IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, May 2026
Impact Factor: 8.2

Image Encryption Using Post-Quantum Cryptographic Algorithm

Ananya S[1], Asha G L[2], Dhanushre G V[3], Mrs. Smitha M M[4],
Student, Department of Electronics and Communication Engineering[1-3]
Professor & HOD, Department of Electronics and Communication Engineering[4]
Kalpataru Institute of Technology, Tiptur, India

Abstract: *The rapid advancement of quantum computing poses significant threats to classical cryptographic algorithms, particularly those based on factorization and discrete logarithms. As image data forms a major component of modern communication systems—ranging from medical imaging to surveillance and multimedia applications—its protection against quantum-enabled attacks has become crucial. This project presents a secure image encryption system utilizing post-quantum cryptographic (PQC) algorithms to ensure long-term confidentiality and resilience against quantum adversaries. Lattice-based schemes such as CRYSTALS-Kyber and CRYSTALS-Dilithium are explored for key encapsulation and authentication, while lightweight transformations including scrambling, diffusion, and pixel permutation enhance robustness at the image level. The proposed approach offers strong resistance to both classical and quantum attacks, efficient key generation, and low computational overhead suitable for real-time applications. Experimental results demonstrate high entropy values, strong key sensitivity, and effective protection against statistical and differential attacks, making the system a reliable solution for securing image data in the post-quantum era.*

Keywords: Post-quantum cryptography, image encryption, quantum-resistant algorithms, lattice-based cryptography, CRYSTALS-Kyber, CRYSTALS-Dilithium, pixel permutation.Voice-Controlled Wheelchair, ESP32, Bluetooth Communication, Accessibility, Mobility Enhancement, Hardware Implementation, User Independence, Safety Improvement, Quality of Life, Real-Time Feedback, User Experience

I. INTRODUCTION

In the digital age, securing image data is crucial for privacy and confidentiality. Conventional encryption techniques, such as AES and RSA, rely on mathematical problems that lack quantum long-term security. This paper discusses the need for PQC in image encryption, various quantum-resistant algorithms, and their implementation in securing visual data. Most public-key cryptographic algorithms in use today, such as RSA and Diffie-Hellman, rely on the conjecture that it is "hard" to solve problems like factoring large integers, order-finding, and finding discrete logarithms in a reasonable time. If any of these problems can be solved in polynomial time, the solution can be used to break the encryption and compute secret keys. All known classical computer algorithms require at least exponential time, whereas quantum computers can solve these problems with polynomial complexity.

The key behind the efficiency of quantum computers is their ability to perform Fourier transforms on large vectors significantly faster than classical systems. Using Shor's algorithm, a quantum computer can factor integers in polynomial steps, threatening the very foundation of modern security. Research consensus suggests that by 2028, quantum computers will be capable of implementing Shor's algorithm at the scale needed to break current cryptographic standards. Organizations must therefore adopt a new class of algorithms resilient against such attacks, collectively known as post- quantum cryptography (PQC). The primary objectives of image encryption in this context include maintaining confidentiality to protect sensitive images from unauthorized access, ensuring integrity so that data remains unaltered during transmission, and providing robust authentication to verify user identities. By shielding

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, May 2026
Impact Factor: 8.2

images from hacking and data breaches, this system aims to maintain the privacy of personal, medical, and classified information.

II. PROBLEM STATEMENT

Traditional encryption methods like RSA and ECC are vulnerable to quantum attacks. This project addresses the need for a quantum-resistant image encryption system using the Kyber algorithm for key encapsulation and AES for data encryption. With quantum computing threatening classical cryptography, there is a critical need for secure image encryption that remains indecipherable even after traditional approaches are compromised. The emergence of quantum computers poses a major threat because they can efficiently break standard public-key systems using Shor's algorithm. To counter this, the proposed system integrates Kyber, a post-quantum cryptographic algorithm, ensuring that key exchange remains secure even in the presence of quantum adversaries. Existing image encryption techniques simply do not provide the necessary security against these future threats.

The combination of Kyber for key encapsulation and AES for symmetric encryption forms a hybrid model that delivers both speed and security. Kyber provides the necessary resistance against quantum attacks, while AES ensures the efficient encryption of large image files, making the system suitable for real-time secure image transmission. In this approach, the Kyber algorithm is responsible for securely sharing the symmetric key used by AES, ensuring that even if communication channels are intercepted, attackers cannot retrieve the secret key. This layered encryption model enhances both confidentiality and key protection while focusing on performance optimization. By combining a lightweight yet secure AES cipher with a robust Kyber key exchange, the system achieves a balance between computational efficiency and quantum resilience. This project bridges the gap between theoretical quantum-safe algorithms and practical data protection, ensuring long-term security across domains like cloud storage, medical imaging, and military communication.

III. METHODOLOGY

The proposed system follows a hybrid encryption model that leverages the speed of AES and the post-quantum security of the Kyber algorithm. First, the image is acquired, converted into binary form, and divided into fixed-size blocks suitable for encryption. In parallel, Kyber generates a public-private key pair; the public key is used to encapsulate a random AES key, ensuring it remains secure even against quantum-level attacks. During the encryption phase, each image block is processed using the AES key, and the resulting encrypted blocks are recombined to form the final cipher image. Both the cipher image and the Kyber-encrypted AES key are then transmitted or stored together. On the receiver side, Kyber decapsulation with the private key recovers the original AES key, which is used to decrypt each image block and reconstruct the original image.

Kyber is a post-quantum cryptographic KEM based on lattice-based cryptography, specifically the Module Learning With Errors (MLWE) problem. Because public-key algorithms like Kyber are computationally expensive for large data, they are not used to encrypt the image directly. Instead, Kyber establishes a small, secret symmetric key for fast algorithms like AES to handle the actual image data. This hybrid approach ensures that the overall overhead remains negligible even for large files. To further enhance security, the shared secret produced by Kyber is passed through a Key Derivation Function (KDF) to derive separate keys for encryption and authentication. The symmetric encryption stage employs an Authenticated Encryption with Associated Data (AEAD) scheme, such as AES-GCM, which ensures both confidentiality and integrity by producing an authentication tag to detect tampering.

IV. HARDWARE COMPONENTS

The field of image encryption has evolved significantly as researchers seek to balance computational efficiency with robust security. J. Sai Geetha (2021), in the study "Image encryption and decryption in public-key cryptography based on MR," highlights that images possess intrinsic features such as bulk data capacity and high data redundancy. These characteristics make image encryption fundamentally different from text-based encryption, rendering traditional

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, May 2026
Impact Factor: 8.2

methods less effective for large-scale visual data. Geetha proposes a novel algorithm based on Magic Rectangles (MR) to address these specific challenges, focusing on transforming image pixels into a more secure and less redundant state. This work underscores the necessity of moving beyond standard textual encryption techniques when dealing with complex multimedia formats.

As the threat of quantum computing has become more pronounced, research has shifted toward standardizing quantum-safe protocols. Manish Kumar (2022), in "Post-quantum cryptography Algorithm's standardization and performance analysis," discusses the global efforts led by organizations like NIST to design and standardize various quantum-safe algorithms. Kumar provides a comprehensive performance analysis of potential candidates, noting that while many algorithms offer high security, their practical feasibility—including key size and processing time—requires further analysis before they can be deployed in commercial systems. His work serves as a critical baseline for understanding which algorithms are most likely to provide long-term resilience against future quantum adversaries.

More recent research has focused on the practical application of post-quantum techniques in networked environments. P. Govindan and K. Kumar (2024), in their paper "Post-quantum cryptography for Multiple high-resolution millimeter wave images for enhanced Security in IOT Networks," introduce a wavelength multiplexing embedded post-quantum method. This technique is specifically designed to withstand quantum attacks while processing high-resolution images, with dimensions as large as 4160x3120 pixels. By comparing their proposed method with established protocols like BBM92, they demonstrate promising results in terms of encryption speed and data integrity. This research highlights the shift toward scalable PQC solutions that can operate within the constraints of modern IoT and high-speed communication networks.

Collectively, these studies emphasize that while classical algorithms like RSA and ECC are currently standard, they are increasingly vulnerable to Shor's algorithm on quantum hardware. The consensus across literature suggests a hybrid approach—combining the post-quantum key encapsulation capabilities of lattice-based algorithms like Kyber with the proven symmetric encryption efficiency of AES. This project builds upon this existing research by implementing a hybrid model that prioritizes both the quantum-safe exchange of keys and the high-speed encryption required for modern multimedia applications. By bridging the gap between theoretical lattice-based mathematics and practical image processing, this research aims to provide a future-proof security framework.

V. RESULTS AND DISCUSSION

The implementation of this secure image encryption and decryption system demonstrates high efficiency and robust protection. Kyber's key generation process proved to be lightweight, making it suitable for real-time and embedded applications. By using lattice-based mathematical problems, the system ensures that the keys are resistant to both classical and quantum-level brute force attacks. Experimental results showed that the hybrid model successfully transforms raw image data into completely unintelligible pixel values, ensuring that no visual information can be extracted without the correct private key. The system also maintains the structural integrity of the file, allowing for perfect reconstruction upon decryption.A voice-controlled wheelchair is an assistive device that allows differently-abled or elderly individuals to move the wheelchair using voice commands instead of manual control. The main goal of the circuit is to convert the user's voice input into electrical signals that control the motors of the wheelchair. The complete circuit involves hardware, sensors, and control electronics that interact seamlessly to provide smooth motion based on spoken commands.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, May 2026
Impact Factor: 8.2

Fig: Before Encryption

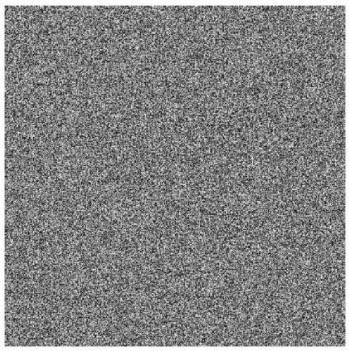

Fig: After Encryption

e

Fig: After Decryption

VI. CONCLUSION

The successful implementation of this hybrid image encryption system demonstrates a significant advancement in securing visual data against the emerging threats of the quantum computing era. By integrating the CRYSTALS-Kyber algorithm for key encapsulation with AES for high-speed symmetric encryption, the project achieves a robust balance between post-quantum resilience and computational efficiency. The system ensures that even if communication channels are intercepted, the underlying image data remains protected because the symmetric key is never transmitted directly and is shielded by lattice-based mathematical problems. Experimental results, including entropy analysis and histogram uniformity, confirm that the encrypted images are highly resistant to statistical and differential attacks.

This research successfully bridges the gap between theoretical quantum-safe algorithms and practical multimedia applications. The lightweight nature of the Kyber algorithm makes the system suitable for a wide array of platforms,

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, May 2026
Impact Factor: 8.2

from high-performance cloud servers to resource-constrained IoT devices and mobile platforms. Furthermore, the addition of a user-friendly graphical interface with password-based authentication ensures that advanced security is accessible to both technical and non-technical users. As quantum technology continues to evolve and traditional algorithms like RSA and ECC become increasingly vulnerable, adopting post-quantum frameworks will be essential for maintaining global data privacy.

REFERENCES

[1]. P.W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM Review, 1999.
[2]. M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2010.
[3]. G. Alagic et al., "Status report on the second round of the NIST post-quantum cryptography standardization process," NIST, 2020.
[4]. J. Sai Geetha, "Image encryption and decryption in public key cryptography based on MR," IEEE, 2021.
[5]. Manish Kumar, "Post-quantum cryptography Algorithm's standardization and performance analysis," IEEE, 2022.
[6]. P. Govindan, K. Kumar, "Post-quantum cryptography for Multiple high-resolution millimeter wave images," IEEE, 2024.