A Survey on Quantum-Cryptographic Image Encryption for Secure Storage

Mr. R Suresh[1], Charumathi K[2], Pooja S[3], Thenmalar S[4]
[1,2,3,4]*Department of Information Technology, Sri Manakula Vinayagar Engineering College, Madagadipet, Puducherry 605107, India*
Email: sureshramanujam@smvec.ac.in[1], charumathiit@smvec.ac.in[2] , poojait@smvec.ac.in[3], thenmalarit@smvec.ac.in[4]

Abstract — The aim of this paper is to explore and implement cutting-edge quantum cryptographic techniques to enhance the security of image data storage. Leveraging principles from quantum computing and cryptography, the project seeks to develop an advanced image encryption system that ensures unprecedented levels of security. By harnessing the unique properties of quantum mechanics, such as superposition and entanglement, the proposed system will establish a robust foundation for encrypting images, surpassing the limitations of classical cryptographic methods. The utilization of quantum key distribution protocols will add an additional layer of security, making it virtually impossible for adversaries to intercept or compromise sensitive image data during storage. This endeavor not only addresses the escalating cybersecurity concerns surrounding image storage but also contributes to the advancement of quantum technologies in practical applications. The project envisions a novel paradigm in image encryption, fostering a secure environment for sensitive visual information across various domains, including healthcare, finance, and defense.

Keywords—Quantum Mechanics, Quantum Computing, cryptography, secure.

I. INTRODUCTION

1.1 Quantum Computing

Quantum computing, rooted in quantum mechanics, uses qubits with superposition and entanglement properties. Quantum algorithms, like Shor's and Grover's, exploit qubits for exponentially faster problem-solving, impacting cryptography and optimization. Quantum supremacy, exemplified by Google in 2019, signifies when a quantum computer surpasses classical supercomputers in specific tasks, marking a crucial milestone in practical quantum computing development.

1.2 Applications Across Fields:

Quantum computing presents a dual impact on cryptography, with Shor's algorithm threatening traditional protocols like RSA while quantum key distribution (QKD) promises ultra-secure communication via quantum mechanics principles. In optimization, quantum computing excels in logistics, finance, and operations research. For drug discovery and material science, it simulates molecular interactions precisely. Quantum machine learning holds potential for enhancing AI tasks, and in finance, it efficiently handles modeling and risk analysis. Quantum computing benefits climate modeling, supply chain optimization, and quantum sensing applications. Quantum communication ensures secure data transmission, and in space exploration, it aids trajectory optimization and complex problem-solving. The energy sector can leverage quantum computing for efficient production and exploration of new materials. Incorporating quantum cryptography safeguards against potential vulnerabilities, ensuring secure communication in the quantum computing era.

1.3 Cryptography

Cryptography, a cornerstone of information security, involves the design and implementation of techniques to secure communication and protect sensitive data from unauthorized access. In essence, it is the science and art of encoding information to render it unreadable without the appropriate decryption key. Cryptographic methods are employed in various applications, from securing online transactions and communication to safeguarding national security secrets. The field encompasses both classical techniques, like the venerable Caesar cipher, and advanced algorithms such as the RSA and AES, which rely on complex mathematical principles. Public-key cryptography, a significant advancement, utilizes pairs of keys—one public and one private—for secure communication between parties who may not share a prior secret. As our digital landscape evolves, cryptography plays an increasingly vital role in ensuring the confidentiality, integrity, and authenticity of information, making it an indispensable tool in the realm of cybersecurity.

1.4 Quantum Cryptography: Enhancing Security Through Quantum Mechanics

Quantum cryptography, or quantum key distribution (QKD), revolutionizes secure communication by applying quantum mechanics principles to address vulnerabilities in classical cryptographic systems, particularly in key exchange. Exploiting superposition and entanglement, QKD involves protocols such as the BBM92, named after its inventors Bennett, Brassard, Mermin, and others. In this protocol, Alice sends quantum bits (qubits) to Bob through a quantum channel, like a fiber-optic cable, encoding them using methods like polarized photons. Bob measures the qubits, with the basis communicated later over a classical channel, ensuring the entangled nature of qubits detects eavesdropping attempts. Error detection and key extraction follow if the error rate is low. Security features include the Heisenberg Uncertainty Principle and the No-Cloning Theorem, providing built-in mechanisms for detecting eavesdropping. Practical implementations involve photonic QKD systems using single photons and quantum key distribution networks demonstrating secure communication over longer distances.

Challenges and Advancements: Distance limitations in quantum communication arise from signal attenuation in optical fibers, constraining secure key exchange distances. Quantum repeaters, under development, aim to extend communication range by addressing signal loss and decoherence. Progress in quantum hardware, including robust quantum key distribution technology, plays a crucial role in overcoming practical implementation challenges.

Quantum Cryptography in the Future: Post-Quantum Cryptography addresses the threat posed by quantum computers to traditional cryptographic systems, relying on quantum mechanics for security. Integration with classical cryptographic protocols is envisioned for future applications, creating hybrid systems that leverage the strengths of both approaches.

Quantum Cryptography Applications: Quantum cryptography ensures secure communication by preserving the confidentiality and integrity of transmitted information. Its application in financial transactions enhances security against quantum threats, safeguarding sensitive data. Government and defense agencies are particularly interested in its use for highly secure communication channels. In healthcare, quantum cryptography provides a robust solution to protect patient data and medical records in the era of secure digital communication.

Ethical and Regulatory Considerations: Standardization efforts for quantum cryptography are advancing globally to ensure interoperability and security across diverse implementations. Regulatory bodies are addressing the implications of quantum technologies on communication security, developing frameworks that consider ethical and legal considerations. As quantum key distribution evolves in practical applications, it has the potential to reshape secure communication, offering unprecedented security levels against classical and quantum threats in the quantum era.

II. LITERATURE SURVEY

A Hybrid Cryptography Approach Using Symmetric, Asymmetric and DNA Based Encryption

The paper encompasses a multifaceted strategy that combines various cryptographic techniques to bolster the security of data.**[1]** This hybrid approach integrates symmetric encryption, leveraging a single key for both encryption and decryption to efficiently process large volumes of data. Additionally, asymmetric encryption introduces an extra layer of security by utilizing a pair of public and private keys. The innovative inclusion of DNA-based encryption adds a bio-inspired element, capitalizing on the unique properties of DNA molecules for encoding and decoding information. By amalgamating these diverse encryption methods, the hybrid cryptography approach aims to synergistically enhance overall security, capitalizing on the efficiency of symmetric encryption, the robustness of asymmetric encryption, and the unique features of DNA-based encryption. This comprehensive strategy is designed to provide a high level of data security suitable for various applications.

Proposed Security Enhancement Conceptual Models Using Quantum Key Distribution for Future Cryptography

In this paper, the focus is on introducing conceptual models for enhancing security through the utilization of Quantum Key Distribution (QKD) in the realm of future cryptography**.[2]** The primary objective is to address the evolving challenges in information security by leveraging the principles of quantum mechanics. The procedure involves the conceptualization of novel security enhancement models that employ QKD, a quantum communication method that utilizes quantum properties to secure communication channels. Quantum Key Distribution, as a fundamental concept in quantum cryptography, enables the distribution of cryptographic keys with a level of security that is theoretically unbreakable. By integrating QKD into the proposed conceptual models, the paper aims to contribute to the development of advanced cryptographic frameworks capable of withstanding emerging threats. The exploration of these models signifies a forward-looking approach in cryptography, anticipating the need for heightened security measures in the face of evolving technologies and potential quantum computing advancements. This research underscores the significance of quantum-based approaches in fortifying the foundations of future cryptographic systems, ensuring resilience against potential threats to data confidentiality and integrity.

Secure File Sharing System Using Image Steganography and Cryptography Techniques

In this paper, the focus is on presenting a secure file sharing system that leverages the combined strengths of image steganography and cryptography techniques **[3]**. The primary objective is to enhance the security of file sharing processes by integrating two robust methods. The procedure involves the development of a system that employs image steganography to conceal sensitive information within images, adding an additional layer of covert protection. Simultaneously, cryptography techniques are utilized to encrypt the files, ensuring that even if unauthorized access occurs, the content remains unintelligible without the appropriate decryption key. The synergy between image steganography and cryptography in the proposed system addresses the multifaceted aspects of secure file sharing, providing a comprehensive approach to safeguarding data during transmission and storage. This research signifies a concerted effort to fortify file-sharing systems against potential security breaches, emphasizing the importance of combining these techniques to create a robust and versatile security framework.

Design and Analysis of Octa-phase Shift Keying Based Quantum Key Distribution System

In this paper, the emphasis is on the design and analysis of a Quantum Key Distribution (QKD) system employing Octa-phase Shift Keying. The primary objective is to investigate the application of Octa-phase Shift Keying in the context of QKD, exploring its potential to enhance quantum communication systems.**[4]** The procedure involves the systematic design and thorough analysis of the proposed QKD system, with Octa-phase Shift Keying serving as a pivotal modulation scheme. This method holds promise for improving the security and efficiency of quantum key distribution protocols. The research underscores the significance of leveraging advanced modulation techniques within quantum communication, contributing to the ongoing development of secure and reliable quantum key distribution

systems. The analysis within this paper aims to provide insights into the performance and viability of Octa-phase Shift Keying in the quantum realm, offering valuable considerations for the advancement of quantum communication technologies.

Area-Efficient Intellectual Property (IP) Design of Advanced Encryption Standard

In this paper, the primary focus lies in the exploration of an area-efficient Intellectual Property (IP) design for the Advanced Encryption Standard (AES). The overarching objective is to address the demand for optimized and space-conscious implementations of AES cryptographic algorithms**. [5]** The procedure involves the meticulous design and analysis of an IP that adheres to the AES standard while prioritizing area efficiency. This research aims to contribute to the field of cryptographic hardware design by providing a solution that balances robust security measures with resource optimization. The significance of this work is underscored by the growing need for compact and efficient cryptographic implementations in various computing and communication systems. The paper delves into the intricacies of designing an IP for AES, emphasizing the importance of achieving a balance between functionality and resource utilization. Through this exploration, the research aims to advance the state-of-the-art in intellectual property design, offering a valuable contribution to the broader landscape of secure hardware implementations.

Lightweight Biomedical Image Encryption Approach

In this paper, the primary focus centers on the development and exploration of a lightweight biomedical image encryption approach**.[6]** The central objective is to address the specific requirements and challenges associated with securing biomedical images through an encryption method that prioritizes efficiency and reduced computational overhead. The procedure involves the careful design and analysis of an encryption approach tailored to the unique characteristics of biomedical images, aiming to strike a balance between security and computational lightweight. This research endeavors to contribute to the field of biomedical image security by providing an approach that is not only robust but also resource-efficient, making it well-suited for real-world biomedical applications. The paper underscores the significance of creating encryption techniques tailored to the demands of biomedical imaging, acknowledging the need for lightweight solutions that ensure secure transmission and storage of sensitive medical data. Through this exploration, the research seeks to advance the state-of-the-art in secure biomedical image processing, offering a valuable contribution to the intersection of medical imaging and information security.

Double Medical Image Cryptosystem Based on Quantum Walk

In this paper, the primary focus is on the development and exploration of a double medical image cryptosystem based on quantum walk.**[7]** The central objective is to address the challenges associated with securing medical images through an innovative cryptographic approach grounded in quantum walk principles. The procedure involves the meticulous design and analysis of a cryptosystem that leverages quantum walk for enhanced security in medical image encryption. This research aims to contribute to the field of medical image security by providing a dual-layered cryptographic solution that incorporates the inherent advantages of quantum walk principles. The paper underscores the significance of this novel approach in strengthening the security measures for medical image transmission and storage, acknowledging the critical importance of safeguarding sensitive healthcare data. Through this exploration, the research seeks to advance the state-of-the-art in secure medical image processing, offering a valuable contribution to the intersection of quantum computing and medical imaging security.

An Integrated Image Encryption Scheme Based on Elliptic Curve

In this paper, the central focus is on the development and exploration of an integrated image encryption scheme based on elliptic curve cryptography. **[8]** The primary objective is to address the need for secure image communication through a comprehensive cryptographic approach grounded in the principles of elliptic curve cryptography. The procedure involves the systematic design and analysis of an encryption scheme that leverages elliptic curve techniques, providing a robust and integrated solution for image security. This research aims to contribute to the field of image

encryption by offering a comprehensive and efficient cryptographic framework that aligns with the strengths of elliptic curve cryptography. The paper underscores the significance of this integrated approach in enhancing the security measures for image transmission and storage, acknowledging the critical importance of safeguarding visual data. Through this exploration, the research seeks to advance the state-of-the-art in secure image processing, offering a valuable contribution to the broader landscape of visual information security.

A Remote Security Computational Ghost Imaging Method Based on Quantum Key Distribution Technology

In this paper, the central focus is on the development and exploration of a remote security computational ghost imaging method based on quantum key distribution (QKD) technology. The primary objective is to address the challenges associated with secure remote imaging through an innovative computational ghost imaging approach grounded in the principles of quantum key distribution**.[9]** The procedure involves the meticulous design and analysis of a method that integrates computational ghost imaging with QKD, providing a robust and secure solution for remote imaging applications. This research aims to contribute to the field of secure remote imaging by offering a comprehensive and quantum-inspired framework that aligns with the strengths of QKD. The paper underscores the significance of this integrated approach in enhancing the security measures for remote imaging, acknowledging the critical importance of safeguarding visual data in remote communication scenarios. Through this exploration, the research seeks to advance the state-of-the-art in secure remote imaging, offering a valuable contribution to the broader landscape of quantum-enhanced visual information security.

A Survey of Important Issues in Quantum Computing and Communications

In this survey paper, the central focus is on providing an overview and analysis of important issues in the domains of quantum computing and quantum communications. The primary objective is to comprehensively explore and discuss key challenges, advancements, and considerations within these rapidly evolving fields.**[10]** The procedure involves a systematic examination of critical issues that encompass both quantum computing and quantum communications, shedding light on the current state of research, emerging trends, and potential future directions. This survey aims to contribute to the broader understanding of the challenges and opportunities in quantum information science, acknowledging the significance of addressing these issues for the advancement of quantum technologies. The paper underscores the importance of surveying the landscape of quantum computing and communications to facilitate a comprehensive understanding of the current research landscape and guide future endeavors in these transformative fields. Through this exploration, the research seeks to provide a valuable resource for researchers, practitioners, and enthusiasts interested in the intricate and dynamic realms of quantum information science.

III. CONCLUSION

These papers give us a brief idea about Quantum Computing and its limitations in the various fields and gave us a brief knowledge about the Cryptography and QKD(Quantum Key Distribution) and gave us idea of combining these two technologies to make a hybrid system for secure image storage

IV.REFERENCES

[1] Vikas Yadav; Manoj Kumar "A Hybrid Cryptography Approach Using Symmetric, Asymmetric and DNA Based Encryption" (IEEE Xplore Issue :27 March, 2023)

[2] Phone Naing; Kyaw Zin Oo; Mie Mie Su Thwin "Proposed Security Enhancement Conceptual Models Using Quantum Key Distribution for Future Cryptography" (IEEE Xplore Issue: 19 July, 2023)

[3] U A Solomon Raj; C P. Maheswaran "Secure File Sharing System Using Image Steganography and Cryptography Techniques" (IEEE Xplore Issue: 1 June, 2023)

[4] Ragini Verma; Anshul Jaiswal; Anh T. Pham "Design and Analysis of Octa-phase Shift Keying Based Quantum Key Distribution System" (IEEE Xplore Issue: 15 Aug, 2023)

[5] Useok Lee; Ho Keun Kim; Jeahack Lee; Myung Hoon Sunwoo "Area-Efficient Intellectual Property (IP) Design of Advanced Encryption Standard" (IEEE Xplore Issue: 11 July, 2023)

[6] Manjit Kaur; Ahmad Ali AlZubi; Dilbag Singh; Vijay Kumar; Heung-No Lee "Lightweight Biomedical Image Encryption Approach" (IEEE Xplore Issue:12 July, 2023)

[7] Bassem Abd-El-Atty; Mohammed A. El-Affendi; Samia Allaoua Chelloug "Double Medical Image Cryptosystem Based on Quantum Walk" (IEEE Xplore Issue:27 June, 2023)

[8] Ijaz Khalid; Tariq Shah; Sayed M. Eldin; Dawood Shah; Muhammad Asif; Imran Saddique "An Integrated Image Encryption Scheme Based on Elliptic Curve" (IEEE Xplore Issue:16 Dec, 2022)

[9] Jianan Wu; Yun Chen; Cheng Zhou; Zhongyang Chen; Chengqian Xu; Lijun Song "A Remote Security Computational Ghost Imaging Method Based on Quantum Key Distribution Technology" (IEEE Xplore Issue:18 Jan, 2022)

[10] Zebo Yang; Maede Zolanvari; Raj Jain "A Survey of Important Issues in Quantum Computing and Communications" (IEEE Xplore Issue:8 March,, 2022)

[11] Siyao; Yu Lu; Xiangguang Xiong "Reversible Data Hiding Algorithm in Encrypted Domain Based on Image Interpolation" (IEEE Xplore Issue:2 Oct, 2023)

[12] Bishoy K. Sharobim; Marwan A. Fetteha; Salwa K. Abd-El-Hafiz; Wafaa S. Sayed "An Efficient Multi-Secret Image Sharing System Based on Chinese Remainder Theorem and Its FPGA Realization"(IEEE Xplore Issue:27 Jan, 2023)

[13] Mingji Yu; Heng Yao; Chuan Qin; Xinpeng Zhang "Reversible Data Hiding in Palette Images" (IEEE Xplore Issue:16 Sep, 2022)

[14] Xi Ye; Yushu Zhang; Xiangli Xiao; Shuang Yi; Rushi Lan "Usability Enhanced Thumbnail-Preserving Encryption Based on Data Hiding for JPEG Images" (IEEE Xplore Issue:29 Jun, 2023)

[15] Chunqiang Yu; Xianquan Zhang; Chuan Qin; Zhenjun Tang "Reversible Data Hiding in Encrypted Images With Secret Sharing and Hybrid Coding" (IEEE Xplore Issue:27 April, 2023)

[16] Tianshuo Zhang; Yiqun Ma "Stable Image Encryption Algorithm Based on Expanded One-Dimensional Chaotic Jumping and Parallel Encoding Operation Grouping" (IEEE Xplore Issue:6 Sep, 2023)

[17] Yuejing Yan; Yanyan Xu; Zhiheng Wang; Xue Ouyang; Bo Zhang; Zheheng Rao "Privacy-Preserving Multi-Source Image Retrieval in Edge Computing" (IEEE Xplore Issue:25 Nov, 2022)

[18] Zahra Boreiri; Alireza Norouzi Azad; Nayereh Majd "Optimized Quantum Circuits in Quantum Image Processing Using Qiskit" (IEEE Xplore Issue:22Mar, 2022)

[19] Haisheng Li; Qingxin Zhu; Rigui Zhou; Yonghua Pu; Lan Song "Image storage, retrieval and compression in entangled quantum systems" (IEEE Xplore Issue:04 Dec, 2022)

[20] Zheng Xing; Xiaochen Yuan; Chan-Tong Lam "A Quantum Watermarking Scheme Using New Enhanced Quantum Image Representation" (IEEE Xplore Issue:29 Oct, 2023)