm for the presented ASQKD1 protocol, in the case of the pre-established master key is $\omega = 0, \theta_0 = 60, \theta_1 = 45$, and $\theta_2 = 36$

resources required to send and prepare qubits in the computational basis and running quantum walks, while Bob has access to those quantum resources needed to receive and measure qubits with the computational basis, as well as for running quantum walks. The presented ASQKD2 protocol relies on one-way quantum communication, not relying on two-way quantum communication as stated in the previously presented SQKD protocols.

The procedure of the ASQKD2 protocol is illustrated in Fig. 4.10 and presented in Algorithm 7.

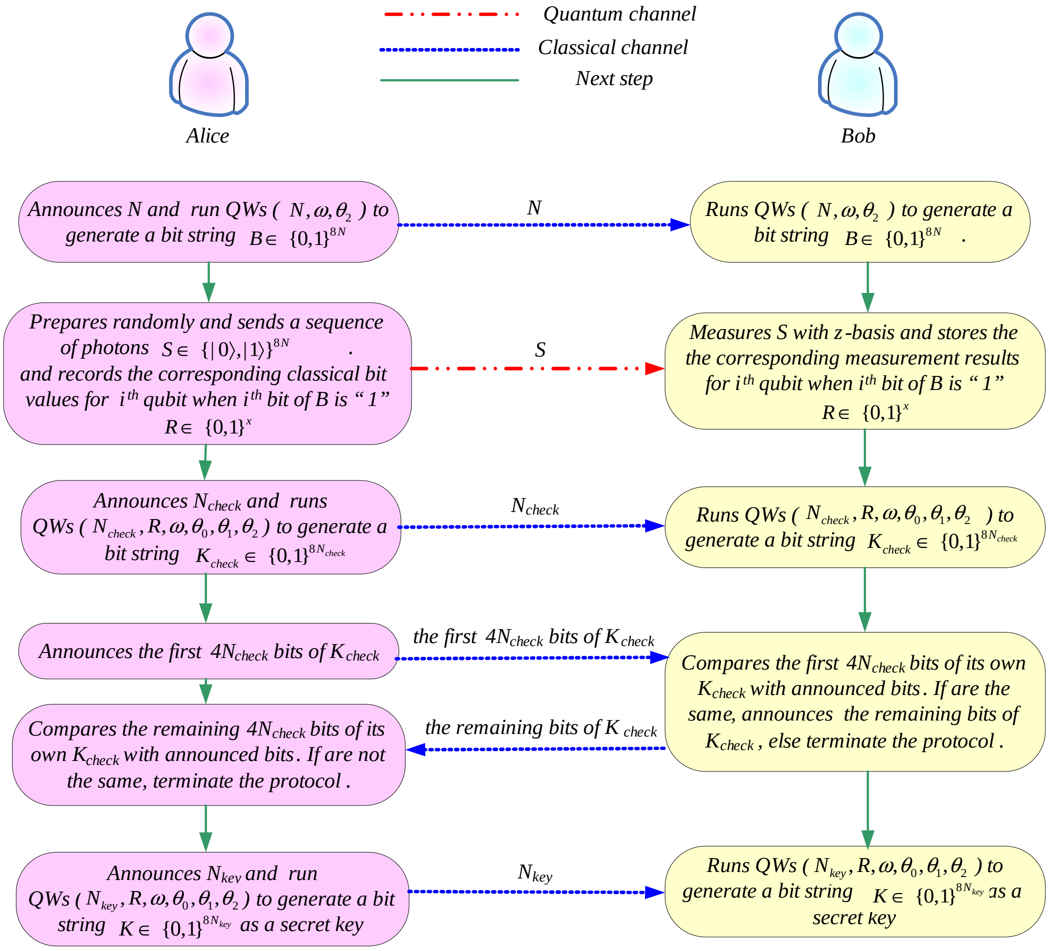
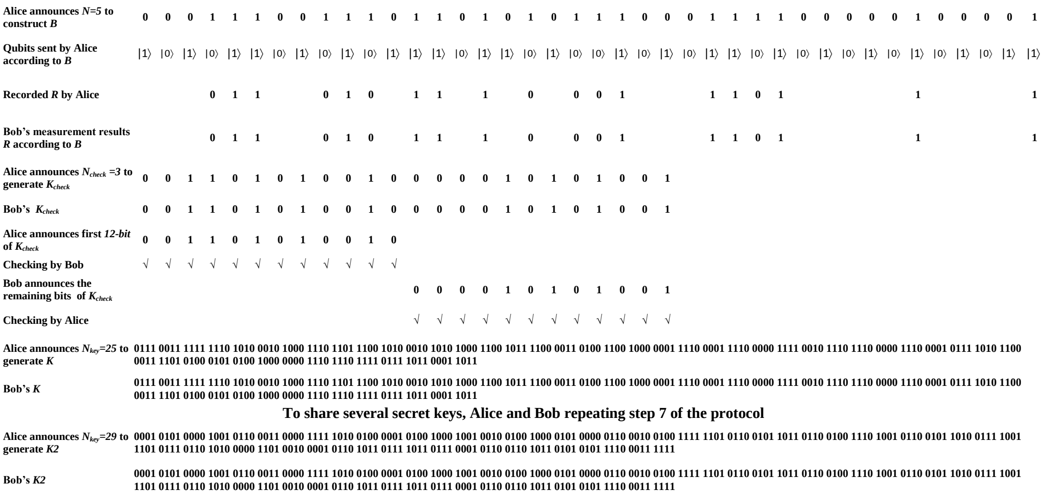

Quantum channel
Classical channel
Next step
Alice
Bob
Announces N and run QWs (N,ω,θ_2) to generate a bit string $B\in\{0,1\}^{8N}$
N
Runs QWs (N,ω,θ_2) to generate a bit string $B\in\{0,1\}^{8N}$.
Prepares randomly and sends a sequence of photons $S\in\{|0\rangle,|1\rangle\}^{8N}$. and records the corresponding classical bit values for i^{th} qubit when i^{th} bit of B is " 1" $R\in\{0,1\}^{x}$
S
Measures S with z-basis and stores the the corresponding measurement results for i^{th} qubit when i^{th} bit of B is " 1" $R\in\{0,1\}^{x}$
Announces N_{check} and runs QWs ($N_{check},R,\omega,\theta_0,\theta_1,\theta_2$) to generate a bit string $K_{check}\in\{0,1\}^{8N_{check}}$
N_{check}
Runs QWs ($N_{check},R,\omega,\theta_0,\theta_1,\theta_2$) to generate a bit string $K_{check}\in\{0,1\}^{8N_{check}}$
Announces the first $4N_{check}$ bits of K_{check}
the first $4N_{check}$ bits of K_{check}
Compares the first $4N_{check}$ bits of its own K_{check} with announced bits. If are the same, announces the remaining bits of K_{check}, else terminate the protocol.
Compares the remaining $4N_{check}$ bits of its own K_{check} with announced bits. If are not the same, terminate the protocol.
the remaining bits of K_{check}
Announces N_{key} and run QWs ($N_{key},R,\omega,\theta_0,\theta_1,\theta_2$) to generate a bit string $K\in\{0,1\}^{8N_{key}}$ as a secret key
N_{key}
Runs QWs ($N_{key},R,\omega,\theta_0,\theta_1,\theta_2$) to generate a bit string $K\in\{0,1\}^{8N_{key}}$ as a secret key

Figure 4.10: The proposed ASQKD2 protocol, which Alice limited to prepare qubits in computational basis and running quantum walks, while Bob limited to measure the received qubits with computational basis besides running quantum walks



Alice announces *N=5* to construct *B*	0	0	0	1	1	1	0	0	1	1	1	0	1	1	0	1	0	1	0	1	1	1	0	0	0	1	1	1	1	0	0	0	0	0	1	0	0	0	0	1
Qubits sent by Alice according to *B*	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
Recorded *R* by Alice				0	1	1			0	1	0		1	1		1		0		0	0	1				1	1	0	1						1					1
Bob's measurement results *R* according to *B*				0	1	1			0	1	0		1	1		1		0		0	0	1				1	1	0	1						1					1
Alice announces N_{check} *=3* to generate K_{check}	0	0	1	1	0	1	0	1	0	0	1	0	0	0	0	0	1	0	1	0	1	0	0	1																
Bob's K_{check}	0	0	1	1	0	1	0	1	0	0	1	0	0	0	0	0	1	0	1	0	1	0	0	1																
Alice announces first *12-bit* of K_{check}	0	0	1	1	0	1	0	1	0	0	1	0																												
Checking by Bob	√	√	√	√	√	√	√	√	√	√	√	√																												
Bob announces the remaining bits of K_{check}													0	0	0	0	1	0	1	0	1	0	0	1																
Checking by Alice													√	√	√	√	√	√	√	√	√	√	√	√																

Alice announces N_{key}*=25* to generate *K*	**0111 0011 1111 1110 1010 0010 1000 1110 1101 1100 1010 0010 1010 1000 1100 1011 1100 0011 0100 1100 1000 0001 1110 0001 1110 0000 1111 0010 1110 1110 0000 1110 0001 0111 1010 1100 0011 1101 0100 0101 0100 1000 0000 1110 1110 1111 0111 1011 0001 1011**
Bob's *K*	**0111 0011 1111 1110 1010 0010 1000 1110 1101 1100 1010 0010 1010 1000 1100 1011 1100 0011 0100 1100 1000 0001 1110 0001 1110 0000 1111 0010 1110 1110 0000 1110 0001 0111 1010 1100 0011 1101 0100 0101 0100 1000 0000 1110 1110 1111 0111 1011 0001 1011**

To share several secret keys, Alice and Bob repeating step 7 of the protocol

Alice announces N_{key}*=29* to generate *K2*	**0001 0101 0000 1001 0110 0011 0000 1111 1010 0100 0001 0100 1000 1001 0010 0100 1000 0101 0000 0110 0010 0100 1111 1101 0110 0101 1011 0110 0100 1110 1001 0110 0101 1010 0111 1001 1101 0111 0110 1010 0000 1101 0010 0001 0110 1011 0111 1011 0111 0001 0110 0110 1011 0101 0101 1110 0011 1111**
Bob's *K2*	**0001 0101 0000 1001 0110 0011 0000 1111 1010 0100 0001 0100 1000 1001 0010 0100 1000 0101 0000 0110 0010 0100 1111 1101 0110 0101 1011 0110 0100 1110 1001 0110 0101 1010 0111 1001 1101 0111 0110 1010 0000 1101 0010 0001 0110 1011 0111 1011 0111 0001 0110 0110 1011 0101 0101 1110 0011 1111**

Figure 4.11: An illustrated paradigm for the presented ASQKD2 protocol, in the case of the pre-established master key is $\omega = 0, \theta_0 = 60, \theta_1 = 45$, and $\theta_2 = 36$

Algorithm 7: Procedure of ASQKD2 protocol

```
1 Perform step 1 as in the presented AQKD protocol (Algorithm 5). ;
2 Alice produces a random sequence of single photons $S \in \{|0\rangle, |1\rangle\}^{8N}$ using
  the computational basis and records the corresponding classical values of
  $i^{th}$ qubit when $i^{th}$ bit of $B$ is "1". ;
3 Performing step 3 in the proposed AQKD protocol (Algorithm 5). ;
4 As Bob receives a photon stream $S$, he measures all received qubits using
  the computational basis and stores the measurement results of $i^{th}$ qubit
  when $i^{th}$ bit of $B$ is "1", to get the classical bit string $R \in \{0,1\}^x$. ;
5 Perform steps 5, 6, and 7 in the proposed AQKD protocol (Algorithm 5). ;
6 End of the algorithm
```

The main contribution of proposing ASQKD2 is to share a random secret key between two semi-quantum participants without using a mediated quantum server, to reduce the amount of consumed quantum resources and to make quantum communications more realizable and practical. For more illustration, see the example presented in Fig. 4.11.

Conclusion

In this chapter, novel cryptosystems based on quantum walks/chaotic systems are presented.

At first, a new cipher image mechanism based on chaotic systems for secure data transfer in cloud-based smart cities is proposed. The proposed encryption system is applicable to both color and grayscale images. The system is based on cascading two integrated 1D chaotic maps: Logistic-Chebyshev and Logistic-Sine. Logistic-Sine map is used to permute the plain image, and Logistic-Chebyshev map is used to substitute the permuted image, while the cascading of both integrated maps is used in performing the XOR procedure on the substituted image.

The second multimedia cryptosystem is based on quantum walks to possess the ability to withstand potential attacks from quantum and classical computers.

The third multimedia cryptosystem explores the integration of QW into optical image encryption frameworks. The proposed protocol is designed so that QW is used to generate two random masks used in the DRPE system, as well as to permute and diffuse the original image.

Finally, the benefits of quantum walks are utilized to propose three authenticated quantum cryptography protocols based on quantum walks for secure wireless sensor communications: the first one is authenticated quantum key distribution, the second is authenticated semi-quantum key distribution with one of the two participants having limited quantum capabilities, and the last protocol is authenticated semi-quantum key distribution with both legitimate users having limited quantum capabilities.

The advantages of the proposed quantum cryptography protocols are: a) the pre-shared master key parameters can be reused several times, b) the authenticated partners can establish various secret keys with the same transferred qubits, c) the number of bits for the shared secret key may be greater than the number of shared qubits several times according to the used N and N_{key}, and d) the protocols rely on a one-way quantum communication channel, while all previous proposed SQKD protocols rely on a two-way quantum communication.

CHAPTER 5

RESULTS AND EVALUATION

5.1 Introduction

This thesis encompasses both theoretical analyses and simulation evaluations. The algorithms will be investigated by assessing their performance using simulations, among other methods. The proposed cryptographic mechanisms will be characterized for high security, efficiency, and robustness against several well-known attacks from the literature.

To evaluate the proposed image cryptosystems, simulations were performed on a laptop equipped with an Intel Core$^{\text{TM}}$ i5-2450M processor, 6GB of RAM, and MATLAB R2016b. In the following sections, the simulation outcomes for each proposed method are presented.

5.2 Experimental Results for CIC Method

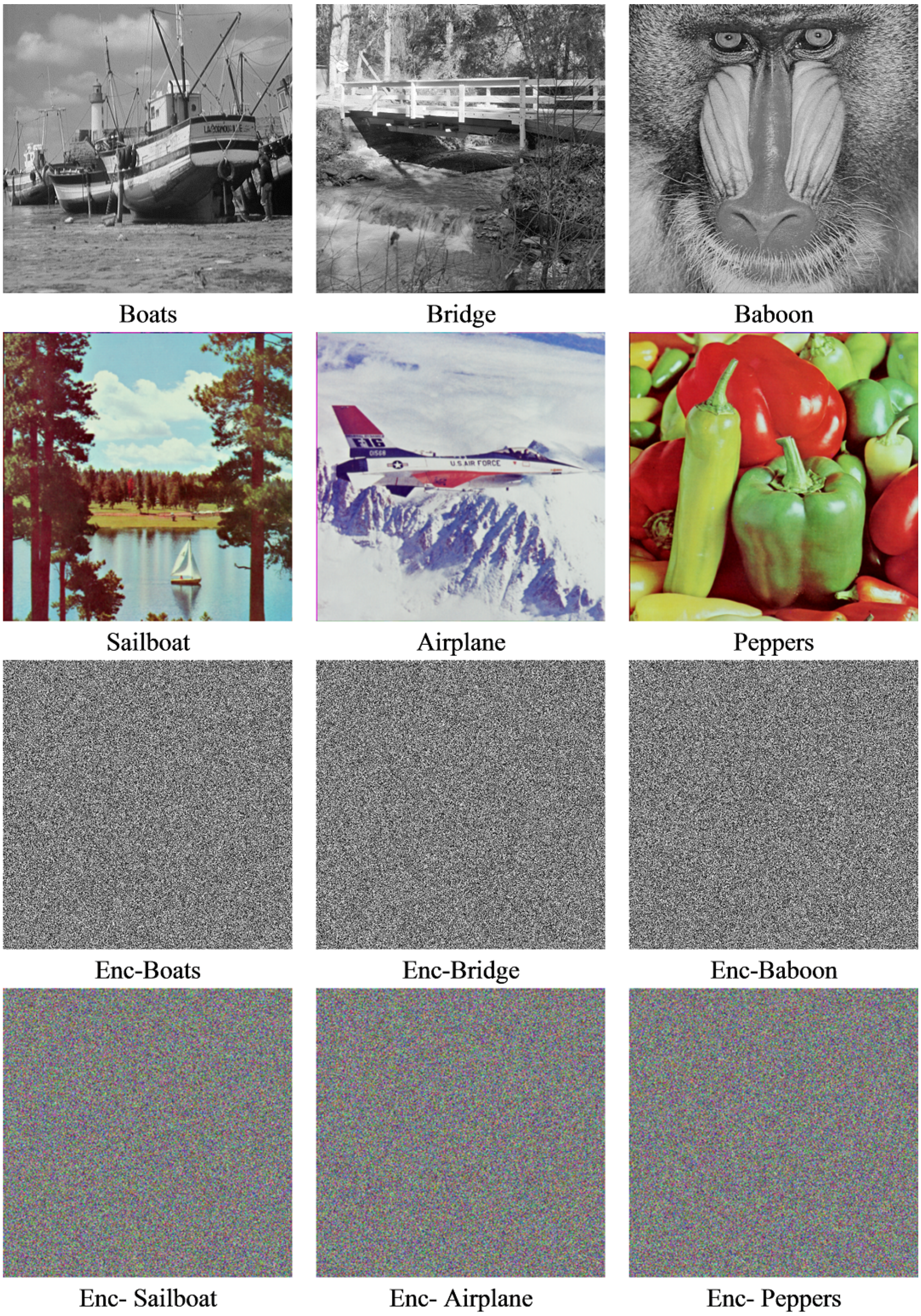
Data security plays a significant role in data transfer in cloud-based smart cities. Chaotic maps are commonly used in designing modern cryptographic applications, with 1D chaotic systems being widely employed due to their simple design and low computational complexity. However, 1D chaotic maps are susceptible to various attacks due to their chaotic, discontinuous ranges, and small key-space. To harness the benefits of 1D chaotic maps while mitigating their drawbacks, we utilize the cascading of two integrated 1D chaotic systems.

The presented CIC method is designed for data transfer in cloud-based smart cities, employing the cascading of Logistic-Chebyshev and Logistic-Sine maps. The Logistic-Sine map is used to permute the plain image, and the Logistic-Chebyshev map is used to substitute the permuted image. Both integrated maps are cascaded and utilized in performing an XOR procedure on the substituted image.

To assess the performance of the presented encryption system, the Classical image cryptosystem (CIC) in 4.2, standard test images from the SIPI database (SIPI (2020)) with dimensions of 512×512 are used, as shown in Fig. 5.1. These images are labeled as (Boats, Bridge, Baboon, Sailboat, Airplane, and Peppers). The key parameters utilized to iterate Logistic-Chebyshev and Logistic-Sine maps are initialized as follows: $LC_0 = 0.684$, $\alpha = 3.356$, $A = 152$, $LS_0 = 0.4794$, and $\beta = 3.8435$. For more information about these symbols, refer to 4.2.

5.2.1 NIST SP 800-22 Test

To assess the random characteristics of the generated sequence from cascading chaotic maps and the constructed encrypted images, NIST SP 800-22 tests (Etem and Kaya (2020)) are employed for statistical evaluations. The primary objective of these tests is to measure the randomness of a sequence and identify any non-random characteristics within it. Each test produces a P-value in the range [0, 1]. If the P-value exceeds the threshold value $\mu = 0.01$, it indicates that the sequence passes the test (EL-Latif et al. (2020a)). The results of the NIST SP 800-22 tests are presented in Table 5.1, where both the cipher image Enc-Sailboat and the key stream generated from chaotic maps successfully passed all NIST SP 800-22 tests.



Boats
Bridge
Baboon
Sailboat
Airplane
Peppers
Enc-Boats
Enc-Bridge
Enc-Baboon
Enc- Sailboat
Enc- Airplane
Enc- Peppers

Figure 5.1: The first two rows display the used investigation images, whereas the last two rows display their ciphered images using the presented cryptosystem

5.2.2 Time Efficiency

To assess the time efficiency of the proposed cryptosystem for the encryption process, Table 5.2 provides a straightforward comparison of encryption times

Table 5.1: P-values and outcomes of NIST SP 800-22 tests for the cipher image Enc-Sailboat

Test name		P-value		Outcome
		Enc- Sailboat	Key stream	
Rank		0.277427	0.023295	Passed
Random excursions variant (x = 1)		0.758288	0.911716	Passed
Random excursions (x = 1)		0.759421	0.324551	Passed
Long runs of ones		0.538239	0.047194	Passed
Overlapping templates		0.309669	0.864874	Passed
Frequency		0.275713	0.305835	Passed
Linear complexity		0.299882	0.348444	Passed
Block-frequency		0.469785	0.646149	Passed
Runs		0.423022	0.456241	Passed
No overlapping templates		0.686946	0.311721	Passed
Universal statistical		0.943058	0.638841	Passed
Spectral DFT		0.912314	0.890517	Passed
Approximate entropy		0.358094	0.373851	Passed
Serial	test1	0.752991	0.278112	Passed
	test2	0.551133	0.465868	Passed
Cumulative sums	forward	0.483105	0.282021	Passed
	reverse	0.388377	0.348202	Passed

Table 5.2: Comparisons of encryption time (in seconds) for the proposed image cryptosystem with related cryptosystems for different sizes of images 256, 512, and 1024

Encryption scheme	Image size		
	256 × 256	512×512	1024×1024
Proposed	0.0494	0.3033	1.0453
Xian and Wang (2021)	0.0779	0.3261	1.3146
Hua et al. (2015)	0.0538	0.2338	1.1494
Zhou et al. (2014a)	0.1789	0.6639	3.1426
Hua et al. (2019)	0.0949	0.4010	1.9857

for the proposed image cryptosystem and related cryptosystems across various image sizes. The encryption times for related works are reported in (Xian and Wang (2021); Hua et al. (2015); Zhou et al. (2014a); Hua et al. (2019)). The data in Table 5.2 clearly demonstrates that the presented mechanism outperforms other systems in terms of encryption time.

5.2.3 Correlation Analysis

In plain images, each pixel is highly correlated with its neighboring pixels, and the correlation value is close to 1 in all directions (horizontal, vertical, and diagonal). However, for the generated ciphered images using a well-designed image cryptosystem, the correlation values should be close to 0 (Abd-El-Atty et al. (2019a)). To calculate the correlation values between cipher images and their corresponding plain ones, we randomly select 10^4 pairs of adjacent pixels in each direction.

The correlation value is computed using the following equation:

$$V = \frac{\sum_{x=1}^{T}\left(P_x - \bar{P}\right)\left(C_x - \bar{C}\right)}{\sqrt{\sum_{x=1}^{T}\left(P_x - \bar{P}\right)^2 \sum_{x=1}^{T}\left(C_x - \bar{C}\right)^2}} \tag{5.1}$$

Here, T refers to the total number of neighboring pixel pairs in each direction, and P_x and C_x denote the values of neighboring pixels. The correlation values for the experimental datasets are provided in Tables 5.3 and 5.4. The correlation distribution of neighboring pixels for the grayscale Boats image before and after encryption is plotted in Fig. 5.2, while the correlation distribution of the color Sailboat image before and after encryption is plotted in Figs. 5.3, 5.4, and 5.5.

Based on the results in Tables 5.3 and 5.4, and the correlation distributions in Figs. 5.2, 5.3, 5.4, and 5.5, it is evident that the presented image cryptosystem is secure against correlation analysis, as the correlation values of the ciphered images are very close to 0.

Table 5.3: Correlation coefficients of the experimented grey-scale dataset in all directions(horizontal, vertical, and diagonal)

Image	Direction		
	Hor.	Ver.	Dia.
Boats	0.9713	0.9367	0.9212
Enc- Boats	-0.0011	0.0004	-0.0005
Bridge	0.9270	0.9397	0.8937
Enc-Bridge	0.0015	0.0004	0.0011
Baboon	0.7623	0.8641	0.7274
Enc-Baboon	-0.0002	-0.0001	0.0011

Table 5.4: Correlation coefficients of the tested color dataset in all directions(horizontal, vertical, and diagonal)

Image	Direction								
	Hor.			Ver.			Dia.		
	Red	Green	Blue	Red	Green	Blue	Red	Green	Blue
Sailboat	0.9562	0.9701	0.9708	0.9565	0.9736	0.9735	0.9464	0.9584	0.9558
Enc-Sailboat	-0.0002	-0.0003	-0.0002	0.0007	0.0002	-0.0012	-0.0006	-0.0014	0.0007
Airplane	0.9625	0.9710	0.9455	0.9721	0.9623	0.9639	0.9391	0.9406	0.9263
Enc-Airplane	-0.0003	-0.0011	-0.0001	0.0002	-0.0001	-0.0001	0.0002	-0.0005	0.0005
Peppers	0.9682	0.9846	0.9689	0.9670	0.9832	0.9671	0.9619	0.9722	0.9518
Enc- Peppers	-0.0012	-0.0009	0.0009	0.0003	-0.0008	-0.0009	0.0003	0.0003	-0.0004

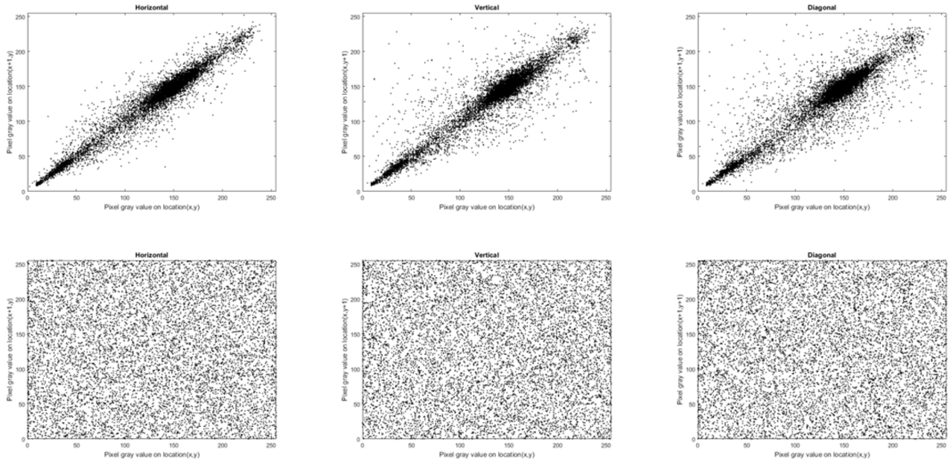


Figure 5.2: Correlation distribution of Boats image, wherever the correlation distribution of the plain image is stated in the first row, and the correlation distribution of the cipher image is stated in the last row

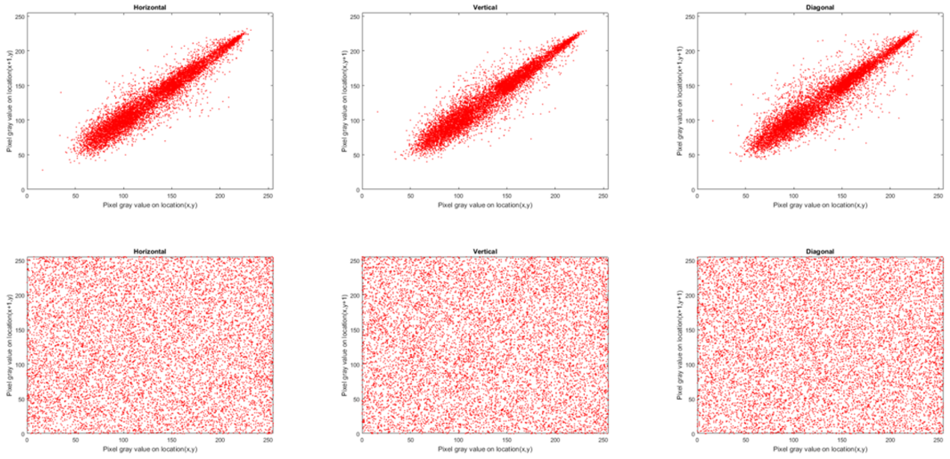


Figure 5.3: Red channel of Sailboat-Correlation distribution

5.2.4 Pixels change rate

To evaluate the sensitivity of plain images to minor bit changes, we employ two measures: Unified Average Changing Intensity (UACI) and Number of Pixels Change Rate (NPCR). The mathematical representations of NPCR and UACI are as follows:

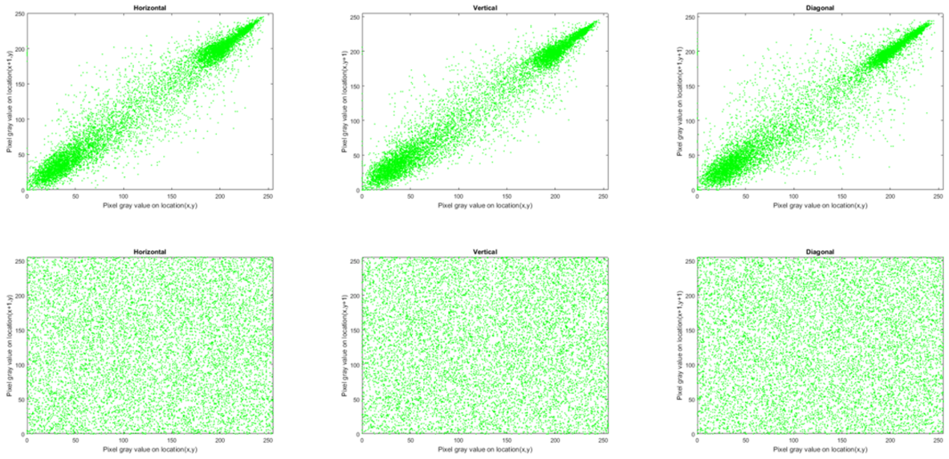


Figure 5.4: Green channel of Sailboat-Correlation distribution

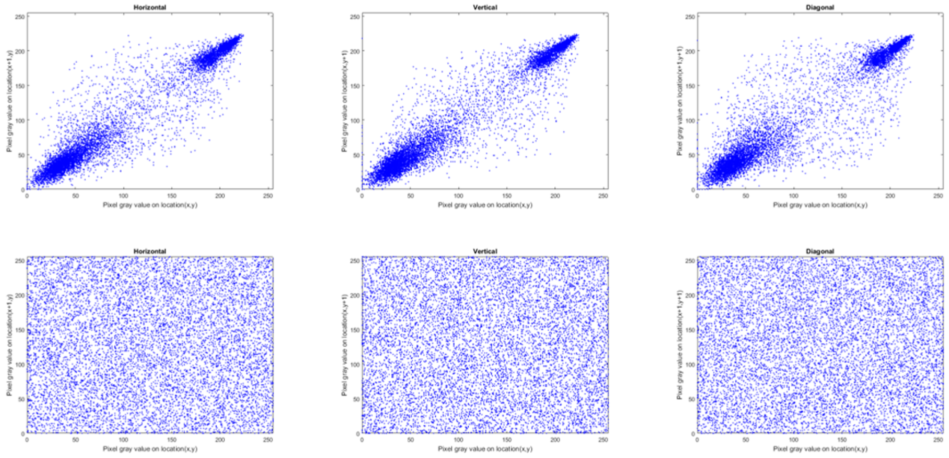


Figure 5.5: Blue channel of Sailboat-Correlation distribution

$$
\begin{aligned}
NPCR &= \frac{\sum_{x;y} Diff(x,y)}{T} \times 100\%,\\
Diff(x,y) &= \begin{cases} 0 \; if \; C1(x,y) = C2(x,y) \\ 1 \; if \; C1(x,y) \neq C2(x,y) \end{cases}
\end{aligned}
\tag{5.2}
$$

$$
UACI = \frac{1}{T}\left(\sum_{x,y} \frac{|C1(x,y) - C2(x,y)|}{2^b - 1}\right) \times 100\% \tag{5.3}
$$

Here, *C1* and *C2* represent two encrypted images for a single plain image with changes of one bit, T refers to the total number of pixels in the image, and b indicates the number of bits used to describe the pixel value. The outcomes of NPCR and UACI for plain and cipher images are provided in Table 5.5,

Table 5.5: Results of NPCR and UACI values of the experimented datasets

Image	NPCR (%)	UACI (%)
Boats	99.61776	33.44965
Bridge	99.62539	33.46607
Baboon	99.62387	33.56153
Sailboat	99.62043	33.44339
Airplane	99.62234	33.45237
Peppers	99.62209	33.45786

demonstrating that the proposed image cryptosystem is highly sensitive to minor pixel variations in the plain image.

5.2.5 Histogram Analysis

A histogram provides insight into the frequency distribution of pixel values within an image. An effective cryptosystem should ensure the uniformity of histograms for different encrypted images. Figure 5.6 displays the histograms of grayscale images before and after the encryption process, while Figure 5.7 shows the histograms of the plain and the cipher Sailboat image. The histograms of plain images exhibit differences among themselves, while the histograms of the corresponding cipher images are consistent and uniform.

To quantitatively assess the histogram test, a chi-square test (χ^2) is conducted, as expressed in Eq. (5.4) (Tsafack et al. (2020a)). This statistical analysis helps confirm the uniformity of the histograms and the effectiveness of the encryption process.

$$\chi^2 = \sum_{i=0}^{255} \frac{(f_i - s)^2}{s} \tag{5.4}$$

Here, f_i represents the frequency of the pixel value i, and s is the image dimension. Assuming a significance level of $\lambda = 0.05$, we have $\chi^2_\lambda(255) = 293.25$. For a given image, if the χ^2 value is less than $\chi^2_\lambda(255)$, it confirms the uniformity of the histogram for that image. Conversely, if the χ^2 value is greater, the image exhibits a non-uniform distribution.

Tables 5.6 and 5.7 present the results of χ^2 for the analyzed dataset. Notably, the χ^2 values for all cipher images are smaller than $\chi^2_\lambda(255)$. As a result, the presented encryption algorithm effectively resists histogram analysis attacks.

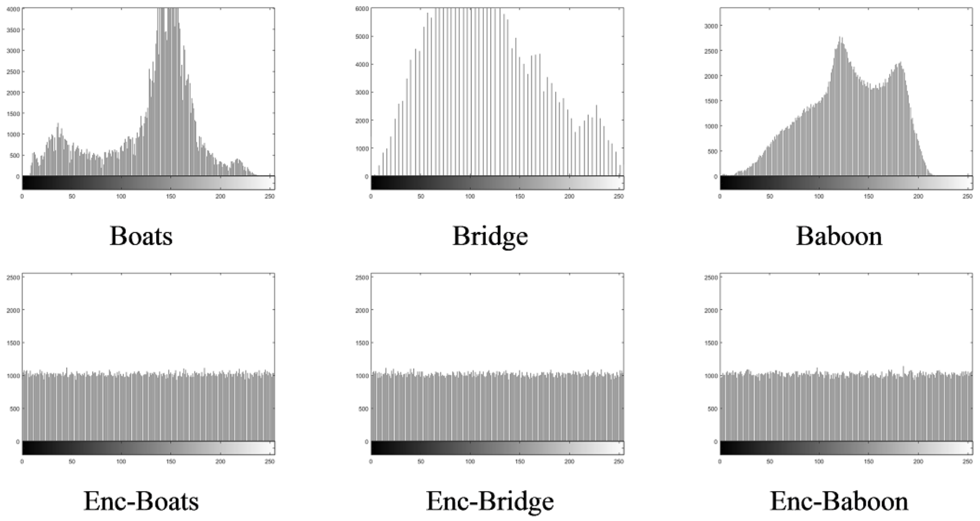


Figure 5.6: The histogram of the tested greyscale images, in which the encrypted images are totally having a uniform distribution

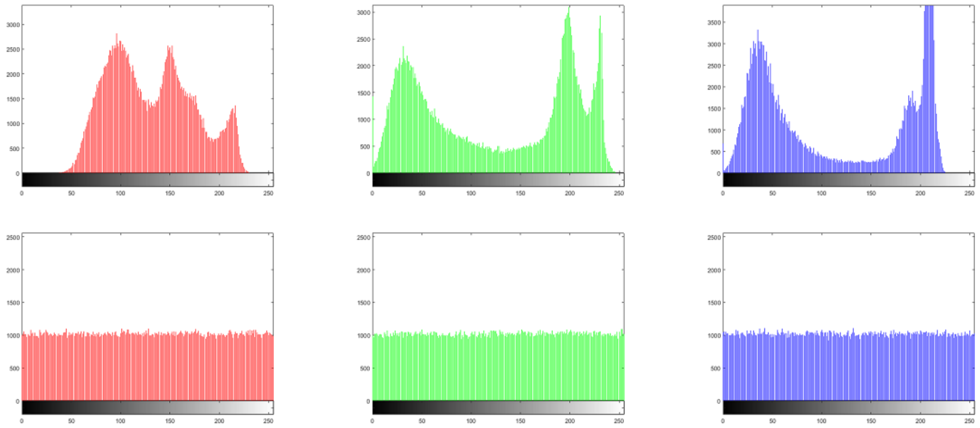


Figure 5.7: The histogram of Sailboat color image, in which the three channels of the cipher image are totally having a uniform distribution.

5.2.6 Information entropy analysis

To compute the distribution of pixel values per level in an image, the global entropy test is employed, which can be defined as follows:

Table 5.6: χ^2 values of the experimented greyscale images

Image	Chi-square value	Result
Boats	383969.687	Non-uniform
Bridge	1185618.347	Non-uniform
Baboon	187692.171	Non-uniform
Enc-Boats	277.561	Uniform
Enc-Bridge	263.324	Uniform
Enc-Baboon	286.876	Uniform

Table 5.7: χ^2 values of the experimented color images

Image	Chi-square value			Result
	R	G	B	
Sailboat	1.96697306	1.30154716	3.44571537	Non-uniform
Airplane	678424.492	682495.382	1107858.005	Non-uniform
Peppers	213187.216	318382.929	491428.177	Non-uniform
Enc-Sailboat	215.636	243.337	232.412	Uniform
Enc-Airplane	204.193	269.281	287.061	Uniform
Enc-Peppers	235.867	251.417	239.181	Uniform

$$E(X) = \sum_{i=0}^{255} p(x_i)\log_2 \frac{1}{p(x_i)} \tag{5.5}$$

Here, $p(x_i)$ represents the probability of x_i. In grayscale images, there are 2^8 possible values, so the ideal entropy value is 8 bits. To assess the effectiveness of the proposed image cryptosystem, the entropy values for the ciphered image should be close to 8 bits. However, global entropy alone may not fully assess the true randomness of encrypted images. Therefore, local entropy can be estimated by calculating the mean of global entropies for non-overlapping blocks (with 1936 pixels per block).

Table 5.8 displays the values of global and local entropies for plain images and their corresponding ciphered images. Notably, all information entropy values for the encrypted images closely approach 8 bits. This demonstrates that the suggested cryptosystem is resilient against entropy attacks.

Table 5.8: Global and local information entropies for the investigated dataset

Image	Global entropy		Local entropy	
	Original	Encrypted	Original	Encrypted
Boats	7.19137	7.99923	6.10263	7.90249
Bridge	5.70556	7.99927	4.81525	7.90286
Baboon	7.35787	7.99918	6.66019	7.90322
Sailboat	7.76216	7.99976	6.07741	7.90136
Airplane	6.66391	7.99974	5.52864	7.90223
Peppers	7.66982	7.99976	6.04964	7.90145

Table 5.9: Contrast values of the experimented greyscale images

Image	Original	Encrypted
Boats	0.37994	10.51092
Bridge	0.47895	10.49715
Baboon	0.61842	10.51323

Table 5.10: Contrast values of the experimented color

Image	Original			Encrypted		
	R	G	B	R	G	B
Sailboat	0.29432	0.48611	0.46158	10.48872	10.48024	10.50732
Airplane	0.18473	0.28502	0.13335	10.48935	10.52216	10.50711
Peppers	0.27514	0.30299	0.22137	10.50131	10.47429	10.53328

5.2.7 Contrast Analysis

To assess the variation in local intensity within an image, the contrast test is employed as a statistical measure, defined as follows in Eq. (5.6) (Ahmad and Hwang (2015)):

$$Contrast = \sum_{x=1,y=1}^{M,N} |x-y|^2 \, p(x,y) \tag{5.6}$$

Here, *p(x, y)* represents the gray-level co-occurrence matrices. High contrast values for an image indicate significant variations in gray levels, while lower values suggest more uniform gray levels.

The contrast values for both plain and cipher images are presented in Tables 5.9 and 5.10, where all cipher images exhibit high contrast values.

Table 5.11: PSNR and MSE values of experimented datasets

Image	PSNR	MSE
Boats	9.29525	7.64812
Bridge	8.77761	8.61627
Baboon	8.64496	7.28999
Sailboat	7.87325	1.01174
Airplane	7.23595	1.03475
Peppers	7.44729	1.01103

5.2.8 Peak signal-to-noise ratio analysis

To measure the noise ratio between the plain and cipher images, peak signal-to-noise ratio (PSNR) tool is employed which can be defined as given in Eq. (5.7) (Abd-El-Atty et al. (2020)).

$$\begin{aligned} &PSNR\left(P,C\right) = 20\log_{10}\left(\frac{MAX_P}{\sqrt{MSE}}\right), \\ &MSE = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}[P(x,y)-C(x,y)]^2 \end{aligned} \tag{5.7}$$

Here, MAX_P represents the maximum pixel value of the plain image P, while C indicates its corresponding cipher image, both having dimensions $M \times N$. Higher PSNR (Peak Signal-to-Noise Ratio) values suggest that the cipher image is closer to the plain image. Consequently, a well-designed encryption algorithm should yield low PSNR values, indicating that the cipher image is significantly dissimilar from its corresponding plain image.

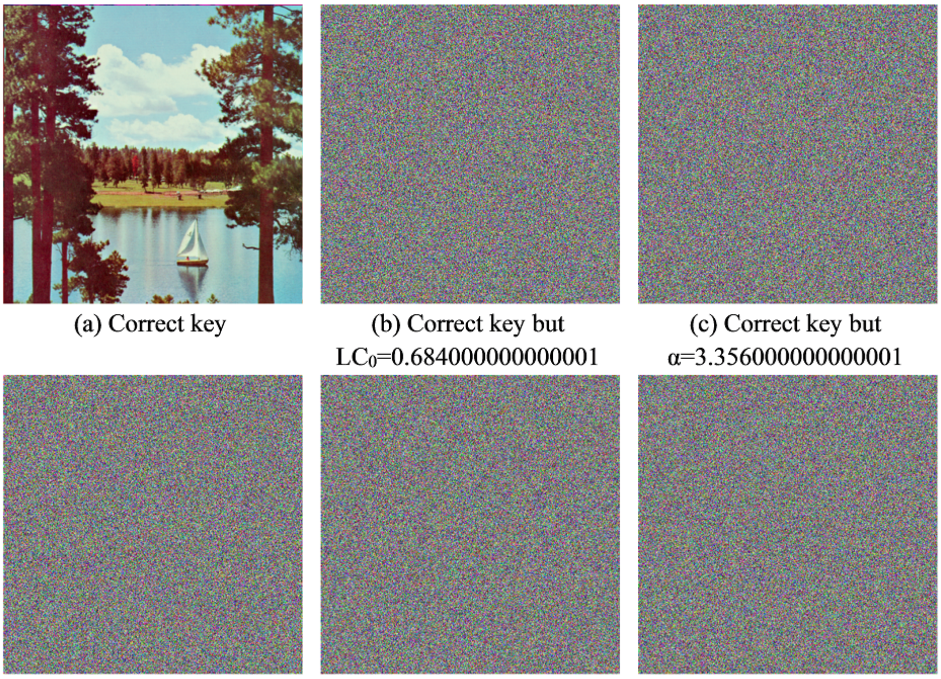
The results of PSNR and MSE (Mean Squared Error) values for the analyzed dataset are provided in Table 5.11, where the PSNR values are notably low.

5.2.9 Key space and key sensitivity analyses

The term "key space" refers to the set of various keys that could be used in brute force attacks, and it must be sufficiently large to withstand such attacks. The proposed image cryptosystem employs key parameters (LS_0, β, LC_0, α, and A) to control chaotic maps during the encryption and decryption processes. Assuming a computational precision of 10^{-16} for digital computers, the key space for the proposed cryptosystem is 10^{80}, which is ample for any modern cryptographic mechanism.

Key sensitivity indicates that even slight modifications in the initial keys should result in significant variations in the outcomes. To assess the key sensitivity of the presented cryptosystem, the encrypted Sailboat image is decrypted with minor modifications in the primary keys. The results of the key sensitivity for the presented mechanism are depicted in Fig. 5.8.

In quantitative terms, key sensitivity is evaluated using NPCR and UACI on the decrypted Sailboat image with the correct key and on other decrypted Sailboat images with slight modifications in the initial keys. The outcomes are detailed in Table 5.12. Both the table and the figure demonstrate that the proposed cryptosystem exhibits high key sensitivity, as even minor modifications in the initial keys lead to significant variations in the outcomes.



(a) Correct key

(b) Correct key but LC$_0$=0.684000000000001

(c) Correct key but α=3.356000000000001

(d) Correct key but A=153

(e) Correct key but LS$_0$= 0.479400000000001

(f) Correct key but β= 3.84350000000001

Figure 5.8: Key sensitivity of the presented encryption approach

Table 5.12: NPCR and UACI of decrypted Sailboat image with the correct key and other decrypted Sailboat images with tiny modifications in the initial keys

Image	NPCR (%)	UACI (%)
Figs. 5.8(a) and 5.8(b)	99.604415	32.209367
Figs. 5.8(a) and 5.8(c)	99.618912	32.198207
Figs. 5.8(a) and 5.8(d)	99.613063	32.211601
Figs. 5.8(a) and 5.8(e)	99.605052	32.217681
Figs. 5.8(a) and 5.8(f)	99.600856	32.191464

5.2.10 Classical Types of Attacks

During the cryptanalysis of a cryptosystem, it is generally assumed that cryptanalysts possess a complete understanding of the cryptosystem's design and have knowledge of everything related to the cryptosystem except for the values of the initial key parameters. This is a fundamental requirement for modern cryptosystems. Four classic types of attacks include ciphertext-only, known-plaintext, chosen-plaintext, and chosen-ciphertext attacks. Among these, the chosen-plaintext attack is considered the most potent, as it allows the attacker temporary access to the cryptosystem and the ability to generate ciphertext corresponding to the chosen plaintext. If a cryptosystem can withstand a chosen-plaintext attack, it is typically resilient to other types of attacks.

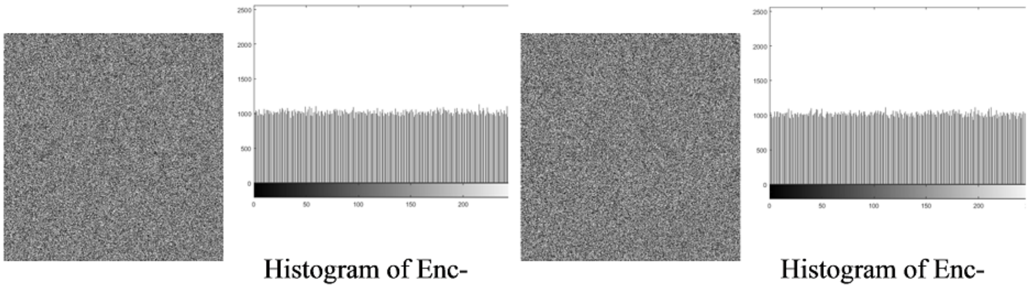
The presented cryptosystem exhibits high sensitivity to the secret key parameters (LS_0, β, LC_0, α, and A). Even minor changes in one of these secret keys lead to significant variations in the outcomes. Moreover, the proposed cryptosystem relies not only on key parameters but also on the hash value of the plain image to update the initial key parameters. Cryptanalysts attempt to extract valuable information about the secret key using full black and white images because these images can potentially disable the permutation and substitution processes.

Figure 5.9 displays the corresponding cipher images for black and white plain images, along with their histograms. These cipher images provide no visual information, and Table 5.13 offers statistical analyses for these images. As a result, the proposed encryption approach demonstrates the ability to

Table 5.13: Statistical examines of the cipher full- white and full-black images

Image	Chi value	Correlation			Entropy		Contrast
		Hor.	Ver.	Dia.	Global	Local	
Enc-white	279.8320	-0.0015	0.0004	0.0007	7.99923	7.9023	10.50954
Enc-black	280.1445	-0.0002	0.0001	0.0011	7.99922	7.9026	10.46016

withstand chosen-ciphertext and chosen-plaintext attacks.



Enc-white

Histogram of Enc-white

Enc- black

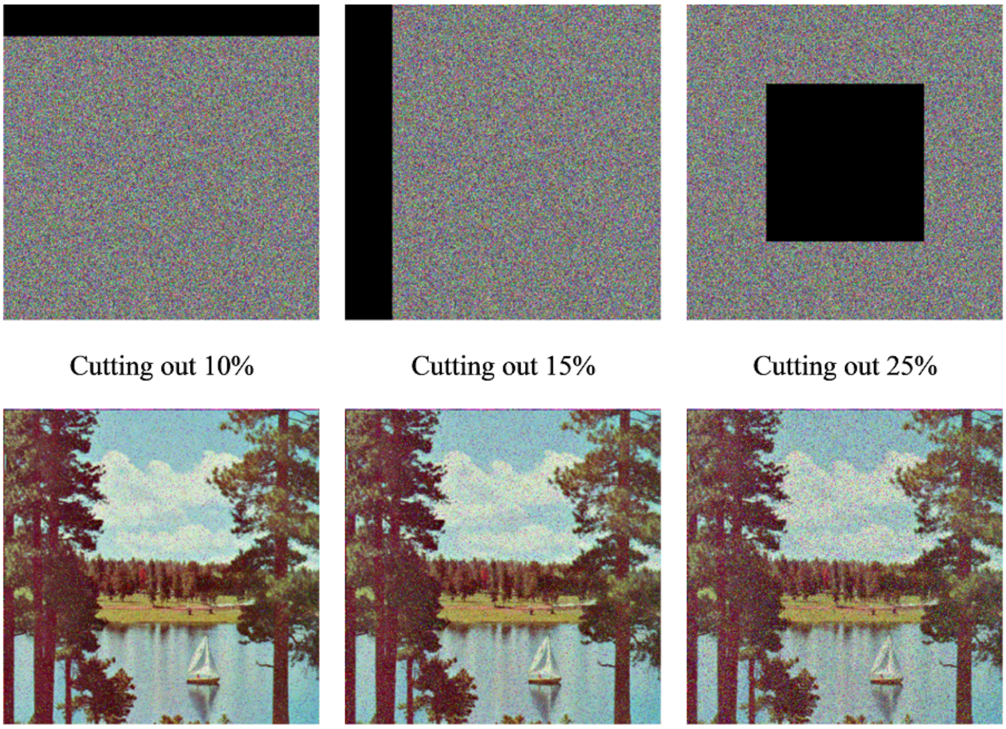
Histogram of Enc-black

Figure 5.9: Cipher images of full white and black images, and their corresponding histograms

5.2.11 Noise and data loss attacks

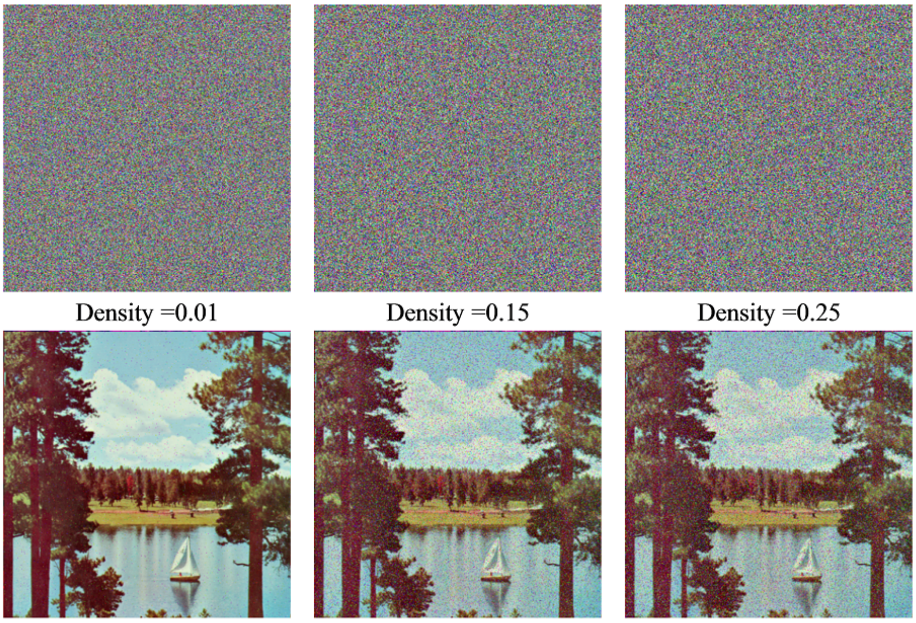
During the transmission of data over a communication channel, noise can affect the transmitted information, potentially causing data loss or corruption. Therefore, a well-designed encryption approach should have the capability to withstand data loss and noise attacks. To evaluate the resilience of the proposed cryptosystem against these attacks, occlusion attacks are conducted by removing portions of the cipher image or introducing Salt and Pepper noise to it. Subsequently, attempts are made to recover the secret image from the corrupted cipher image through the decryption process.

Figures 5.10 and 5.11 display the results of occlusion attacks, where the original image is successfully recovered after the decryption procedure.



Cutting out 10% Cutting out 15% Cutting out 25%

Figure 5.10: Data loss attack, which the first row denotes the defective cipher images by cutting out some parts and the last row signifies the corresponding deciphered ones



Density =0.01 Density =0.15 Density =0.25

Figure 5.11: Noise attack, which the first row denotes the defective cipher images by varying Salt & Pepper noise density and the last row signifies the corresponding deciphered ones

5.2.12 Comparative analysis

To confirm the effectiveness of the proposed cryptosystem in comparison to other related approaches, Tables 5.14 and 5.15 provide the average values of correlation, NPCR, UACI, local and global information entropies, Chi-square, contrast, and PSNR for the presented cryptosystem along with the average values reported in previous studies (Wang et al. (2015); Xian and Wang (2021); Gan et al. (2018); Chai et al. (2020a); Wang et al. (2019); Tsafack et al. (2020a); Ahmad and Hwang (2015); Askar et al. (2019)).

The outcomes presented in Tables 5.2, 5.14, and 5.15 clearly demonstrate the effectiveness of the proposed cryptosystem when compared to other related approaches.

Table 5.14: Comparison of the proposed algorithm with other related cryptosystems in terms of average values of correlation, NPCR, UACI, local entropy, and global entropy

Cryptosystem	Correlation			NPCR (%)	UACI (%)	Information entropy	
	Hor.	Ver.	Dia.			Global	Local
Proposed	-0.00016	0.00002	0.00023	99.62198	33.47181	7.99949	7.90227
Wang et al. (2015)	0.00200	-0.00070	-0.00140	99.65000	33.48000	7.99700	-
Xian and Wang (2021)	0.00052	0.00033	0.00087	99.60960	33.45960	7.99930	7.90237
Gan et al. (2018)	-0.00970	-0.00870	0.00650	99.60000	33.44000	7.99700	7.90217
Chai et al. (2020a)	-0.00074	0.00120	-0.00320	-	-	7.99830	-
Wang et al. (2019)	0.00219	0.00169	0.00186	99.61100	33.47567	7.99929	7.90238
Tsafack et al. (2020a)	-0.00420	-0.00490	-0.00450	99.6101	33.52520	7.9995	7.90300
Ahmad and Hwang (2015)	0.00180	-0.00161	0.00463	99.6225	33.59500	7.99301	-
Askar et al. (2019)	0.00050	0.00170	-0.00250	99.60667	33.42667	7.99866	-

Table 5.15: Comparison of the proposed cryptosystem with other related cryptosystems in terms of average values of Chi-square, contrast, and PSNR

Cryptosystem	Chi-square	Contrast	PSNR
Proposed	250.51217	10.50209	8.21239
Gan et al. (2018)	257.33667	-	-
Wang et al. (2019)	249.42857	-	-
Tsafack et al. (2020a)	249.84440	-	-
Ahmad and Hwang (2015)	-	10.43525	8.53790
Askar et al. (2019)	256.75146	10.62060	8.41076

5.3 Simulation Outcomes for QIC Method

Data security and privacy play essential roles in our daily lives. As quantum resources continue to advance, traditional cryptosystems become vulnerable to attacks. Therefore, there is a growing need for new cryptosystems based on quantum concepts. The proposed Quantum Image Cryptosystem (QIC) is an image encryption system rooted in quantum walks.

To assess the performance of the proposed image cryptosystem (see Section 4.3), simulations were conducted on a laptop equipped with an Intel Core^{TM} i5-2450M processor, 6GB of RAM, and MATLAB R2016b. The test images used in the evaluation consist of four images, each with a size of 512×512, and are labeled as Butterfly, Fish, Boats, and Houses (refer to Fig. 5.12).

The initial parameters for conducting Quantum Walks (QWs) on a circular graph are set as follows: *message=" 0010 0111 0111 0110 0011 1010 1000 0111 0100 0111", N=281, r= 561,* α*=0,* β*=1,* $\theta_0=\pi/6$*,* $\theta_1=\pi/4$*,* and $\theta_2=\pi/3$.

5.3.1 Correlation of adjacent pixels

To assess the correlation coefficient, 10^4 pairs of adjacent pixels in each direction are randomly selected, and the results are presented in Table 5.16 for the dataset under investigation. In this table, the correlation values for ciphered images are extremely close to 0. The distribution of correlation values for the Butterfly image is visualized in Fig. 5.13.

It is evident from the results shown in Table 5.16 and the plots presented in

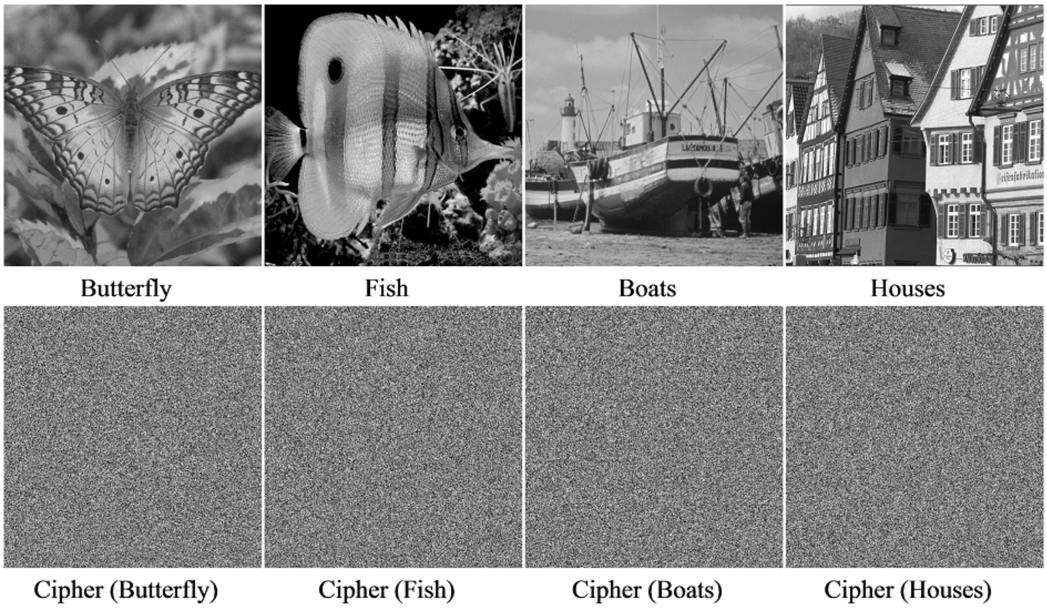


Figure 5.12: Encryption outcomes and investigated dataset of images

Fig. 5.13 that investigating the correlations in ciphered objects does not yield valuable information about the plain image.

Table 5.16: Values of correlation coefficients of the experimented images

image	Direction		
	H	V	D
Butterfly	0.9520	0.9581	0.9306
Cipher (Butterfly)	0.0002	-0.0008	0.0001
Fish	0.9657	0.9619	0.9440
Cipher (Fish)	-0.0006	-0.0003	-0.0012
Boats	0.9806	0.9631	0.9472
Cipher (Boats)	0.0001	-0.0013	0.0003
Houses	0.9239	0.8764	0.8048
Cipher (Houses)	-0.0009	0.0001	0.0009

5.3.2 Plain sensitivity test

To assess the sensitivity of tiny pixel variations in the plain image to their corresponding ciphered image, the NPCR ("Number of Pixels Change Rate") and UACI ("Unified Averaged Changed Intensity") tests are conducted (Tsafack et al. (2020b)). The results of these tests are presented in Table 5.17, where the average value of NPCR is 99.61443%. This high NPCR value indicates

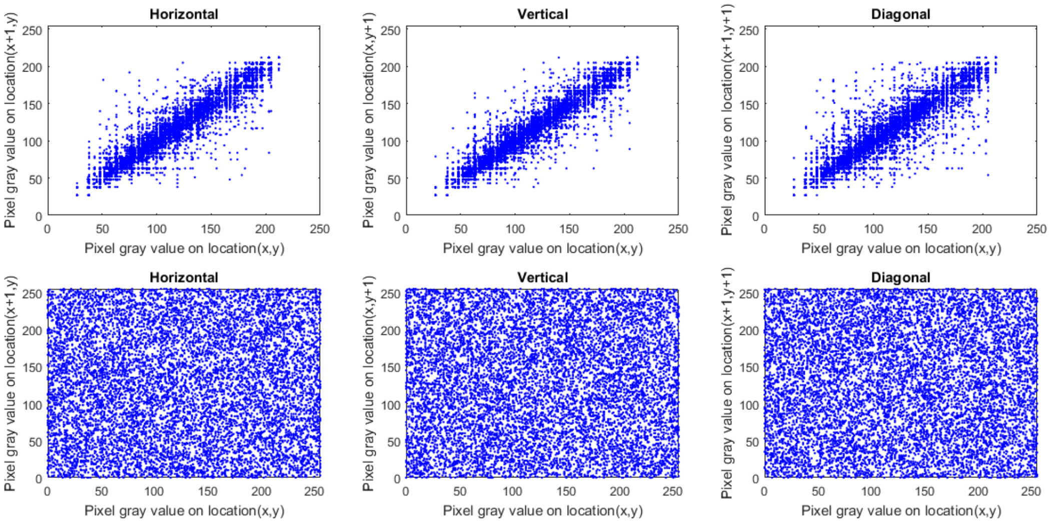


Figure 5.13: Correlation distribution for original and cipher Butterfly image

that the proposed encryption scheme is exceptionally sensitive to even minor modifications in the original image.

Table 5.17: Outcomes of UACI and NPCR tests for the experimented dataset

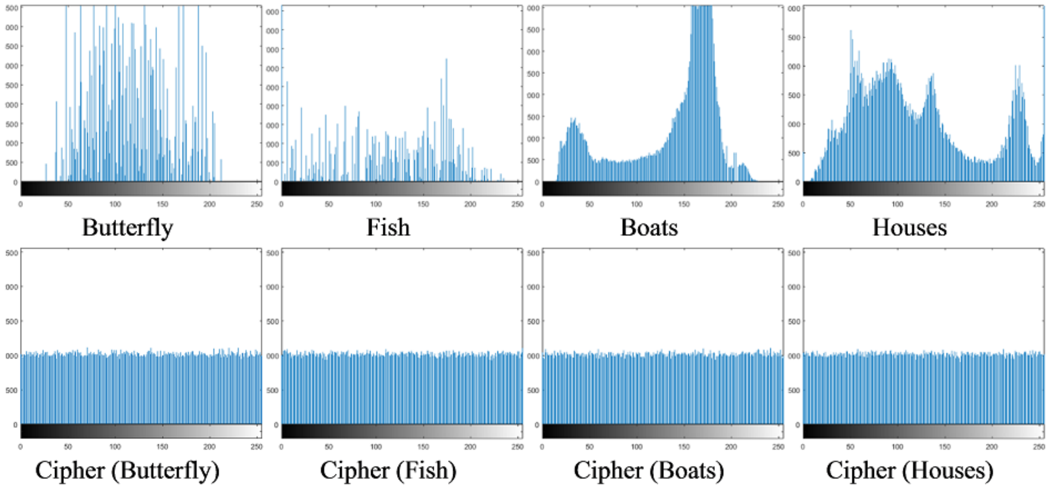
Image	UACI(%)	NPCR (%)
Butterfly	33.42073	99.60212
Fish	33.46324	99.61967
Boats	33.43596	99.61166
Houses	33.51981	99.62425

5.3.3 Histogram test

Figure 5.14 illustrates the histograms of the investigated images, which exhibit distinguishable characteristics. In contrast, the distributions of their corresponding cipher images are notably similar to each other. To confirm the uniform distribution in the encrypted images, the Chi-square test (χ^2) is employed (Alanezi et al. (2021)), and the results are presented in Table 5.18.

5.3.4 Entropy test

Table 5.19 presents the results of entropy values for the plain images and their corresponding cipher images. Notably, the entropy values of the cipher images are remarkably close to 8.



Butterfly

Fish

Boats

Houses

Cipher (Butterfly)

Cipher (Fish)

Cipher (Boats)

Cipher (Houses)

Figure 5.14: Histograms of original and cipher images for the experimented images

Table 5.18: χ^2 values for the experimented images

Image	χ^2 value	Distribution
Butterfly	567991.4023	Non-Uniform
Cipher (Butterfly)	247.6719	Uniform
Fish	3214112.7891	Non-Uniform
Cipher (Fish)	249.7734	Uniform
Boats	395837.9004	Non-Uniform
Cipher (Boats)	241.9570	Uniform
Houses	110213.4726	Non-Uniform
Cipher (Houses)	218.7012	Uniform

Table 5.19: Results of information entropy

Image	Plain	Cipher
Butterfly	6.61443	7.99932
Fish	6.01722	7.99931
Boats	7.12375	7.99933
Houses	7.69421	7.99939

5.3.5 Occlusion analysis

To assess the effectiveness of the presented encryption approach against occlusion attacks, various block sizes are used to cut out portions of the ciphered Butterfly image, followed by decryption. Figure 5.15 displays the results of occlusion attacks, where the deciphered images exhibit excellent visual quality, and no visual data is lost in the region of the truncated part.

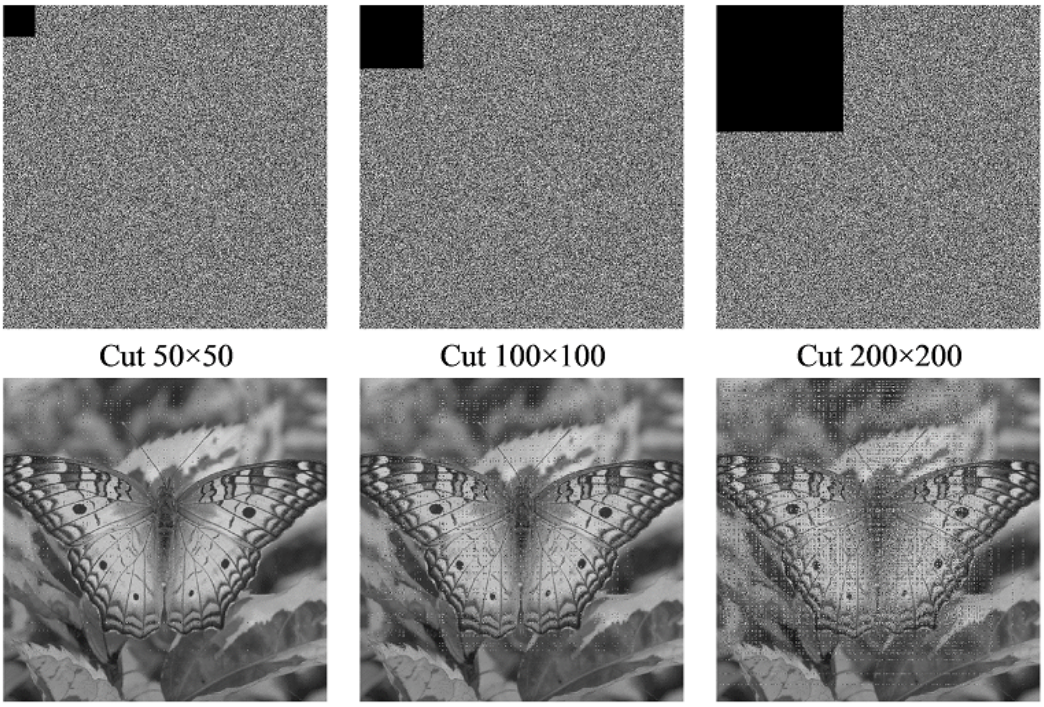
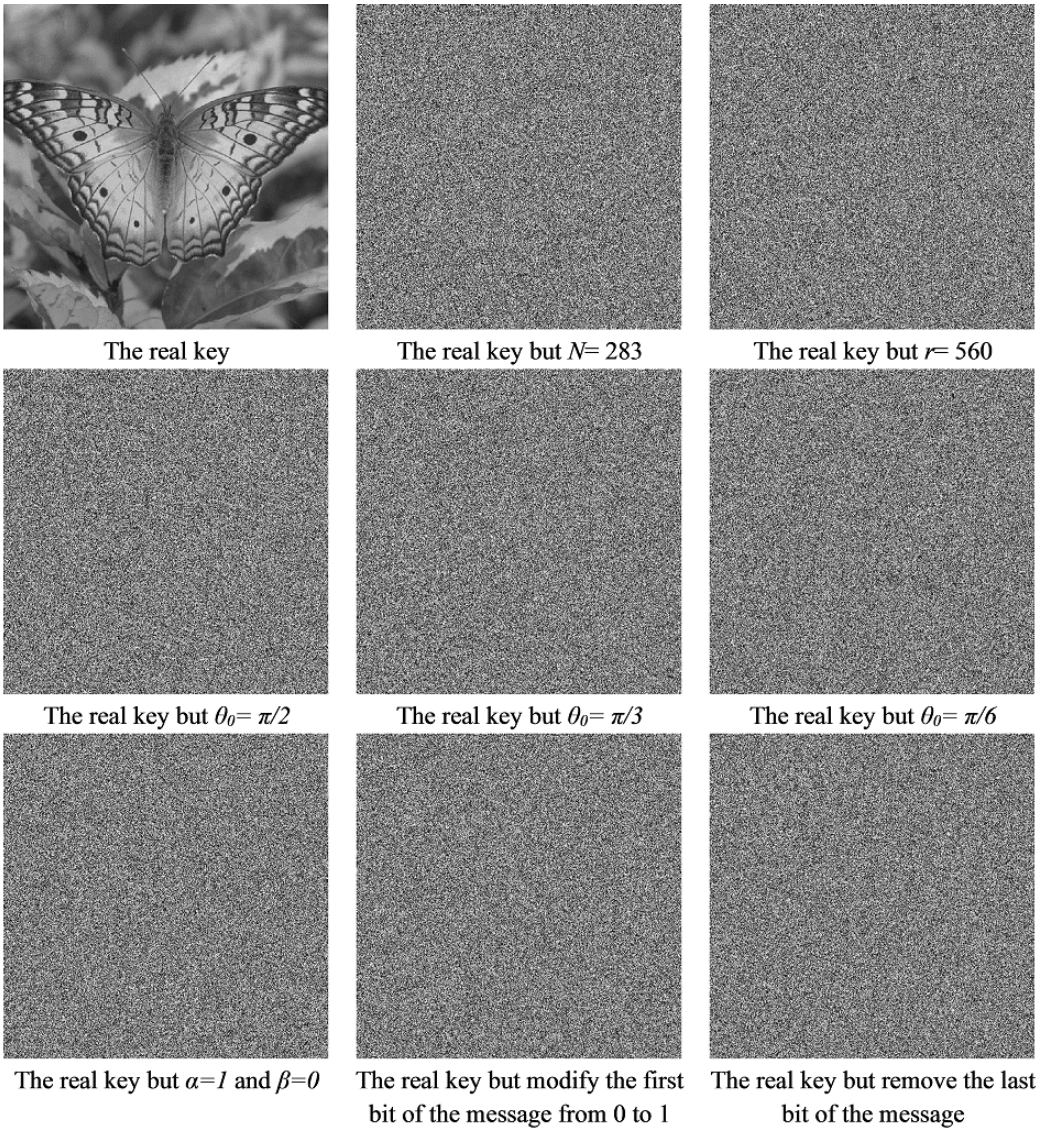


Figure 5.15: Occlusion attack, in which the top row indicates the tampered cipher images and the bottom row indicates their corresponding decrypted ones

5.3.6 Key sensitivity test

To evaluate the key sensitivity of the presented approach, the decryption procedure is executed for the cipher image Butterfly using the correct initial values with minor modifications. The results are illustrated in Fig. 5.16.



The real key

The real key but N= 283

The real key but r= 560

The real key but θ_0= $\pi/2$

The real key but θ_0= $\pi/3$

The real key but θ_0= $\pi/6$

The real key but α=1 and β=0

The real key but modify the first bit of the message from 0 to 1

The real key but remove the last bit of the message

Figure 5.16: Outcomes of executing decryption procedure for the cipher image Butterfly using true initial values with slight modifications

Table 5.20: Comparative analysis for the suggested image encryption strategy alongside some related approaches that its construction is based on quantum walks in terms of average values for correlation, Shannon entropy, NPCR, and UACI values

Cryptosystem	Correlation			Shannon entropy	NPCR (%)	UACI (%)
	H	V	D			
Proposed	-0.0003	-0.00058	0.000025	7.99934	99.614425	33.459935
Abd-El-Atty et al. (2019a)	-0.0067	-0.0021	-0.0027	7.9971	99.58	30.584
El-Latif et al. (2020d)	-0.0012	0.0004	0.0003	7.9984	99.6256	-
EL-Latif et al. (2020)	-0.0022	-0.0025	-0.0035	7.9981	99.619	-
El-Latif et al. (2020a)	0.0002	0.00135	0.0006	7.9972	99.614	-
EL-Latif et al. (2020a)	-0.0023	-0.0031	-0.0091	7.9972	99.598	-
El-Latif et al. (2020)	-0.00063	-0.00005	0.00057	7.9993	99.618	-

5.3.7 Comparative Analysis

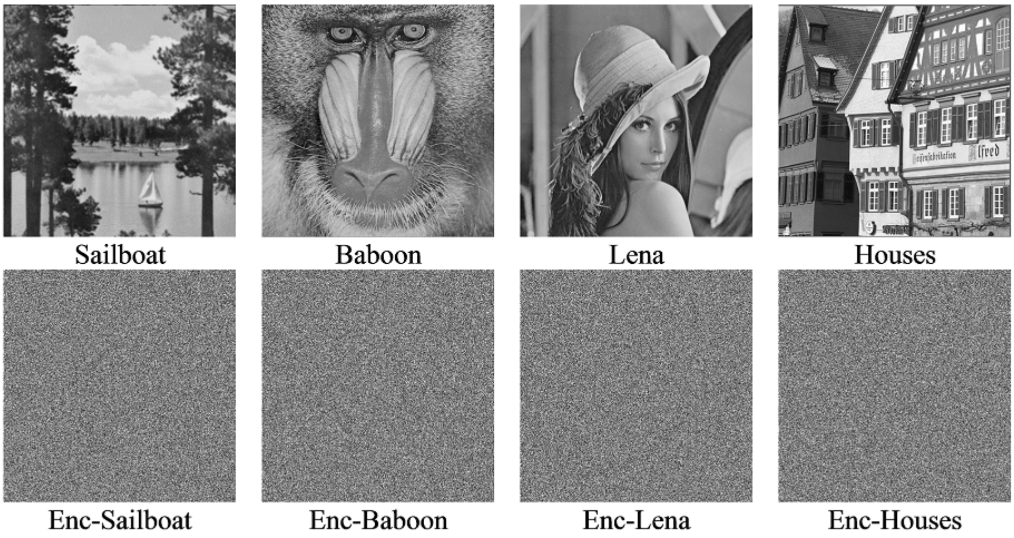
To highlight the advantages of the presented cryptosystem over some state-of-the-art cryptosystems, Table 5.20 provides a comparative analysis of the suggested image encryption strategy and related approaches based on Quantum Walks (QWs). This analysis includes average values for correlation, Shannon entropy, NPCR, and UACI. Table 5.20 unequivocally demonstrates the superior performance of the proposed cryptosystem compared to robust state-of-the-art alternatives.

5.4 Simulation Results and Analysis for OIC Method

The OIC (Optical Image Cryptosystem) is an encryption approach founded on Quantum Walks and the double random phase encoding technique. Quantum walks have proven to be a valuable tool for designing modern cryptographic mechanisms due to their ability to resist potential attacks from both digital and quantum computers. In the proposed approach, alternate quantum walks (AQW) are utilized in two encryption stages. The first stage involves inner encryption and encoding by double random phase encoding (DRPE), executed through permutation followed by substitution. Furthermore, AQW is employed to generate two random masks for the DRPE process.

To assess the effectiveness of the proposed optical image encryption approach 4.4, a dataset of images with dimensions of 512×512 is employed, including Sailboat, Baboon, Lena, and Houses (see Fig. 5.17). The initial key parameters (N_1, T_1, α_1, β_1, N_2, T_2, α_2, β_2) used for performing AQWs twice are set to ($N_1 = 17$, $T_1 = 46$, $\alpha_1 = 0$, $\beta_1 = \pi/6$, $N_2 = 17$, $T_2 = 46$, $\alpha_2 = \pi/2$, $\beta_2 = \pi/3$).

In this section, the presented mechanism is evaluated through correlation analysis, histogram analysis, data loss, and noise analysis, key space assessment, and key sensitivity analysis.


Sailboat Baboon Lena Houses

Enc-Sailboat Enc-Baboon Enc-Lena Enc-Houses

Figure 5.17: Experimental dataset and its encrypted versions

5.4.1 Correlation analysis

The correlation coefficient of neighboring pixels (C_{AB}) is employed to assess the content of an image. For plain images, its values are close to 1 in every direction, while for ciphered images, they should be close to 0. To calculate the values of C_{AB}, 10^4 pairs of neighboring pixels in each direction are randomly selected. The resulting values of C_{AB} are presented in Table 5.21, where the values for encoded images are extremely close to 0. Additionally, the distribution of correlations for the Sailboat image is depicted in Fig 5.18. It is evident from the results provided in Table 5.21 and the diagrams in Fig. 5.18 that no valuable information can be extracted from the plain images through correlation analysis of the encoded images.

5.4.2 Histogram analysis

Figure 5.19 displays the histograms of various original images, which differ from each other, while the distributions of their encoded analogue images are similar to each other. Therefore, the presented optical image encryption scheme can withstand histogram analysis attacks.

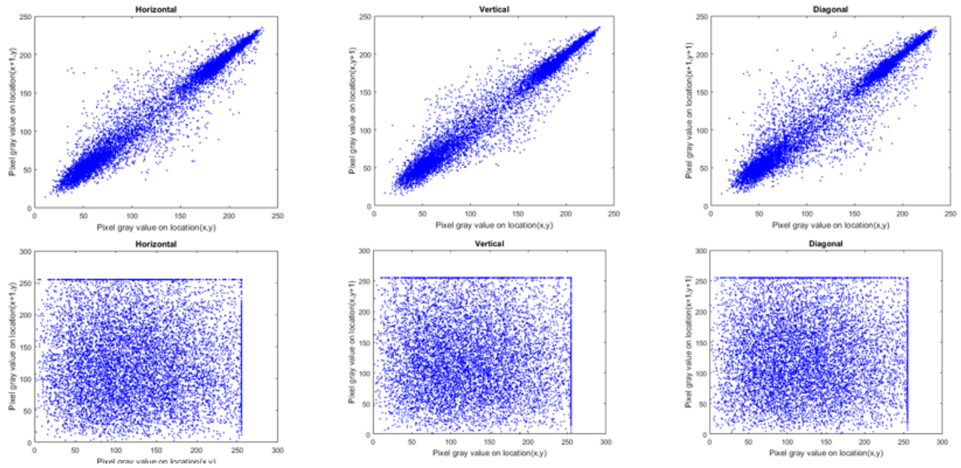
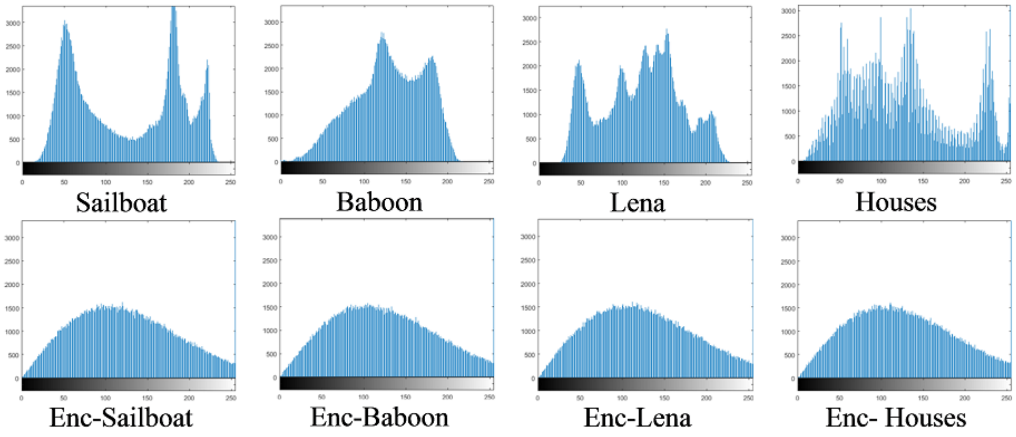


Figure 5.18: Distribution of correlation for Sailboat image.

Table 5.21: C_{AB} values for the experimented dataset

Image	Direction	C_{AB} value	
		Plain	Encoded
Sailboat	H	0.9725	0.0010
	V	0.9780	-0.0004
	D	0.9590	0.0009
Baboon	H	0.7544	0.0009
	V	0.8612	-0.0008
	D	0.7236	-0.0005
Lena	H	0.9856	-0.0002
	V	0.9714	0.0001
	D	0.9589	-0.0013
Houses	H	0.9189	-0.0008
	V	0.9079	-0.0009
	D	0.8328	0.0011


Sailboat Baboon Lena Houses

Enc-Sailboat Enc-Baboon Enc-Lena Enc- Houses

Figure 5.19: Histograms of plain and encoded images.

5.4.3 Noise and data loss analysis

Admittedly, most data channels are noisy channels. When data is transmitted over noisy channels, it can easily be damaged by noise or data loss. Therefore, a well-designed optical cryptosystem must be able to withstand noise and data loss attacks. To evaluate the presented mechanism against data loss and noise attacks, data cutting blocks of different sizes or Salt & Pepper noise with varying densities were applied to the encoded image, and then it was decrypted. Figures 5.20 and 5.21 show the outcomes of noise and data loss attacks, respectively. It is evident that when a part of the encoded image is lost, the decoded image maintains good visual quality without loss of visual information in the affected area.

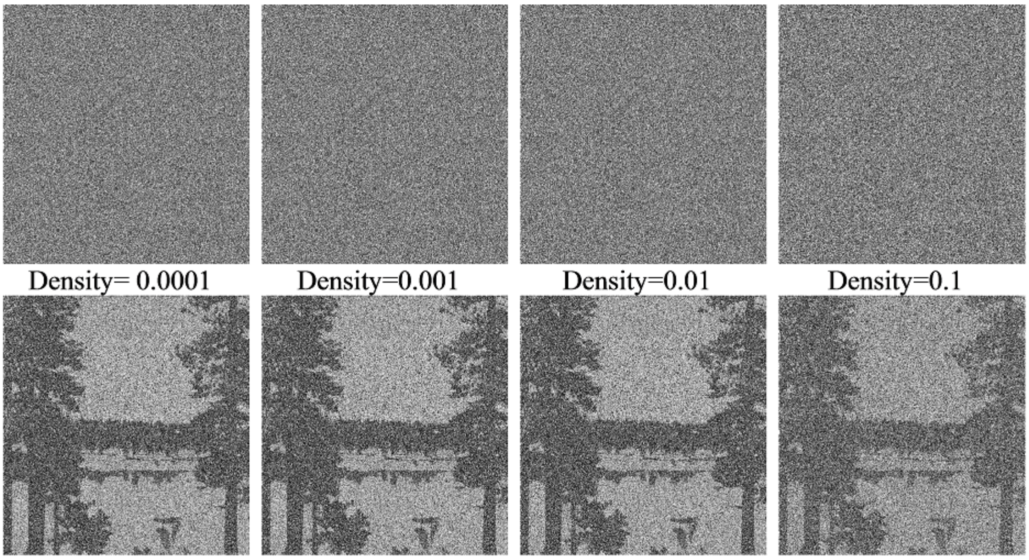


Figure 5.20: Noise attack analysis. The first row points to the noisy encoded image with different noise density while the second row represents the corresponding decoded image

5.4.4 Keyspace and key sensitivity analysis

A well-designed optical encryption mechanism must have a sufficiently large key space for the keys used in the encoding process. In this context, the presented optical encryption mechanism utilizes the key parameters (N_1, T_1, α_1, β_1, N_2, T_2, α_2, β_2) to perform AQW twice, generating a probability dis-

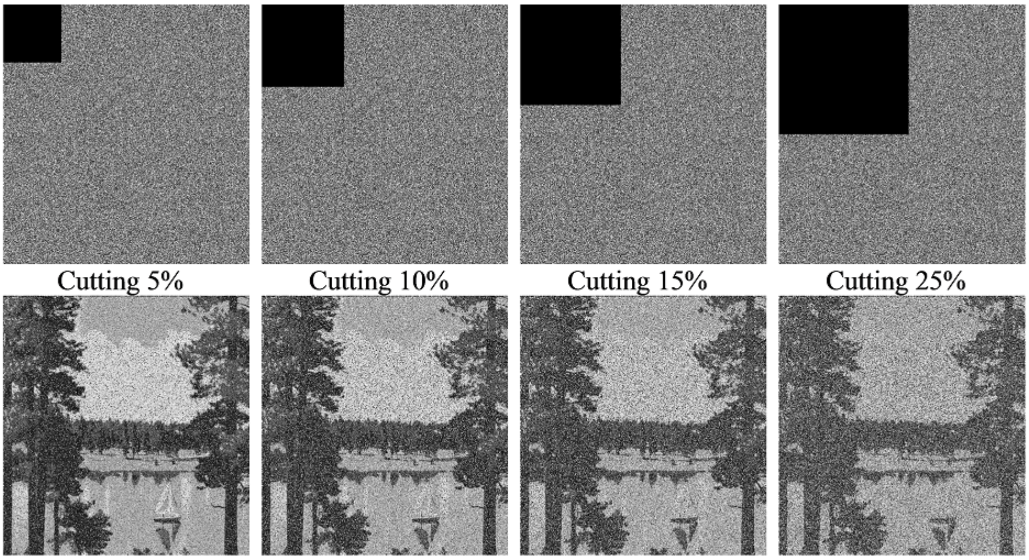


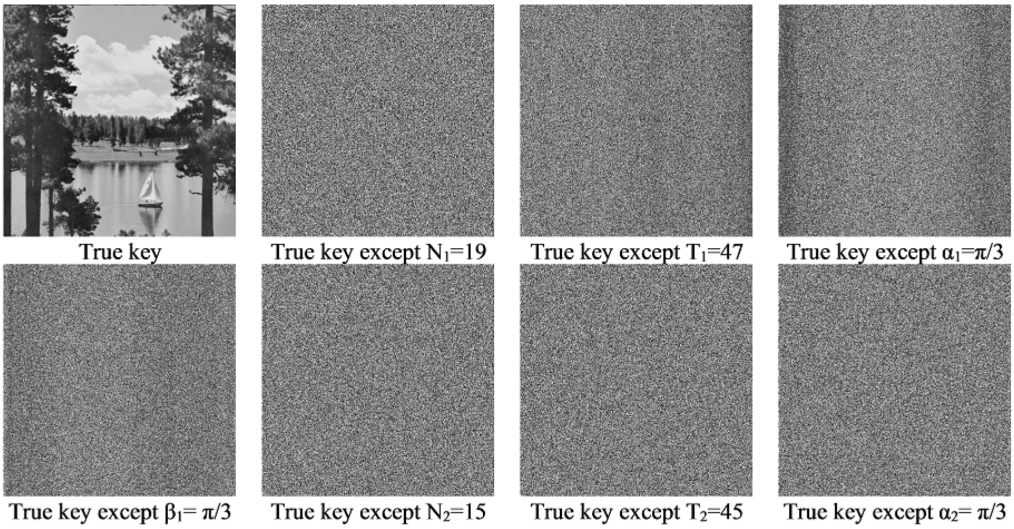
Figure 5.21: Data loss analysis. The first row points to the encoded image with a block data loss while the second row represents the equivalent decoded image.

tribution matrix used in the substitution, permutation, and random phase mask generation processes. AQW theoretically has an infinite key space, but in practice, the key space is finite. Assuming a computation precision of 10^{-16}, the key space for the proposed optical encryption method is 10^{128}, which is more than sufficient for any optical encryption approach. Additionally, the presented mechanism is based on quantum walks, and its security is guaranteed by quantum mechanics.

Furthermore, to assess the key sensitivity of the suggested optical encryption approach, the decoding procedure was carried out for the encoded Sailboat image with various small changes to the key parameters. The results are provided in Fig. 5.22.

5.5 Analysis of the Proposed AQC Protocols

The benefits of quantum walk characteristics are utilized to propose three authenticated quantum cryptography protocols based on quantum walks for secure wireless sensor communications. The first one is authenticated quantum key distribution, the second is authenticated semi-quantum key distribution



True key

True key except $N_1=19$

True key except $T_1=47$

True key except $\alpha_1=\pi/3$

True key except $\beta_1= \pi/3$

True key except $N_2=15$

True key except $T_2=45$

True key except $\alpha_2= \pi/3$

Figure 5.22: Decoding the encoded Sailboat image with several tiny changes in key parameters.

with one of the two participants having limited quantum capabilities, and the last protocol is authenticated semi-quantum key distribution with both legitimate users having limited quantum capabilities. The advantages of the proposed quantum cryptography protocols are as follows: a) the pre-shared master key parameters can be reused several times, b) the authenticated partners can establish various secret keys with the same transferred qubits, c) the number of bits for the shared secret key may be greater than the number of shared qubits several times according to the used N and N_{key}, and d) the protocols rely on a one-way quantum communication channel, while all previously proposed SQKD protocols rely on a two-way quantum communication.

This section aims to demonstrate that the proposed authenticated quantum cryptography protocols in Section 4.5.2 are highly efficient and secure against several well-known attacks, such as intercept-and-resend attacks and impersonation attacks.

5.5.1 Efficiency analysis

One of the essential tools to measure the efficiency of quantum protocols is the qubit efficiency, which presented by Cabello (2000) and can be denoted as follows:

$$\eta_{qubit} = \frac{K}{B+C} \tag{5.8}$$

where K is the total number of bits for the established secret key, B represents the number of generated qubits, and C refers to the number of exchanged classical bits over the classical channel, except those used for eavesdropping check (Shukla et al. (2017)). One of the main advantages of a quantum hash function based on quantum walks is that the length of the hash value varies with the number of nodes in the circle. In the proposed protocols, Alice informs Bob of a value for N to run QWs (N,ω,θ_2) to produce a hash value $B \in \{0,1\}^{8N}$ with a length of $8\times N$ (step *1*) and announces another integer odd number N_{key} to run the QWs $(N_{key},R,\omega,\theta_0,\theta_1,\theta_2)$ for generating a hash value $K \in \{0,1\}^{8N_{key}}$ with a length of $8\times N_{key}$ as a secret key (step *7*). Therefore, the qubit efficiency of the proposed authenticated quantum cryptography protocols depends only on the number of nodes in the circle (N, N_{key}) announced by Alice for running quantum walks. If the number N_{key} announced by Alice is greater than N several times, then the number of bits for the shared secret key K is greater than the number of shared qubits B several times. In the illustrated examples (see Figs. 4.7, 4.9, and 4.11), Alice communicates with Bob via the classical channel using 5 (3-bit) for N and 25 (5-bit) for N_{key}, so the total number of exchanged classical bits over the classical channel is 8 bits. The number of bits for the shared secret key K is 200 bits, and the total number of generated qubits is 40 qubits. Therefore, the qubit efficiency for the illustrated examples only is $\frac{K}{B+C} = \frac{200}{40+8} = \frac{200}{48} = 4\frac{1}{6}$. Furthermore, the partners can establish various numbers of keys Ks with the same transferred qubits B by repeating step 7 several times with announcing different N_{key} each time (see Figs. 4.7, 4.9, and 4.11).

There are another measure for efficiency is the pre-shared key efficiency, which can be stated as in Eq.(5.9).

$$\eta_{pre-shared} = \frac{K}{M} \tag{5.9}$$

Where K represents the total number of bits for the established secret key, and M denotes the total number of bits for the pre-shared master key. The participants of the presented protocols require pre-shared master key parameters $(\omega, \theta_0, \theta_1, \theta_2)$ for implementing one-walker quantum walks on a circle with an odd N vertices. These parameters are numerical values. In the illustrated examples (see Figs. 4.7, 4.9, and 4.11), $\omega = 0$ (1-bit), $\theta_0 = 60$ (6-bit), $\theta_1 = 45$ (6-bit), and $\theta_2 = 36$ (6-bit). Therefore, the total number of bits for the pre-shared master key is 19 bits. Consequently, the pre-shared key efficiency for the illustrated examples is $\frac{K}{M} = \frac{200}{19} = 10.53$. Table 5.22 demonstrates the efficiency of the presented protocols, providing the qubit efficiency and pre-shared key efficiency for the proposed authenticated quantum cryptography protocols and their related ASQKD protocols (Li et al. (2016a); Yu et al. (2014)). As a result, the proposed protocols exhibit high efficiency.

Table 5.22: Qubit efficiency and pre-shared key efficiency for the proposed authenticated cryptography protocols and its related ASQKD protocols

Protocol	The sender	The receiver	Quantum channel	Quantum information carrier	Pre-shared key efficiency	Qubit efficiency
Proposed AQKD	Fully quantum	Fully quantum	One-way	Single particles	polynomial efficiency is achieved with the key parameters illustrated in the examples with an improvement of 1053%	Depending on the announced N and N_{key}, a polynomial efficiency with 416.67% is achieved
Proposed ASQKD1	Fully quantum	Restricted quantum capabilities				
Proposed ASQKD2	Restricted quantum capabilities	Restricted quantum capabilities				
Yu et al. (2014) ASQKD Randomization -based	Fully quantum	Restricted quantum capabilities	Two-way	Entangled particles	10%	12.5%
Yu et al. (2014) ASQKD Measure -based				Entangled particles	10%	10%
Li et al. (2016a) ASQKD Randomization -based				Single particles	50%	25%
Li et al. (2016a) ASQKD Measure-based				Entangled particles	25%	11.11%

5.5.2 Security Analysis

Eve's primary objective is to obtain any information about the established key from the transferred qubits. Therefore, security analysis is an essential task for any quantum protocol. The security of the proposed quantum cryptography protocols is guaranteed by well-established principles such as the quantum no-cloning theorem and quantum uncertainty postulate, which prevent unconditional attacks. Additionally, security relies on the unique characteristics of quantum walks and their associated key parameters.

In cases where both participants are limited to quantum capabilities, the key established between them may not achieve conditional security but relies on mathematical computation (Zhu et al. (2018)). However, the security of the two proposed Authenticated Semi-Quantum Key Distribution (ASQKD) protocols is primarily based on the principles of quantum walks rather than mathematical computation.

In this section, we provide a detailed security analysis of the presented protocols to confirm their effectiveness in exposing and mitigating any active attacks.

5.5.2.1 Impersonation Analysis

In these types of attacks, Eve assumes the role of Bob to communicate with Alice, or vice versa, in an attempt to obtain the fully established secret key or part of it.

In the Presented AQKD Protocol: Let's assume that Eve impersonates Alice to contact Bob. In step *1*, Eve communicates with Bob and announces the value of N to produce a bit string $B^{'} \in \{0,1\}^{8N}$ by running quantum walks (N, ω, θ_2). However, it is exceedingly challenging for Eve to produce the correct hash value B, as she lacks the full key parameters (ω, θ_2). Furthermore, Eve faces significant difficulties in preparing a sequence of single photons $S \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}^{8N}$ with the correct bases according to B. Eventually, Eve transmits a fake stream of photons S to Bob based on her own bit string $B^{'}$. In step *4*, Bob measures the received qubits according to the hash value B. Then, Eve informs Bob of a value for N_{check}, which is used to generate a bit string $K_{check} \in \{0,1\}^{8N_{check}}$ by running quantum walks $(N_{check}, R, \omega, \theta_0, \theta_1, \theta_2)$.

The bit values of R recorded by Eve (*step 2*) are different from the measurement results R stored by Bob (step *4*) because the generated B streams for both partners are distinct, and Eve does not possess the correct key parameters $\omega, \theta_0, \theta_1$, and θ_2 (step *1*). Therefore, Bob can identify the presence of Eve in step *6*, once Eve publishes the first *4*×N_{check}-bit of K_{check}, thereby causing the protocol to be terminated by Bob.

On the other hand, if Eve attempts to play the role of Bob to contact Alice, she will be revealed by Alice in step *6*. Alice will inform Eve of the first *4*×N_{check}-bit sequence of K_{check} and wait for Eve's response with the remaining bits of K_{check}. By verifying the announced remaining bits of K_{check}, Alice can identify the presence of Eve and terminate the protocol.

As for the security of the proposed ASQKD1 and ASQKD2 protocols, the same analysis can be performed to detect Eve's presence in step *6* of each protocol. Therefore, the proposed authenticated quantum cryptography protocols are secure against active attacks. Moreover, Eve does not gain any information about the master key $(\omega, \theta_0, \theta_1, \theta_2)$. Therefore, the key parameters can be used multiple times.

5.5.2.2 Intercept-Resend Analysis

In this type of attack, Eve attempts to obtain any secret information by intercepting the sequence of photons S sent by Alice and then resending it to Bob.

In the Proposed AQKD Protocol: Eve's goal is to measure the photons in the sequence S transferred by Alice. However, Eve lacks information about the keys (ω, θ_2) required to measure the transferred qubits in the correct bases according to the correct hash value B. Eve ultimately performs quantum measurements in random bases and sends Bob a new sequence of photons according to her used measurement bases and corresponding measurement results. Bob measures the received qubits according to the hash value B to obtain measurement results R (step *4*) that differ from the classical bit values R recorded by Alice (step *2*). This leads to Bob generating a checking hash value K_{check} by running quantum walks (N_{check},R,ω,θ_0,θ_1,θ_2) different from Alice's K_{check} (step *5*) because the bit string R is different for both participants. Consequently, both participants detect the presence of Eve and terminate the protocol (step *6*). Therefore, the proposed AQKD protocol is secure against intercept-resend attacks.

In the Proposed ASQKD1 Protocol: Bob performs quantum measurements in the computational basis on all received qubits. Eve knows this and, since the protocol involves one-way communication, she measures all qubits in the computational basis over the sequence S sent by Alice. Eve then prepares a new sequence of photons in the computational basis according to her measurement results and sends it to Bob. In step *4* of the protocol, Bob performs quantum measurements in the computational basis on all qubits and stores only the measurement results of the i^{th} qubit when the i^{th} bit of B is *"1"* to obtain the classical bit string R. Eve does not have information regarding the key parameters (ω,θ_2) to store the measurement results when the i^{th} bit of B is *"1"*. Therefore, Eve randomly extracts a fake bit string $R^{'}$. In step *6* of the protocol, Alice and Bob check K_{check}, with no detection of the presence of Eve (the quantum channel is assumed to be ideal) because Eve sends a sequence of photons with a computational basis according to her measurement results. As a result, the protocol continues for sharing the random secret key (step *7*). Eve may partially succeed in obtaining R, but she fails to obtain any information regarding the established secret key because Eve does not possess the used master key parameters for generating the secret key through QWs (N_{key},R,ω,θ_0,θ_1,θ_2). Therefore, the proposed ASQKD1 protocol is secure against intercept-resend attacks.

The analysis for the proposed ASQKD2 protocol is similar to the analysis of the proposed ASQKD1 protocol.

5.6 Discursion

5.6.1 Strengths

Experimental validation: All three image cryptosystems were rigorously tested using various metrics, including correlation, entropy, UACI, NPCR, sensitivity, and noise analysis. These tests demonstrated strong encryption against both classical and quantum attacks. Quantum-resistant: The second and third image cryptosystems leverage quantum walks, offering potential resistance to attacks from future quantum computers. Applicability: The proposed schemes handle both color and grayscale images, and the third system integrates with optical encryption frameworks. Secure communication: The final quantum protocols for wireless sensor networks offer high efficiency and security against known attacks.

5.6.2 Limitations

Theoretical security: While experimental results are promising, further theoretical analysis is needed to fully assess the long-term security against advanced attacks. Practical adoption: Integrating quantum technologies into real-world scenarios may require overcoming additional challenges beyond encryption itself.

5.7 Conclusion

In this chapter, the performance of the presented cryptosystems based on quantum walks/chaotic systems is evaluated. First, the experimental results of the suggested approach based on chaotic systems demonstrate the effectiveness of the presented cryptosystem. The proposed encryption system is applicable to both color and grayscale images.

The second multimedia cryptosystem is based on quantum walks, providing the ability to withstand potential attacks from quantum and classical computers. A variety of tools are employed for the experimental assessment of the presented cryptosystem, including correlation analysis, histogram analysis, Shannon entropy analysis, UACI and NPCR analyses, key sensitivity analysis, and occlusion analysis. These metrics highlight the advantages of the presented cryptosystem over some robust state-of-the-art cryptosystems.

The third multimedia cryptosystem explores the integration of quantum walks into optical image encryption frameworks. Simulation-based validation of the proposed technique, including correlation, histogram, sensitivity, key space, as well as noise and data loss analysis, provides impetus to consider its use in applications in modern optical cryptosystems.

Finally, security analyses of the proposed three authenticated quantum cryptography protocols based on quantum walks for secure wireless sensor communications show that these protocols are highly efficient and secure against several well-known attacks, such as intercept-and-resend attacks and impersonation attacks. The main goal of the presented work is to open the door for integrating quantum technologies with wireless sensor networks and various Internet of Things devices to achieve high security and efficiency.

CHAPTER 6

CONCLUSION AND FUTURE WORKS

6.1 Overall Conclusions

In this comprehensive dissertation, innovative security paradigms for smart IoT systems have been presented, seamlessly integrating quantum computing algorithms and chaotic dynamical systems. The proposed security solutions span classical encryption, quantum encryption, optical encryption tailored for digital images, and authentication protocols tailored for secure communications within IoT systems embedded in smart cities. The findings can be summarized as follows:

Novel Cipher Image Mechanism: A groundbreaking contribution is made in the form of a novel cipher image mechanism designed for secure data transfer within cloud-based smart cities. This mechanism, hinging on the cascading of two chaotic maps, is proven versatile, accommodating both colour and grayscale images. Through rigorous experimental evaluation, the mechanism exhibits noteworthy effectiveness, showcasing its potential for practical applications in secure data transfer scenarios. (Alanezi et al. (2021))

Quantum Walks-Based Image Cryptosystem: A state-of-the-art image cryptosystem is introduced in the dissertation, built on the principles of quantum walks. In extensive experimental analyses, the cryptosystem emerges as a robust contender, surpassing the performance of various state-of-the-art counterparts. This contribution signifies a stride forward in the realm of quantum-based image security, demonstrating the viability and superiority of quantum walks in cryptographic applications. (Alanezi et al. (2021))

Optical Encryption with Quantum Walks and Double Random Phase Encoding: An innovative optical encryption approach, integrating quantum walks and double random phase encoding, is proposed. Through meticulous simulation, the approach demonstrates resilience against potential attacks, establishing its suitability for modern optical cryptosystems. This novel fusion of quantum walks and optical encryption stands as a testament to the versatility and effectiveness of quantum technologies in securing multimedia data. (Alanezi et al. (2021))

Secure Quantum Cryptography Protocols for Wireless Sensor Networks: The work extends to the realm of wireless sensor networks, introducing secure quantum cryptography protocols. Leveraging pre-shared master key parameters, establishing various secret keys using the same transferred qubits, generating shared secret keys exceeding the number of shared qubits, and relying on a one-way quantum communication channel, these protocols exhibit exceptional efficiency and security. This advancement paves the way for the seamless integration of quantum technologies into wireless sensor networks and IoT devices, promising heightened security and efficiency. (Alanezi et al. (2023))

In conclusion, significant contributions have been made in this research to the evolving landscape of secure IoT systems, showcasing the efficacy of quantum and chaotic systems in safeguarding sensitive data. The proposed mechanisms not only address existing vulnerabilities but also lay the foundation for future advancements in secure communication, encryption, and authentication within smart cities and IoT environments. As the transformative potential of quantum technologies continues to be witnessed, the findings offer a pioneering roadmap for the integration of these technologies into real-world applications, ensuring a future where security and efficiency coalesce seamlessly in the IoT landscape.

6.2 Future Works

As the horizon of future research is embarked upon, this dissertation lays the groundwork for pioneering advancements in securing data transfer among Internet of Things (IoT) devices. The convergence of artificial intelligence (AI) and quantum computing presents a fertile ground for innovative security mechanisms. The envisioned future works are outlined below, aiming to push the boundaries of IoT security, quantum cryptography, and quantum technologies integrated with machine learning.

Advancements in Quantum Cryptography for IoT Security:

- *Tailored Protocols for IoT Devices:* New quantum cryptography protocols will be developed, specifically designed to accommodate the unique constraints and requirements of IoT devices. This entails an in-depth exploration of the intricacies of IoT ecosystems, ensuring that the protocols align seamlessly with the diverse array of devices interconnected within these environments.

- *Real-world Implementation and Evaluation:* Quantum cryptography protocols will be implemented on actual IoT devices to bridge the gap between theoretical advancements and practical applicability. Rigorous evaluations will be conducted to assess the performance and security of these protocols in real-world scenarios, providing invaluable insights into their effectiveness and potential challenges.

- *Efficient Quantum Key Distribution:* New methods for distributing quantum keys to IoT devices will be innovated, ensuring both security and efficiency. This involves exploring novel cryptographic mechanisms and leveraging quantum principles to establish a secure and streamlined process for key distribution, addressing a critical aspect of quantum communication in IoT.

- *Integration with Machine Learning:* The synergy between quantum cryptography and machine learning will be explored to fortify IoT systems further. By integrating quantum cryptography with AI-driven security technologies, the creation of a symbiotic relationship that enhances the overall security posture of IoT environments is anticipated. This fusion has the potential to elevate the resilience of IoT systems against evolving threats.

Advancing Quantum Technologies with Machine Learning:

- *Efficient Quantum Algorithms and Protocols:* Machine learning will be utilized to develop innovative quantum algorithms and protocols that surpass the efficiency and security metrics of existing counterparts. This approach seeks to harness the computational power of quantum technologies while optimizing their performance through intelligent machine learning-driven design.
- *Scalable Quantum Computer Architectures:* Machine learning will be leveraged to design scalable and powerful quantum computer architectures. This future work envisions overcoming current limitations in scalability by integrating machine learning principles into the architectural design, unlocking new dimensions of computational prowess in quantum systems.
- *Quantum Error Correction and Fault Tolerance:* Machine learning techniques will be employed to revolutionize quantum error correction and fault tolerance mechanisms. By integrating adaptive machine learning models, the aim is to enhance the robustness and reliability of quan-

tum computations, paving the way for more stable and error-resilient quantum information processing.

- *Machine Learning-enhanced Quantum Cryptography:* Machine learning methodologies will be applied to quantum cryptography, aiming to devise innovative strategies for protecting data from a spectrum of attacks. This intersection of quantum principles and adaptive machine learning promises to create dynamic defense mechanisms, capable of evolving in response to emerging threats in real-time.

As these future endeavours are embarked upon, the integration of quantum technologies, artificial intelligence, and IoT security is poised to redefine the boundaries of secure data transfer, ushering in a new era of resilient and intelligent IoT ecosystems. The envisioned future works aim not only to address current challenges but also to anticipate and proactively mitigate the complexities that may arise in the dynamic landscape of IoT security and quantum computing.

References

Abd-El-Atty, B. (2022). Quaternion with quantum walks for designing a novel color image cryptosystem. *Journal of Information Security and Applications*, 71:103367.

Abd-El-Atty, B. (2023). A robust medical image steganography approach based on particle swarm optimization algorithm and quantum walks. *Neural Computing and Applications*, 35:773–785.

Abd-El-Atty, B., El-Latif, A. A. A., and Venegas-Andraca, S. E. (2019a). An encryption protocol for NEQR images based on one-particle quantum walks on a circle. *Quantum Information Processing*, 18(9):272.

Abd-El-Atty, B., ElAffendi, M., and El-Latif, A. A. A. (2022). A novel image cryptosystem using gray code, quantum walks, and henon map for cloud applications. *Complex & Intelligent Systems*.

Alanezi, A., Abd-El-Atty, B., Kolivand, H., and El-latif, A. A. A. (2021). Quantum based encryption approach for secure images *1st International Conference on Artificial Intelligence and Data Analytics (CAIDA)*, 176-181. IEEE.

Alanezi, A., El-latif, A. A. A., Kolivand, H., and Abd-El-Atty, B., (2023). Quantum based encryption approach for secure images *New Journal of Physics 25*, 12: 123041.

Abd-El-Atty, B., Iliyasu, A. M., Alanezi, A., and El-latif, A. A. A. (2021). Optical image encryption based on quantum walks. *Optics and Lasers in Engineering*, 138:106403.

Abd-El-Atty, B., Iliyasu, A. M., Alaskar, H., and El-Latif, A. A. A. (2020). A robust quasi-quantum walks-based steganography protocol for secure transmission of images on cloud-based e-healthcare platforms. *Sensors*, 20(11):3108.

Abd-El-Atty, B., Ugail, H., Mehmood, I., Amin, M., and El-Latif, A. A. A. (2019b). An efficient cryptosystem based on the logistic-chebyshev map. In *13th International Conference on Software, Knowledge, Information Management and Applications (SKIMA2019)*. IEEE.

Abd-El-Atty, B., Venegas-Andraca, S. E., and El-Latif, A. A. A. (2018). Quantum Information Protocols for Cryptography.

Abd El-Latif, A. A., Abd-El-Atty, B., Mehmood, I., Muhammad, K., Venegas-Andraca, S. E., and Peng, J. (2021). Quantum-inspired blockchain-based cybersecurity: Securing smart edge utilities in iot-based smart cities. *Information Processing & Management*, 58(4):102549.

Aharonov, D., Ambainis, A., Kempe, J., and Vazirani, U. (2001). Quantum walks on graphs. In *Proceedings of the thirty-third annual ACM symposium on Theory of computing*, pages 50–59. ACM.

Aharonov, Y., Davidovich, L., and Zagury, N. (1993). Quantum random walks. *Phys. Rev. A*, 48:1687–1690.

Ahmad, I., Rahman, T., Zeb, A., Khan, I., Ullah, I., Hamam, H., and Cheikhrouhou, O. (2021). Analysis of security attacks and taxonomy in underwater wireless sensor networks. *Wireless Communications and Mobile Computing*, 2021.

Ahmad, J. and Hwang, S. O. (2015). A secure image encryption scheme based on chaotic maps and affine transformation. *Multimedia Tools and Applications*, 75(21):13951–13976.

Akerele, M., Al-Anbagi, I., and Erol-Kantarci, M. (2019). A fiber-wireless sensor networks qos mechanism for smart grid applications. *IEEE Access*, 7:37601–37610.

Akhshani, A., Akhavan, A., Mobaraki, A., Lim, S.-C., and Hassan, Z. (2014). Pseudo random number generator based on quantum chaotic map. *Communications in Nonlinear Science and Numerical Simulation*, 19(1):101–111.

Al-Saedi, A. A., Boeva, V., Casalicchio, E., and Exner, P. (2022). Context-aware edge-based ai models for wireless sensor networksâ€"an overview. *Sensors*, 22(15):5544.

Alanezi, A., Abd-El-Atty, B., Kolivand, H., El-Latif, A., Ahmed, A., El-Rahiem, A., Sankar, S., S Khalifa, H., et al. (2021). Securing digital images through simple permutation-substitution mechanism in cloud-based smart city environment. *Security and Communication Networks*, 2021.

Ali, K. M. and Khan, M. (2019). Application based construction and optimization of substitution boxes over 2d mixed chaotic maps. *International Journal of Theoretical Physics*, 58(9):3091–3117.

Alturki, R., Alyamani, H. J., Ikram, M. A., Rahman, M. A., Alshehri, M. D., Khan, F., and Haleem, M. (2021). Sensor-cloud architecture: A taxonomy of security issues in cloud-assisted sensor networks. *IEEE Access*, 9:89344–89359.

Atzori, Luigi and Iera, Antonio and Morabito, Giacomo (2017). Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm. *Ad Hoc Networks*, 56:122-140.

Akpakwu, Godfrey Anuga and Silva, Bruno J and Hancke, Gerhard P and Abu-Mahfouz, Adnan M (2017). A survey on 5G networks for the Internet of Things: Communication technologies and challenges. *IEEE access*, 61:3619–3647.

Alvarez, G. and Li, S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems. *International Journal of Bifurcation and Chaos*, 16(8):2129–2151.

Amin, M. and EL-Latif, A. A. A. (2010). Efficient modified RC5 based on chaos adapted to image encryption. *Journal of Electronic Imaging*, 19(1):013012.

Anitha, S., Jayanthi, P., and Chandrasekaran, V. (2021). An intelligent based healthcare security monitoring schemes for detection of node replication attack in wireless sensor networks. *Measurement*, 167:108272.

Arul, R., Raja, G., Bashir, A. K., Chaudry, J., and Ali, A. (2018). A console grid leveraged authentication and key agreement mechanism for lte/sae. *IEEE Transactions on Industrial Informatics*, 14(6):2677–2689.

Askar, S., Karawia, A., Al-Khedhairi, A., and Al-Ammar, F. (2019). An algorithm of image encryption using logistic and two-dimensional chaotic economic maps. *Entropy*, 21(1):44.

Awan, I. A., Shiraz, M., Hashmi, M. U., Shaheen, Q., Akhtar, R., and Ditta, A. (2020). Secure framework enhancing AES algorithm in cloud computing. *Security and Communication Networks*, 2020:1–16.

Azoug, S. E. and Bouguezel, S. (2016). A non-linear preprocessing for opto-digital image encryption using multiple-parameter discrete fractional fourier transform. *Optics Communications*, 359:85–94.

Atzori, Luigi and Iera, Antonio and Morabito, Giacomo (2017). Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm. *Ad Hoc Networks*, 56:122-140.

Al-Qerem, Ahmad and Ali, Ali Mohd and Nashwan, Shadi and Alauthman, Mohammad and Hamarsheh, Ala and Nabot, Ahmad and Jibreen, Issam(2023). Transactional Services for Concurrent Mobile Agents over Edge/Cloud

Computing-Assisted Social Internet of Things. *ACM Journal of Data and Information Quality*, 15:1–20.

Baghezza, R., Bouchard, K., Bouzouane, A., and Gouin-Vallerand, C. (2021). From offline to real-time distributed activity recognition in wireless sensor networks for healthcare: A review. *Sensors*, 21(8):2786.

Belazi, A., El-Latif, A. A. A., Rhouma, R., and Belghith, S. (2015). Selective image encryption scheme based on DWT, AES s-box and chaotic permutation. In *2015 International Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE.

Bennett, C. and Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179.

Boyer, M., Gelles, R., Kenigsberg, D., and Mor, T. (2009). Semiquantum key distribution. *Phys. Rev.A*, 79:032341.

Boyer, M., Kenigsberg, D., and Mor, T. (2007). Quantum key distribution with classical Bob. *Phys. Rev. Lett.*, 99(14):140501.

Cabello, A. (2000). Quantum key distribution in the holevo limit. *Physical Review Letters*, 85(26):5635.

Carson, G. R., Loke, T., and Wang, J. B. (2015). Entanglement dynamics of two-particle quantum walks. *Quantum Information Processing*, 14(9):3193–3210.

Clemente-López, Daniel and Munoz-Pacheco, Jesus M and Rangel-Magdaleno, Jose de Jesus (2023). A review of the digital implementation of continuous-time fractional-order chaotic systems using FPGAs and embedded hardware. *Ad Hoc Networks*, 30:951–983.

Chai, X., Bi, J., Gan, Z., Liu, X., Zhang, Y., and Chen, Y. (2020a). Color image compression and encryption scheme based on compressive sensing and double random encryption strategy. *Signal Processing*, 176:107684.

Chai, X., Wu, H., Gan, Z., Zhang, Y., and Chen, Y. (2020b). Hiding cipher-images generated by 2-d compressive sensing with a multi-embedding strategy. *Signal Processing*, 171:107525.

Chen, H., Liu, Z., Zhu, L., Tanougast, C., and Blondel, W. (2019). Asymmetric color cryptosystem using chaotic ushiki map and equal modulus decomposition in fractional fourier transform domains. *Optics and Lasers in Engineering*, 112:7–15.

Childs, A. (2009). Universal computation by quantum walk. *Phys. Rev. Lett.*, 102:180501.

Dou, S., Shen, X., Zhou, B., Wang, L., and Lin, C. (2019). Experimental research on optical image encryption system based on joint fresnel transform correlator. *Optics & Laser Technology*, 112:56–64.

EL-Latif, A. A. A., Abd-El-Atty, B., Abou-Nassar, E. M., and Venegas-Andraca, S. E. (2020). Controlled alternate quantum walks based privacy preserving healthcare images in internet of things. *Optics & Laser Technology*, 124:105942.

El-Latif, A. A. A., Abd-El-Atty, B., Amin, M., and Iliyasu, A. M. (2020a). Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications. *Scientific Reports*, 10(1).

El-Latif, A. A. A., Abd-El-Atty, B., Amin, M., and Iliyasu, A. M. (2020b). Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications. *Scientific Reports*, 10(1):1–16.

El-Latif, A. A. A., Abd-El-Atty, B., Elseuofi, S., Khalifa, H. S., Alghamdi, A. S., Polat, K., and Amin, M. (2020c). Secret images transfer in cloud system based on investigating quantum walks in steganography approaches. *Physica A: Statistical Mechanics and its Applications*, 541:123687.

El-Latif, A. A. A., Abd-El-Atty, B., Mazurczyk, W., Fung, C., and Venegas-Andraca, S. E. (2020d). Secure data encryption based on quantum walks for 5g internet of things scenario. *IEEE Transactions on Network and Service Management*, 17(1):118–131.

El-Latif, A. A. A., Abd-El-Atty, B., Mazurczyk, W., Fung, C., and Venegas-Andraca, S. E. (2020e). Secure data encryption based on quantum walks for 5g internet of things scenario. *IEEE Transactions on Network and Service Management*.

EL-Latif, A. A. A., Abd-El-Atty, B., and Venegas-Andraca, S. E. (2019a). A novel image steganography technique based on quantum substitution boxes. *Optics & Laser Technology*, 116:92–102.

EL-Latif, A. A. A., Abd-El-Atty, B., and Venegas-Andraca, S. E. (2020a). Controlled alternate quantum walk-based pseudo-random number generator and its application to quantum color image encryption. *Physica A: Statistical Mechanics and its Applications*, 547:123869.

EL-Latif, A. A. A., Abd-El-Atty, B., and Venegas-Andraca, S. E. (2020b). Controlled alternate quantum walk-based pseudo-random number generator and its application to quantum color image encryption. *Physica A: Statistical Mechanics and its Applications*, page 123869.

El-Latif, A. A. A., Abd-El-Atty, B., Venegas-Andraca, S. E., Elwahsh, H., Piran, M. J., Bashir, A. K., Song, O.-Y., and Mazurczyk, W. (2020). Providing end-to-end security using quantum walks in IoT networks. *IEEE Access*, 8:92687–92696.

EL-Latif, A. A. A., Abd-El-Atty, B., Venegas-Andraca, S. E., and Mazurczyk, W. (2019b). Efficient quantum-based security protocols for information sharing and data protection in 5g networks. *Future Generation Computer Systems*, 100:893–906.

EL-Latif, A. A. A., Abd-El-Atty, B., Venegas-Andraca, S. E., and Mazurczyk, W. (2019c). Efficient quantum-based security protocols for information sharing and data protection in 5g networks. *Future Generation Computer Systems*, 100:893–906.

El-Latif, A. A. A., Li, L., and Niu, X. (2014). A new image encryption scheme based on cyclic elliptic curve and chaotic system. *Multimedia tools and applications*, 70(3):1559–1584.

Etem, Taha and Kaya, Turgay (2020). A novel true random bit generator design for image encryption. *Physica A: Statistical Mechanics and Its Applications*, 540: 122750.

Farah, M. B., Guesmi, R., Kachouri, A., and Samet, M. (2020). A novel chaos based optical image encryption using fractional fourier transform and DNA sequence operation. *Optics & Laser Technology*, 121:105777.

Feldman, E. and Hillery, M. (2007). Modifying quantum walks: a scattering theory approach. *J. Phys. A: Math. Theor.*, 40:11343–11359.

Francois, M., Grosges, T., Barchiesi, D., and Erra, R. (2013). A new pseudo-random number generator based on two chaotic maps. *Informatica*, 24(2):181–197.

François, M., Grosges, T., Barchiesi, D., and Erra, R. (2014). Pseudo-random number generator based on mixing of three chaotic maps. *Communications in Nonlinear Science and Numerical Simulation*, 19(4):887–895.

Iftikhar, Abeer and Qureshi, Kashif Naseer and Shiraz, Muhammad and Albahli, Saleh. (2023). Cascade chaotic system with applications. *Journal of King Saud University-Computer and Information Sciences*, 101788.

Gan, Z.-H., li Chai, X., jun Han, D., and ran Chen, Y. (2018). A chaotic image encryption algorithm based on 3-d bit-plane permutation. *Neural Computing and Applications*, 31(11):7111–7130.

Gu, Xiu and Allcock, Jonathan and An, Shuoming and Liu, Yu-xi (2021). Efficient multi-qubit subspace rotations via topological quantum walks. *arXiv preprint arXiv*, 2111.06534.

Gong, L.-H., He, X.-T., Cheng, S., Hua, T.-X., and Zhou, N.-R. (2016). Quantum image encryption algorithm based on quantum image XOR operations. *International Journal of Theoretical Physics*, 55(7):3234–3250.

Guan, D.-J., Wang, Y.-J., and Zhuang, E. (2014). A practical protocol for three-party authenticated quantum key distribution. *Quantum information processing*, 13(11):2355–2374.

Hu, H., Liu, L., and Ding, N. (2013). Pseudorandom sequence generator based on the chen chaotic system. *Computer Physics Communications*, 184(3):765–768.

Hua, Z., Zhou, Y., and Huang, H. (2019). Cosine-transform-based chaotic system for image encryption. *Information Sciences*, 480:403–419.

Hua, Z., Zhou, Y., Pun, C.-M., and Chen, C. P. (2015). 2d sine logistic modulation map for image encryption. *Information Sciences*, 297:80–94.

Huang, Q., Wang, L., and Yang, Y. (2017). Secure and privacy-preserving data sharing and collaboration in mobile healthcare social networks of smart cities. *Security and Communication Networks*, 2017:1–12.

Huang, W., Xu, B. J., Duan, J. T., Liu, B., Su, Q., He, Y. H., and Jia, H. Y. (2016). Authenticated Quantum Key Distribution with Collective Detection using Single Photons. *International Journal of Theoretical Physics*, 55(10):4238–4256.

Heidari, Arash and Jafari Navimipour, Nima and Unal, Mehmet and Zhang, Guodao (2023). Machine learning applications in internet-of-drones: systematic review, recent deployments, and open issues. *ACM Computing Surveys*, 55:1-45.

Kiktenko, E. O., Pozhar, N. O., Anufriev, M. N., Trushechkin, A. S., Yunusov, R. R., Kurochkin, Y. V., Lvovsky, A. I., and Fedorov, A. K. (2018). Quantum-secured blockchain. *Quantum Science and Technology*, 3(3):035004.

Konno, N., Mitsuhashi, H., and Sato, I. (2016). The discrete-time quaternionic quantum walk on a graph. *Quantum Information Processing*, 15(2):651–673.

Krawec, W. (2015). Mediated semiquantum key distribution. *Phys. Rev. A*, 91(3):032323.

Krawec, W. (2016). Security of a semi-quantum protocol where reflections contribute to the secret key. *Quantum Inf. Process.*, 15(5):2067–2090.

Kendon, Viv (2017). Decoherence in quantum walks–a review. *Mathematical structures in computer science*, 17:6:1169–1220.

Kumar, R. and Bhaduri, B. (2017). Optical image encryption using kronecker product and hybrid phase masks. *Optics & Laser Technology*, 95:51–55.

Kumar, Rohit and Agrawal, Neha (2023). Analysis of multi-dimensional Industrial IoT (IIoT) data in Edge-Fog-Cloud based architectural frameworks: A survey on current state and research challenges. *Journal of Industrial Information Integration*, 100504.

Li, C. M., Yu, K. F., Kao, S. H., and Hwang, T. (2016a). Authenticated semi-quantum key distributions without classical channel. *Quantum Information Processing*, 15(7):2881–2893.

Li, D., Yang, Y.-G., Bi, J.-L., Yuan, J.-B., and Xu, J. (2018a). Controlled alternate quantum walks based quantum hash function. *Scientific reports*, 8(1):225.

Li, D., Yang, Y. G., Bi, J. L., Yuan, J. B., and Xu, J. (2018b). Controlled Alternate Quantum Walks based Quantum Hash Function. *Scientific reports*, 8.

Li, D., Zhang, J., Guo, F. Z., Huang, W., Wen, Q. Y., and Chen, H. (2013a). Discrete-time interacting quantum walks and quantum Hash schemes. *Quantum Information Processing*, pages 1–13.

Li, D., Zhang, J., Guo, F. Z., Huang, W., Wen, Q. Y., and Chen, H. (2013b). Discrete-time interacting quantum walks and quantum Hash schemes. *Quantum information processing*, pages 1–13.

Li, L., Abd-El-Atty, B., El-Latif, A. A. A., and Ghoneim, A. (2017). Quantum color image encryption based on multiple discrete chaotic systems. In *Federated Conference on Computer Science and Information Systems (FedCSIS)*, pages 555–559. IEEE.

Li, L., Abd-El-Atty, B., Elseuofi, S., El-Rahiem, B. A., and El-Latif, A. A. A. (2019). Quaternion and multiple chaotic systems based pseudo-random number generator. In *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, pages 1–5. IEEE.

Li, Q., Chan, W. H., and Zhang, S. (2016b). Semiquantum key distribution with secure delegated quantum computation. *Scientific reports*, 6:19898.

Liang, H.-R., Tao, X.-Y., and Zhou, N.-R. (2016). Quantum image encryption based on generalized affine transform and logistic map. *Quantum Information Processing*, 15(7):2701–2724.

Liansheng, S., Cong, D., Xiao, Z., Ailing, T., and Anand, A. (2019). Double-image encryption based on interference and logistic map under the framework of double random phase encoding. *Optics and Lasers in Engineering*, 122:113–122.

Lin, J., Yang, C. W., Tsai, C. W., and Hwang, T. (2013a). Intercept-resend attacks on semi-quantum secret sharing and the improvements. *International Journal of Theoretical Physics*, 52(1):156–162.

Lin, S., Huang, C., and Liu, X. (2013b). Multi-user quantum key distribution based on Bell states with mutual authentication. *Phys. Scr.*, 87:035008.

Lindell, Y. and Katz, J. (2014). *Introduction to modern cryptography*. Chapman and Hall/CRC.

Liu, Z. R. and Hwang, T. (2018). Mediated Semi-Quantum Key Distribution Without Invoking Quantum Measurement. *Annalen der Physik*, 530(4):1700206.

Lovett, N. B., Cooper, S., Everitt, M., Trevers, M., and Kendon, V. (2010). Universal quantum computation using the discrete-time quantum walk. *Physical Review A*, 81(4):042330.

Lui, O.-Y., Yuen, C.-H., and Wong, K.-W. (2013). A pseudo-random number generator employing multiple renyi maps. *International Journal of Modern Physics C*, 24(11):1350079.

Luo, H., , and Xue, P. (2015). Properties of long quantum walks in one and two dimensions. *Quantum Information Processing*, 14(12):4361–4394.

Luo, Y.-P., Chou, W.-H., and Hwang, T. (2017). Comment on "a practical protocol for three-party authenticated quantum key distribution". *Quantum Information Processing*, 16(5):119.

Li, Li and Abd El-Latif, Ahmed A and Jafari, Sajad and Rajagopal, Karthikeyan and Nazarimehr, Fahimeh and Abd-El-Atty, Bassem. (2022) Multimedia cryptosystem for IoT applications based on a novel chaotic system around a predefined manifold *Sensors*, 22:334.

Ladd, Thaddeus D and Jelezko, Fedor and Laflamme, Raymond and Nakamura, Yasunobu and Monroe, Christopher and O'Brien, Jeremy Lloyd (2010). Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm. *nature*, 464:45–53.

Meslouhi, A. and Hassouni, Y. (2017). Cryptanalysis on authenticated semi-quantum key distribution protocol using Bell states. *Quantum Information Processing*, 16(1):18.

Muthu, Joan S and Murali, P (2021). Review of chaos detection techniques performed on chaotic maps and systems in image encryption. *SN Computer Science*, 2:1–24.

Nakano, K. and Suzuki, H. (2020). Analysis of singular phase based on double random phase encoding using phase retrieval algorithm. *Optics and Lasers in Engineering*, 134:106300.

Nayak, A. and Vishwanath, A. (2000). Quantum walk on the line. *quant-ph/0010117*.

Nair, Akarsh K and John, Chinju and Sahoo, Jayakrushna. (2022). Implementation of intelligent IoT. *In Book: AI and IoT for Sustainable Development in Emerging Countries: Challenges and Opportunities*, 27-50.

Özkaynak, F. and Yavuz, S. (2013). Security problems for a pseudorandom sequence generator based on the chen chaotic system. *Computer Physics Communications*, 184(9):2178–2181.

Patel, K. D. and Belani, S. (2011). Image encryption using different techniques: A review. *International Journal of Emerging Technology and Advanced Engineering*, 1(1):30–34.

Qin, W. and Peng, X. (2009). Vulnerability to known-plaintext attack of optical encryption schemes based on two fractional fourier transform order keys and double random phase keys. *Journal of Optics A: Pure and Applied Optics*, 11(7):075402.

Refregier, P. and Javidi, B. (1995). Optical image encryption based on input plane and fourier plane random encoding. *Optics Letters*, 20(7):767.

Shahzadi, S., Khaliq, B., Rizwan, M., and Ahmad, F. (2020). Security of cloud computing using adaptive neural fuzzy inference system. *Security and Communication Networks*, 2020:1–15.

Srinivas, Jangirala and Das, Ashok Kumar and Wazid, Mohammad and Kumar, Neeraj (2018). Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial Internet of Things. *IEEE Transactions on Dependable and Secure Computing*, 17:1133–1146.

Shukla, C., Thapliyal, K., and Pathak, A. (2017). Semi-quantum communication: protocols for key agreement, controlled secure direct communication and dialogue. *Quantum Information Processing*, 16(12):295.

SIPI (accessed on March 28, 2020). Sipi image database - misc.

Su, Y., Xu, W., and Zhao, J. (2020). Optical image encryption based on chaotic fingerprint phase mask and pattern-illuminated fourier ptychography. *Optics and Lasers in Engineering*, 128:106042.

Tan, R.-C., Lei, T., Zhao, Q.-M., Gong, L.-H., and Zhou, Z.-H. (2016). Quantum color image encryption algorithm based on a hyper-chaotic system and quantum fourier transform. *International Journal of Theoretical Physics*, 55(12):5368–5384.

Tregenna, B., Flanagan, W., Maile, R., and Kendon, V. (2003). Controlling discrete quantum walks: coins and initial states. *New Journal of Physics*, 5(1).

Tsafack, N., Kengne, J., Abd-El-Atty, B., Iliyasu, A. M., Hirota, K., and EL-Latif, A. A. A. (2020a). Design and implementation of a simple dynamical 4-d chaotic circuit with applications in image encryption. *Information Sciences*, 515:191–217.

Tsafack, N., Sankar, S., Abd-El-Atty, B., Kengne, J., C., J. K., Belazi, A., Mehmood, I., Bashir, A. K., Song, O.-Y., and El-Latif, A. A. A. (2020b). A new chaotic map with dynamic analysis and encryption application in internet of health things. *IEEE Access*, 8:137731–137744.

Venegas-Andraca, S. E. (2012a). Quantum walks: a comprehensive review. *Quantum Information Processing*, 11(5):1015–1106.

Venegas-Andraca, S. E. (2012b). Quantum walks: a comprehensive review. *Quantum Information Processing*, 11(5):1015–1106.

Vlassopoulos, N. and Girau, B. (2014). A metric for evolving 2-d cellular automata as pseudo-random number generators. *Journal of Cellular Automata*, 9.

Wang, J., Zhang, S., Zhang, Q., and Tang, C. (2011). Semiquantum key distribution using entangled states. *Chin. Phys. Lett.*, 28(10):100301.

Wang, X., Feng, L., and Zhao, H. (2019). Fast image encryption algorithm based on parallel computing system. *Information Sciences*, 486:340–358.

Wang, X.-Y., Zhang, Y.-Q., and Bao, X.-M. (2015). A novel chaotic image encryption scheme using DNA sequence operations. *Optics and Lasers in Engineering*, 73:53–61.

Waseem, H. M. and Khan, M. (2019). A new approach to digital content privacy using quantum spin and finite-state machine. *Applied Physics B*, 125(2).

Wayner, Peter (2009). Disappearing cryptography: information hiding: steganography and watermarking. *Ad Hoc Networks*.

Wong, T. G. (2016). Quantum walk on the line through potential barriers. *Quantum Information Processing*, 15(2):675–688.

Xian, Y. and Wang, X. (2021). Fractal sorting matrix and its application on chaotic image encryption. *Information Sciences*, 547:1154–1169.

Xin, X., Hua, X., Li, C., and Chen, D. (2016). Quantum Authentication of Classical Messages Using Non-orthogonal Qubits and Hash Function. International Journal of u-and e-Service. *Science and Technology*, 9(10):181–186.

Yan, T. and Li, D. (2021). A novel quantum color image encryption scheme based on controlled alternate quantum walks. In *Security, Privacy, and Anonymity in Computation, Communication, and Storage*, pages 519–530. Springer International Publishing.

Yang, C. W., Hwang, T., and Lin, T. H. (2013). Modification attack on QSDC with authentication and the improvement. *International Journal of Theoretical Physics*, 52(7):2230–2234.

Yang, Y., Zhang, Y., Xu, G., Chen, X., Zhou, Y. H., and Shi, W. (2018a). Improving the efficiency of quantum Hash function by dense coding of coin operators in discrete-time quantum walk. *SCIENCE CHINA Physics, Mechanics & Astronomy*, 61(3):030312.

Yang, Y. G., Bi, J. L., Chen, X. B., Yuan, Z., Zhou, Y. H., and Shi, W. M. (2018b). Simple hash function using discrete-time quantum walks. *Quantum Information Processing*, 17(8):189.

Yang, Y.-G., Pan, Q.-X., Sun, S.-J., and Xu, P. (2015). Novel image encryption based on quantum walks. *Scientific Reports*, 5(1).

Yang, Y.-G., Xu, P., Yang, R., Zhou, Y.-H., and Shi, W.-M. (2016a). Quantum hash function and its application to privacy amplification in quantum key distribution, pseudo-random number generation and image encryption. *Scientific Reports*, 6(1).

Yang, Y. G., Xu, P., Yang, R., Zhou, Y. H., and Shi, W. M. (2016b). Quantum Hash function and its application to privacy amplification in quantum key distribution, pseudo-random number generation and image encryption. *Scientific reports*, 6.

Yang, Y. G. and Zhao, Q. Q. (2016). Novel pseudo-random number generator based on quantum random walks. *Scientific reports*, 6.

Yan, Shaohui and Wang, Ertong and Wang, Qiyu (2023). Analysis and circuit implementation of a non-equilibrium fractional-order chaotic system with hidden multistability and special offset-boosting. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 33:3.

Yu, K., Yang, C., Liao, C., and Hwang, T. (2014). Authenticated semi-quantum key distribution protocol using bell states. *Quantum Inf. Process.*, 13(6):1457–1465.

Yuan, H., Liu, Y.-m., Pan, G.-z., Zhang, G., Zhou, J., and Zhang, Z.-j. (2014). Quantum identity authentication based on ping-pong technique without entanglements. *Quantum Inf Process*, 13:2535–2549.

Zeng, G. and Zhang, W. (2000). Identity verification in quantum key distribution. *Phys. Rev. A*, 61:022303.

Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., and Shen, X. S. (2017). Security and privacy in smart city applications: Challenges and solutions. *IEEE Communications Magazine*, 55(1):122–129.

Zhang, T. J., Manhrawy, I., Abdo, A., El-Latif, A. A., and Rhouma, R. (2014). Cryptanalysis of elementary cellular automata based image encryption. *Advanced Materials Research*, 981:372–375.

Zhang, W., Qiu, D., and Mateus, P. (2018). Security of a single-state semi-quantum key distribution protocol. *Quantum Information Processing*, 17:1–21.

Zhang, X., Gong, W., and Tan, Y. (2009). Quantum key distribution series network protocolwith m-classical bobs. *Chin. Phys. B*, 18(6):2143.

Zhou, N., Hu, Y., Gong, L., and Li, G. (2017). Quantum image encryption scheme with iterative generalized Arnold transforms and quantum image cycle shift operations. *Quantum Information Processing*, 10.

Zhou, Y., Bao, L., and Chen, C. P. (2014a). A new 1d chaotic system for image encryption. *Signal Processing*, 97:172–182.

Zhou, Y., Hua, Z., Pun, C.-M., and Chen, C. P. (2014b). Cascade chaotic system with applications. *IEEE transactions on cybernetics*, 45(9):2001–2012.

Zhu, K.-N., Zhou, N.-R., Wang, Y.-Q., and Wen, X.-J. (2018). Semi-quantum key distribution protocols with ghz states. *International Journal of Theoretical Physics*.

Zou, X., Qiu, D., Li, L., Wu, L., and Li, L. (2009). Semiquantum-key distribution using less than four quantum states. *Phys. Rev. A*, 79:052312.

Zhang, Wenfang and Jiao, Heng and Yan, Zhuoqun and Wang, Xiaomin and Khan, Muhammad Khurram (2023). Security analysis and improvement of a public auditing scheme for secure data storage in fog-to-cloud computing. *Computers & Security*, 125:103019.