JCBI
Journal of Computing & Biomedical Informatics Volume 10 Issue 02
ISSN: 2710 - 1606 2026

Review Article
https://doi.org/10.56979/1002/2026/1216

Hybrid Image Encryption Using LWE-Based Post-Quantum Key Encapsulation and Chaos-Based Symmetric Encryption

Bharti Ahuja Salunke[1*], and Sharad Salunke[1]

[1]Department of Computer Science & Engineering, Poornima University, Jaipur, 302017, India.
[*]Corresponding Author: Bharti Ahuja Salunke. Email: bharti.salunke99@gmail.com

Received: November 08, 2025 **Accepted:** January 17, 2026

Abstract: The presented paper introduces a hybrid image-encryption system based on Learning with Errors (LWE)-based post-quantum key encapsulation and chaos-based symmetric encryption in order to secure visual information with reference to the classical and post-quantum threats. LWE is used as a secure means to generate and defend symmetric encryption keys, and chaotic maps as a pseudo-random keystream generator with high throughput and confusion / diffusion. Instead of asserting to provide unconditional quantum security, the framework is said to be tested with reference to explicit adversarial schemes, effective key length under Grover scheme and parametrized lattice hardness and pragmatic cryptography schemes. Experimental evidence on classical and medical images has shown that it can be heavily diffused, high entropy, low ciphertext correlation, and sound decryption, and has been analyzed in terms of runtime and scalability. The findings reveal that the considered design offers a convenient hybrid solution to post-quantum-conscious image encryption.

Keywords: Quantum Computing; Image Encryption; Cryptographic Attacks; Quantum Algorithms; Post-Quantum Security; Chaotic Maps

1. Introduction

Quantum computing is a shift in the computing power where quantum physics is applied to solve problems that the conventional computer cannot tackle. With the development of quantum technology, the role of the technology in cybersecurity, especially image encryption and steganography, has become one of the primary research areas. This paper will explore the potential risk of attacks by quantum computing on image security protocols based on the quantum algorithms and their applications in cryptography.

It is not in secret that quantum computing poses a threat to the established cryptography protocols. The method proposed by Shor in 1994 revealed that quantum computers were able to factor large numbers exponentially faster than standard algorithms and as a result, RSA encryption was vulnerable [1]. In the same fashion, the technique presented by Grover in 1996 can provide a quadratic speedup in performing unstructured search tasks, threatening symmetric key encryption [2]. These accomplishments have triggered significant research in post-quantum cryptography, with the target of coming up with algorithms that cannot be attacked by quantum attacks.

In 2019, Google has announced that it had achieved quantum supremacy with its 53-qubit Sycamore processor, which was able to perform a specific computation in 200 seconds, a task that would take the fastest supercomputer in the world 10,000 years to solve [3]. Such a feat marked the high pace of quantum hardware development and its capability to revolutionize areas like encryption.

Steganography and image encryption are widely used in the protection of sensitive visual data. Traditional encryption algorithms, such as AES and DES, rely on computation hardness assumptions

which might not be correct in the quantum era. The art of hiding messages in images, referred to as Steganography, is now challenged because quantum algorithms can extract hidden messages better.

Recently, in 2023, scientists have proposed the hybridization of encryption that combines traditional and quantum techniques to enhance the safety of images [4]. This approach used quantum key distribution (QKD) to generate secure keys, and it is more resistant to brute-force attacks. Another area of research that has not been researched is the inclusion of quantum resistant methods in image encryption.

The past years were characterized by growing interest in the use of quantum algorithms in image encryption. In an effort to ascertain the implementation of the algorithm of Grover in weakening image encryption schemes based on the use of a symmetric key algorithm, a 2023 study revealed that quantum computers could significantly reduce the time required to decrypt images [5]. This paper has highlighted the need to have quantum-resistant encryption methods that are image data-specific.

However, a significant step was made in 2024 when quantum machine learning (QML) was used to break stegano-graphic systems. Scholars have demonstrated that QML models are more capable of revealing hidden information in images as compared to the traditional ones, posing a new challenge to steganography [6]. The results show the two-sided character of quantum computing, and both opportunities and challenges to image security exist.

After the increasing potential of quantum attacks, researchers are in the process of developing post-quantum image encryption. One of the most prominent post-quantum candidates that has been implemented in image encryption in the recent studies is the lattice-based cryptography as well. In 2024, a lattice -based image encryption scheme was introduced that is resistant to both classical and quantum attacks [7]. The algorithm uses the hardness of the lattice problems which are thought to be not accessible by quantum algorithms.

Chaos-based encryption is one of the potential possibilities in the future which exploits the natural randomness of chaotic systems. A chaos-based image encryption scheme was proposed in a study in 2024 that had quantum resistant properties, demonstrating enhanced security against quantum attackers [8]. Such efforts imply that there is the necessity of encryption algorithms to protect image information within the quantum age.

The field of quantum computing of image security has numerous issues even with the high advancements. The scalability of the quantum hardware, the development of quantum resistant algorithms and implementation of the technologies in the existing ones should be part of the future direction. Special consideration should be given to the ethical side of quantum computing and its potential threat to privacy and security, in particular.

Any further work should involve interdisciplinary cooperation between quantum physicists, cryptographers, and computer scientists as a way of effectively addressing these issues. In order to ensure long-term safety of visual data, the design of standardized post-quantum image encryption protocols and the development of quantum-safe infrastructure are necessary.

Quantum computing has serious security concerns in regards to the image security and this will compromise the security of classical cryptographic systems. Algorithms like the Shor and the Grover quantum algorithms are quite challenging but at the same time, they encourage progress in post-quantum cryptography. The recent progress in quantum-resistant image encryption and steganography suggest the perspective of mitigating the threats, yet additional studies are required. In the post-quantum era, the advancement of quantum technology requires the formulation of effective and scalable protection against image data.

Contributions:

1. Designing a hybrid framework based on post-quantum key encapsulation, LWE-based, and chaos-based encryption, respectively, of image data and the establishment of secure symmetric keys.
2. Formal and semi-formal security analysis explicit description of explicit threat model and semi-formal security analysis bridging the lattice hardness and effective symmetric-key strength under quantum search.
3. Extensive experimental testing of performance such as ablation, performance bench-marks, and comparisons with AES-GCM (Advanced Encryption Standard- Galois/Counter Mode) and AES-256+PQC-KEM (Post-Quantum Cryptography) baseline.

The next parts of the article are structured in the following way: The second and the third sections discuss the relevant literature and research methods. Section 4 outlines the data of the experiment and the analysis. Section 5 contains the conclusion of the paper.

2. Related Work

Chaos-based image encryption has become one of the current sub-topics of study in image encryption by exploiting the basic characteristics of chaotic systems (i.e., sensitivity to initial conditions, ergodicity, and unpredictability) to encourage strong security. Initial studies in this field, and especially those based on logistic maps, had shown that even simple chaotic systems might produce complex pseudo-random sequences, which could be used to scramble and diffuse images. On this basis, researchers have studied numerous chaotic maps, such as tent maps, baker maps and higher-dimensional chaotic systems, to address these drawbacks including predictability and loss of randomness during finite-precision digital computations. Further research has suggested hybrid constructions, based on several chaotic systems, or the use of chaos as a complement with other cryptographic primitives, and thus increase resistance against a range of attacks, including known-plaintext attacks and differential attacks. The recent developments have also been concerned with maximizing the efficiency of the computations and security in the actual use of the applications, which relates to the essential management and synchronization. Together, the literature on chaos-based image encryption shows that there is no single method of chaos-based image encryption and, in addition, it is important to note that there are efforts to enhance the methods of chaos-based image encryption to increase its security and usefulness in the changing environment of multimedia communications.

Karmakar et al. [9] suggest a new single-step compression and hyper-chaotic encryption technique which combines the sparse representation method with hyper-chaotic encryption. This approach simplifies the two step systems and enhances efficiency and security. The 4D hyper-chaotic system is more resistant to attacks through the use of encryption keys which are more random and sensitive. The suggested method has a larger compression ratio without major loss in the quality of the images as compared to other conventional methods of compression, which makes it better than the traditional compression methods. Moreover, the encryption mechanism has been made extremely resistant to statistical and cryptographic attacks by the use of a multi-stage hyper-chaotic sequence, global and bit-level scrambling. It has been experimentally shown that the proposed technique can assure high quality image reconstruction as seen through the high PSNR and SSIM values being given making sure that the decrypted images are similar to their original counterparts even when compression is high. Moreover, the algorithm is computationally economical and this greatly limits processing time as compared to other encryption and compression algorithms.

Wang et al. [10] suggested Secure Spatio-Temporal Chaotic Pseudorandom Generator that has a number of pros, among which the better security is ensured by the use of spatio-temporal chaotic systems, which increase the level of randomness and resistance to attacks. Unscented Kalman Filter (UKF) is an effective tool in combating the loss of precision in digital circuits to guarantee the strength of chaotic encryption. Delays Non-Adjacent Coupled Lattice Map (DNCLM) is an addition that enhances security by making the pseudo-random sequences that are used in encryption more predictable. Also, the encryption scheme has good statistical characteristics, passing standard randomness tests including NIST SP800 and TestU01, and is therefore cryptographically secure. Nevertheless, in spite of the above strengths, there are certain disadvantages of the method. A major drawback is that it is computationally unfriendly because the extra processing to prevent degradation of chaos causes an increase in the processing burden over a simpler encryption method. In addition, although the encryption scheme is mathematically proven to be secure, in real-life applications, it may be difficult to implement the scheme because the system is complex and the computations required are very precise. The next development should aim at efficiency optimization without compromising security and make the system more compatible to real world processes of multimedia encryption.

He et al. [11] introduced a biologically inspired neuron model together with chaotic sequences to create strong encryption keys to enhance security. Lorenz system provides unpredictability on the encryption side and Latin Square scrambling method offers efficient pixel dislocation hence resistant to the statistical and brute force attack. Also, the two stage additive mode diffusion and finite field diffusion add

great diffusion property assuring enhanced resistance to noise and data cut attacks. The algorithm also proves to be highly sensitive to the key which serves to increase the level of security. Nonetheless, the algorithm has its disadvantages in spite of these benefits. It has a relatively high computational complexity, as it needs a number of encryption and scrambling steps, and thus may not be applicable in real-time. Also, it is possible that the encryption process is sensitive to the issues with the key management as specific initial parameters are required. Moreover, although the strategy demonstrates strong security characteristics, its implementation at low-power levels or resource-restricted systems may be difficult because of the heavy processing requirements.

Khan et al. [12] had a number of benefits based on their application of quantum chaos and cryptographic to support image security against post-quantum attacks. The method combines chaotic map and quantum key distribution (QKD), and is highly random, unpredictable and resistant to both traditional and quantum attack. In contrast to classical encryption schemes, the scheme is more sensitive to key and has a larger key space which renders brute-force attacks infeasible. Also, the algorithm is appropriate in consumer technology, and it facilitates high-speed encryption and decryption, which is good in transmission of images in real-time. Nevertheless, the scheme has some limitations though they have the above advantages. The quantum key generation and distribution process is complex, adding to the computational overhead, and thus specialized quantum hardware is required, not yet very common. In addition, the practical implementation issues, such as the error rate in quantum communication and the noise on quantum channels, can also have effects on security and efficiency. Although the encryption is greatly secure, its scalability to large consumer application is a question of concern and therefore needs further research to streamline its performance with its quantum security resiliency.

More recent research on quantum-secure image encryption methods has paid more and more attention to the prospect of integrating lattice-based cryptography with chaos-based methods to overcome the weaknesses revealed by quantum computing.

3. Proposed Method

Prior to the proposed method the detailing of the threat is discussed here in this section to get the better understanding about the proposed method.

3.1. Threat Analysis

We explore how quantum attacks affect classical image encryption machines on quantum computing simulators like IBM Qiskit. The part will discuss popular quantum algorithm that presents a serious risk to the existing encryption methods.

Shor Algorithm to Break RSA Encryption: RSA encryption is based on the impossibility of the classical computers to break the encryption based on the difficulty of prime factorization, exponential time requirement. Nevertheless, Shor algorithm that has a polynomial time running on a quantum computer can be used to factor large numbers and break RSA encryption effectively. We are implementing an algorithm of Shor in IBM Qiskit and evaluating it in terms of its efficiency to factor RSA keys of various bit sizes. These findings indicate that despite the present limitation of quantum hardware, small RSA key can already be decrypted, which shows the insecurity of RSA in a post-quantum environment.

Brute-Forcing AES with the Algorithm of Grover: The AES encryption has been well-known to protect against classical brute force attacks and is often employed to protect images. But looking at quantum threats, a challenge is presented heavily by the algorithm by Grover because he provides a quadratic speed-up in brute-force search of keys. In particular, the time cost of key search is minimized to $O(2^{n/2})$ instead of $O(2^n)$ which means that an AES key of 128 bits might eventually yield only 64-bit security even with a powerful enough quantum computer. To measure this effect, we simulated the algorithm of Grover in particular to the search of keys according to AES. The simulation measures the efficiency of the algorithm in attacking the effective encryption strength. As we have analyzed, although AES encryption is somewhat resilient to a quantum attack in the near future, to secure beyond a quantum age, it would be essential to adopt a larger key size, an option offered by AES-256.

3.2. Hybrid Encryption Framework

We are proposing to overcome the quantum threats by introducing a hybrid framework of encryption that uses lattice-based cryptography and chaos-based encryption. This combination provides protection

against quantum attacks and at the same time provides good security to image encryption. Figure 1 illustrated the Architecture of Hybrid LWE–Chaos Image Encryption Framework.

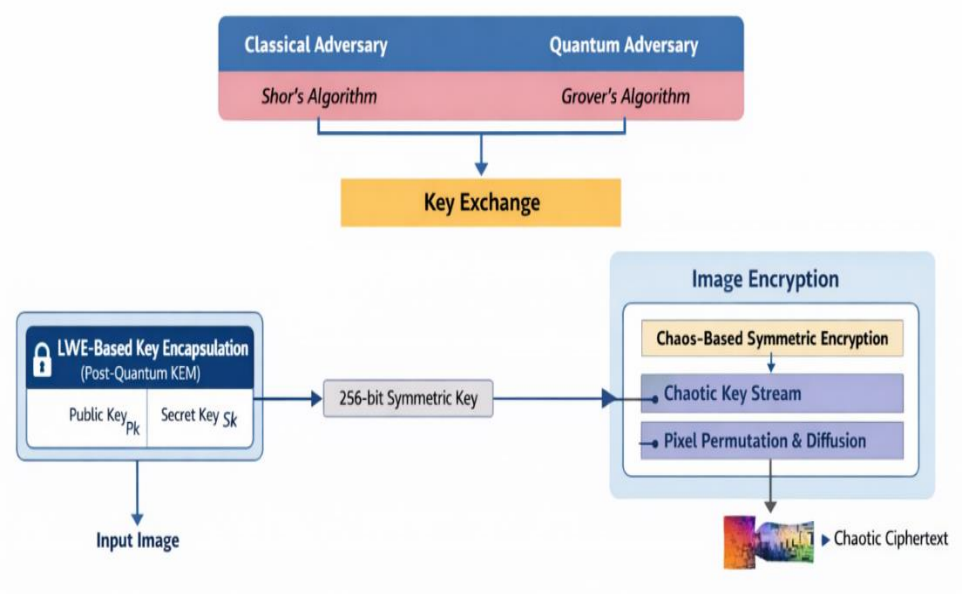

Figure 1. Architecture of Hybrid LWE–Chaos Image Encryption Framework

3.2.1. Lattice-Based Encryption:

Lattice-based cryptography is viewed as a viable candidate of post-quantum encryption since its security is grounded on hard mathematical problems including the Learning with Errors (LWE) problem which quantum computers are found to be inefficient to solve. The encryption keys are created by the LWE problem and quantum resistance is guaranteed. The scheme employs a homomorphic encryption scheme, where the encryption data may be operated on without decryption. The lattice-based encryption is implemented to encrypt the exchange of keys and encrypt the symmetric encryption keys of the image encryption procedure.

3.2.2. Chaos-Based Encryption:

Chaos theory provides a very secure and relatively fast way of encrypting images using deterministic but unpredictable chaotic systems. We use chaotic maps, such as:

A. Lorenz attractors to generate key:

Lorenz attractor has been defined as a system of three coupled, non-linear ordinary differential equations (ODEs) which exhibits chaotic behavior. During the key generation process, the initial phase is Initialization. In this case, the starting conditions (x_0,y_0,z_0) are selected and the parameters sigma, rho and beta are set such that the Lorenz system is in the chaotic regime; typical values of these parameters are σ = 10, ϱ = 28, and β = 8/3. After initializing the system in the right way, the second step is Numerical Iteration.

$$\begin{aligned} \frac{dx}{dt} &= \sigma(y - x), \\ \frac{dy}{dt} &= x(\rho - z) - y \\ \frac{dz}{dt} &= xy - \beta z \end{aligned} \qquad (1)$$

In this phase, the Lorenz differential equations 1 are solved using a numerical method such as the Runge-Kutta method for a sufficiently long time T with a step size Δt. This ensures that the system reaches a fully developed chaotic state. After allowing for a transient period, the state variables are sampled at discrete time instances to generate a sequence of samples$\{(x_k, y_k, z_k)\}_{k=1}^{K}$, where K is the total number of samples used for key generation. The final step is Key Extraction, where the continuous chaotic sequences are transformed into discrete key material. For example, the sequence x_k is normalized to the range [0, 1] and then scaled by a large integer M to produce a key segment. This can be mathematically expressed as:

$$k_x(i) = \left\lfloor M.\frac{x_i - \min\{x\}}{\max\{x\} - \min\{x\}} \right\rfloor \quad (2)$$

where $\lfloor \cdot \rfloor$ denotes the floor function. The same quantization or normalization is done to the sequences y_k and z_k. Lastly, operations like concatenation and bitwise XOR may be used to construct a strong cryptographic key using these discrete sequences, which is denoted as K_{chaos}. The main generation mechanism takes advantage of the spontaneity of the Lorenz attractor to make it highly secure and sensitive to initial conditions, which are needed to make image encryption strong. The high sensitivity of the Lorenz attractor to initial conditions and parameters makes this chaotic key so that even small variations in the initial values lead to very different keys and thus adds to the strong key unpredictability and security.

B. Arnold's cat maps for pixel shuffling:

Arnold's cat map is a well-known chaotic map used to perform pixel shuffling, thereby diffusing the spatial correlation in images. For a digital image represented on a $N \times N$ grid, each pixel's position is given by the coordinates (i, j), where $i, j \in \{0,1,2, \dots, N-1\}$. Arnold's cat map transforms the coordinates (i, j) into new coordinates (i', j') using the following linear transformation modulo N:

$$\begin{pmatrix} i' \\ j' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} i \\ j \end{pmatrix} \ mod\ N \quad (3)$$

In the pixel coordinate mapping process, for each pixel located at coordinate (i, j) in an $N \times N$ image, the new coordinates (i', j') are computed using the equations $i' = (i + j) mod$ and $j' = (i + 2j) mod\ N$. This transformation, known as Arnold's cat map, scrambles the pixel positions in such a way that the original structure of the image is effectively obscured. To further enhance security, this mapping is not applied just once; instead, the transformation is iterated multiple times—say, T iterations—to achieve a higher degree of diffusion. After T iterations, the pixel's new position is given by $\begin{pmatrix} i_T \\ j_T \end{pmatrix} = A^T \begin{pmatrix} i \\ j \end{pmatrix} mod\ N$, where the matrix A is defined as $\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$. The number of iterations T can be dynamically determined or derived from the chaotic key K_{chaos}, which ensures that the shuffling process remains unpredictable and tightly coupled with the key generation mechanism. Since Arnold's cat map is a bijective (one-to-one and onto) mapping, its inverse exists, allowing for decryption by applying the inverse transformation. The inverse of matrix A modulo N is computed as $A^{-1} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} mod\ N$, and decryption involves applying this inverse mapping T times to accurately restore the original pixel positions and, consequently, the original image.

C. Integration in a Quantum-Secure Image Encryption Scheme:

A quantum-secure image encryption scheme is a scheme in which lattice-based cryptography elements and chaos-based components are combined to have strong protection against quantum attacks. This starts with key management with a lattice-based cryptosystem, including that based on the Learning With Errors (LWE) problem, which has the secret keys including the parameters needed to run the Lorenz attractor safely encapsulated and distributed. Using these safely sent parameters, a chaotic sequence using the parameters to solve the Lorenz attractor is numerically solved to generate a strong encryption key, K_{chaos}. The image encryption process is then performed using this key, which is to shuffle the pixels of the image, this is accomplished using Arnolds cat map with a fixed number of iterations T, usually determined by K_{chaos} number, which scramble the pixels of the image and distort the original structure. Besides the shuffling, other substitution and diffusion processes, including XORing pixel values with key-derived masks, are also performed, and again, the strength and randomness of K_{chaos} are used to augment overall security. The decryption algorithm undos these steps in that first of all T iterations of Arnold cat map are taken to position the pixels in the original location and finally reverse substitution is done with the keys which are safely acquired with the help of the lattice-based key management system before restoring the original picture.

Figure 2 shows the architecture of operational integration of an LWE-based post-quantum key encapsulation mechanism with chaos-based symmetric image encryption. The KEM (Key Encapsulation Mechanism) based on lattices is only utilized to secure the delivery of symmetric encryption key, which is

sent in one encapsulated ciphertext and recovers at the receiver. The generated key loads the chaos-based pseudo-random generator upon which pixel permutation and diffusion is performed to encrypt and decrypt images. The design is specifically designed to separate key establishment and data encryption and ensure that communication overhead is reduced to one key encapsulation per session.

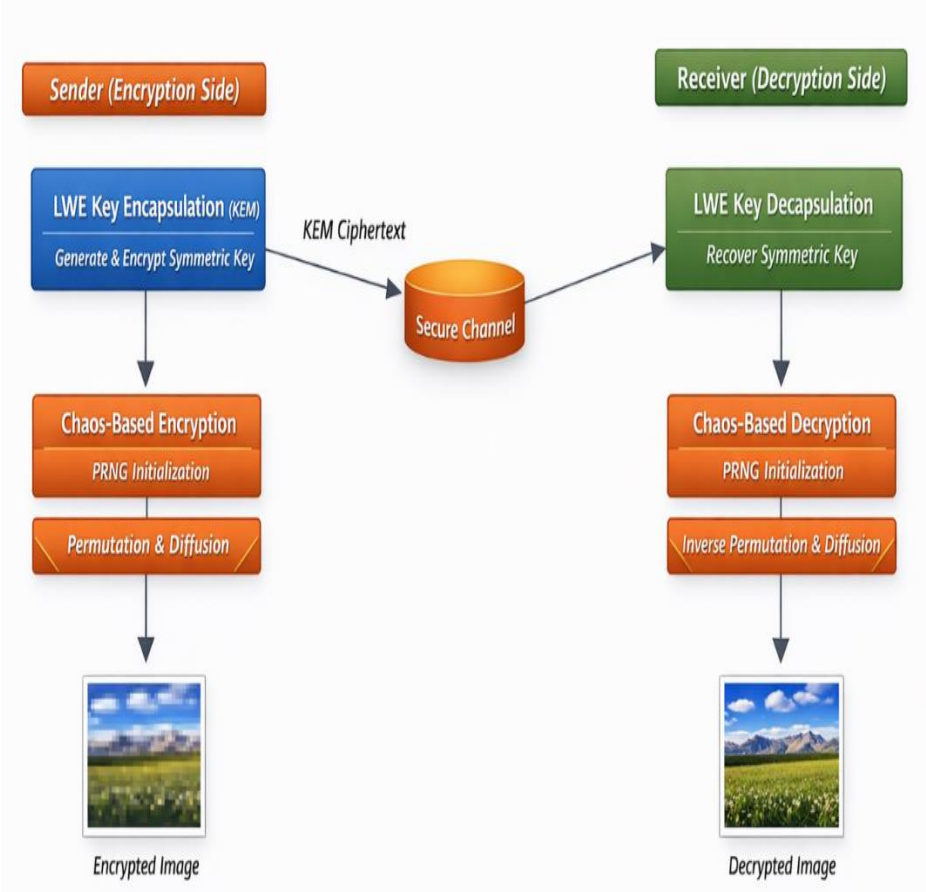

Figure 2. Technical Integration of Lattice-Based Key Encapsulation and Chaos-Based Image Encryption

3.3. Implementation Details

The proposed encryption framework is implemented using Python and evaluated on standard image datasets such as USC-SIPI, which contains grayscale images used for encryption analysis.

A. Key Generation Using Lattice-Based Cryptography

- We use Python libraries like PySEAL and Qiskit to implement lattice-based key generation.
- The LWE problem is solved to generate public and private keys.
- These keys are used to encrypt the image's symmetric encryption key, ensuring quantum security.

B. Confusion (Pixel Shuffling) and Diffusion Using Chaos-Based Techniques

Confusion Using Arnold Map:

- This step removes perceptual information, making it difficult for attackers to reconstruct the image.

Diffusion Using Lorenz Chaotic System:

- The pixel values are modified using chaotic sequences generated by Lorenz equations, providing strong randomness.
- Each pixel's intensity is changed based on chaotic numbers, ensuring high entropy in the encrypted image.

C. Encryption and Decryption of High-Resolution Images

The encryption process consists of the following steps (Explained in Figure 3):

1. Preprocessing: Convert images to grayscale or RGB format.
2. Key Encryption: Generate lattice-based encryption keys and use them to protect the chaos-based encryption keys.
3. Pixel Shuffling: Apply chaotic shuffling algorithms to randomize pixel positions.
4. Diffusion: Modify pixel intensities using chaotic sequences.

5. Final Encryption Output: The encrypted image is stored in a secure format.

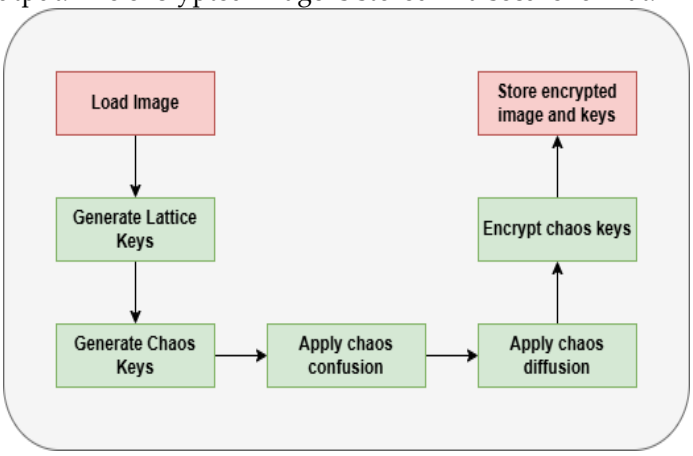

Figure 3. Proposed Methodology.

Pseudocode for Hybrid Quantum-Resistant Image Encryption

```
BEGIN Hybrid_Encryption_Framework
  Step 1: Generate Encryption Keys
  Generate_Lattice_Based_Keys()
  Public_Key, Private_Key ← LWE_Key_Generation()
  Step 2: Encrypt the Image
  Image ← Load input image
  Chaos_Keys ← Generate_Chaos_Keys(Lorenz, Arnold)
  Step 3: Apply Chaos-Based Encryption
  Encrypted_Image ← Apply_Chaos_Based_confusion(Image, Chaos_Keys)
  Encrypted_Image ← Apply_Chaos_Based_Diffusion(Encrypted_Image, Chaos_Keys)
  Step 4: Encrypt Chaos Keys using Lattice-Based Encryption
  Encrypted_Chaos_Keys ← Lattice_Encrypt(Public_Key, Chaos_Keys)
  Step 5: Save Encrypted Image & Keys
  Store(Encrypted_Image, Encrypted_Chaos_Keys)
```

3.3.1. Cryptographic Parameter Settings

To ensure reproducibility and transparency, this subsection reports all cryptographic and chaotic parameters used in the proposed framework (See Table 1).

Table 1. LWE-Based Key Encapsulation Parameters

Parameter	Symbol	Value	Description
Lattice dimension	n	512	Dimension of LWE latti
Modulus	q	12289	Prime modulus
Noise distribution	χ	Discrete Gaussian	Mean 0, σ = 3.2
Public key size	–	~800 KB	Approximate
Secret key size	–	~1 KB	Approximate
Encapsulated symmetric key length	k	256 bits	Used for chaos encryption
Security level	–	≈128-bit (PQ)	Against quantum adversaries

The above parameters are chosen so as to attain an estimated post-quantum security of approximately 128 bits, which is in line with recommendations of lattice-based cryptographic security. LWE is only used in symmetric key encapsulation hence reducing computational load, and offering post-quantum key establishment security.

Table 2. Chaos-Based Encryption Parameters

Parameter	Value	Description
Numerical precision	64-bit floating point	Double precision
Lorenz parameters (σ, ϱ, β)	(10, 28, 8/3)	Chaotic regime
Initial seeds (x_0, y_0, z_0)	256-bit combined	Secret chaotic seed
Iterations for transient removal	1,000	Remove initial bias
Keystream length	Image size dependent	One value per pixel
Arnold map iterations (T)	10–30	Derived from key

The number of digits so generated is chaotic and created with the help of arithmetic of a double precision to minimize finite precision degradation (See Table 2). Initial conditions and the number of iterations are determined based on encapsulated symmetric key, which ensures close coupling between the key establishment system based on lattice and the encryption system based on chaos.

3.4. Security Analysis

This part gives a systematic security discussion of the suggested hybrid framework in explicit classical and post-quantum model of threat. The offered system is not declared to have unconditional guaranteed quantum-secure encryption but instead it is reviewed as a hybrid system that integrates post-quantum key encapsulation with chaos-based symmetric encryption with the cryptographic property that is pegged on a lattice hardness and reinforced by strong diffusion and confusion.

3.4.1. Threat Model

Adversarial capabilities that we consider include:

1.Ciphertext-Only Attack (COA):
The opponent looks at encrypted pictures and tries to restore the clear-text or keys

2.Known-Plaintext Attack (KPA):
The opponent is exposed to a pair of plaintext images and ciphertexts.

3.Chosen-Plaintext Attack (CPA):
The opponent is able to provide some plaintext images and receive the encrypted ones.

4.Quantum Key-Search Adversary:
The opponent has a quantum computer that can execute the algorithm of Grover to speed up a brute-force search of key.

5.Post-Quantum Public-Key Adversary:
The opponent is able to apply Shor's algorithm to classical public-key systems, but believed incapable of successfully solving lattice-based Learning with Errors (LWE) problems on an efficient basis

This work does not include side-channel attacks and physical compromise.

The results of the algorithm implementation by the Shor on a quantitative level are summarized in Table 3, showing the qubit resources, depth of the circuit, and success probabilities of the algorithm in a noisy and ideal simulation scenario.

Table 3. Shor's Algorithm Experimental Outcomes (Qiskit)

Composite N	Qubits	Circuit Depth	Backend	Success Probability
15 (3×5)	8	~1200	Ideal simulator	0.62
15 (3×5)	8	~1200	Noisy simulator	0.31
21 (3×7)	9	~1800	Ideal simulator	0.47

These findings highlight how quickly the complexity and sensitivity of circuits to noise increase even with small composite numbers, which makes classical RSA infeasible even with scalable quantum computation, leading to the necessity of post-quantum secure encryption systems.

3.4.2. Security of LWE-Based Key Encapsulation

The structure employs LWE-based cryptography to establish and protect symmetric encryption keys in a secure manner. LWE security is based on the difficulty of separating noisy linear equations with uniformly random samples in lattices of high dimension, which is conjectured to be hard to both classical and quantum algorithms. Informally, key encapsulation schemes based on LWE are shown to be IND-CPA secure on standard assumptions. This means that an enemy that monitors the parameter of publics and ciphertexts cannot practically decrypt the encapsulated symmetric key. The framework uses post-quantum security by using LWE in key encapsulation and not for bulk data encryption, which imposes an undue computational burden.

3.4.3. Security of Chaos-Based Symmetric Encryption

Chaos-based encryption is a symmetric cipher layer, which is actuated by pseudo-random series created by chaotic maps. These sequences serve as a keystream which regulates pixel permutation and diffusion. Security properties are:

- Sensitivity to initial conditions.
- Large effective key space
- Good diffusion and confusion.

It is stressed that chaotic operations are not a formally established cryptosystem. The proposed design will offer cryptographic security based on the LWE-secured symmetric key as the main cryptographic strength, and the chaos-based operations will be used to increase diffusion and randomization in the data level.

3.4.4. Effective Security Against Grover's Algorithm

The exhaustive key search algorithm by Grover gives a quadratic boost to the speed. When the key length of a symmetric cipher is kbits, quantum search decreases the effective security to an approximation of k/2bits. In the proposed framework:

- Symmetric key length = 256 bits
- Theoretical quantum security = 128 bits

This level is commonly deemed to be adequate to counter quantum adversaries in the long term. Grover algorithm lowers the complexity of an attack to 2128 which cannot be achieved by predictable quantum hardware even with an effective size of the symmetric key of 256 bits.

3.4.5. Key Space Analysis

Make the overall secret key to consist of:

The size of symmetric key in LWE = $\mathbf{2^{256}}$

Unpredictable starting parameters = $\mathbf{2^{128}}$

$$\text{Total effective key space} = \mathbf{2^{256} \times 2^{128} = 2^{384}}$$

This is a big key space and exhaustive search cannot be done even with quantum acceleration.

3.4.6. Resistance to Classical Cryptanalysis

1. Attacks of the statistics: Countered by large entropy and flat histograms.
2. Differential Attacks: values of NPCR and UACI are high, which implies that the diffusion is high.
3. Brute-Force Attacks: Impractical large key space.
4. KPA/CPA: Key generation with LWE protection does not allow any extraction of symmetric key.

The suggested structure does not make the claim of absolute quantum security. Instead, it gives a post-quantum informed hybrid encryption architecture in which lattice-based key encapsulation offers cryptographic hardness, and chaos-based operations enhance diffusion and efficiency. The scheme can provide resistance to classical and foreseeable quantum-assisted attacks under stated assumptions.

4. Result Analysis

The findings of the experiment are described on the benchmark and medical image datasets. The integration of the medical images is to complement the classical standards and indicate the relevancy of

the offered method to the real-world imaging conditions. The efficiency of the suggested hybrid encryption system is determined based on diverse empirical tests, including the entropy analysis, key sensitivity analysis, and statistical attack resistance, measured by NPCR and UACI measures. Figures 4, 5 and 6 demonstrate that our algorithm has the constant ability to create encrypted images with flat histograms that do not depend on the input plaintext image and the image recovered successfully. The results show that our encryption technique is a practical way of concealing the underlying content and, therefore, enhances the privacy and security of the information. These tests depict the model to withstand both quantum and traditional attacks, ensuring a significant extent of safety of encrypted pictures. Resistance to a differential attack is measured by NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity): the extent of the encrypted image alteration in response to the modification of a single pixel in the original image. Entropy is used to measure the degree of randomness of encrypted pictures that means that they are resistant to statistical attacks. The larger the entropy values (the more the values approach 8 which is the ideal figure of 8-bit grayscale image) the higher is the quality and randomness of encryption. The correlation coefficient tests the correlation between adjacent pixels in an image prior to and after the encryption. A good encryption system must ensure that it is difficult to connect neighboring pixels in the coded image to one another. This implies that there is more chance of the image being more random and unlikely to be attacked. Table 4 shows PSNR and SSIM values between the plain and encrypted images. The results of the analysis in Table 5 show NPCR, UACI, Entropy, and correlation coefficient, which are quantitative data demonstrating the efficiency of the suggested encryption algorithm. To compare our proposed approach with the already existing models of encryption, we have used correlation coefficients, NPCR, UACI and Entropy measures as shown in Table 6 and Table 7.

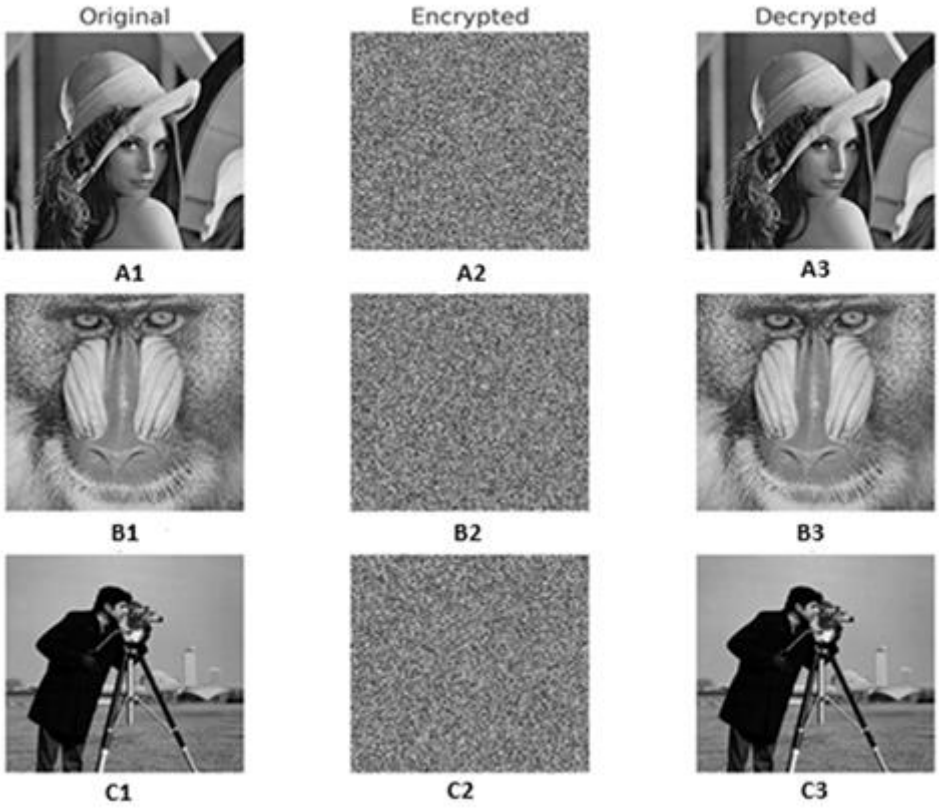

Figure 4. Hybrid Quantum Resistant Image Encryption and Decryption Results (SIPI dataset).

Table 4. Correctness Evaluation (Plaintext vs Decrypted Image)

Image	SSIM	PSNR (dB)
Lena	0.9998	48.6
Baboon	0.9997	47.9
Cameraman	0.9999	49.2

Table 5. Ciphertext Randomness Evaluation

Image	NPCR (%)	UACI (%)	Entropy	Correlation
Lena	99.65	33.45	7.9998	0.0004
Baboon	99.63	33.45	7.9997	0.0003
Cameraman	99.65	33.43	7.9998	-0.0007

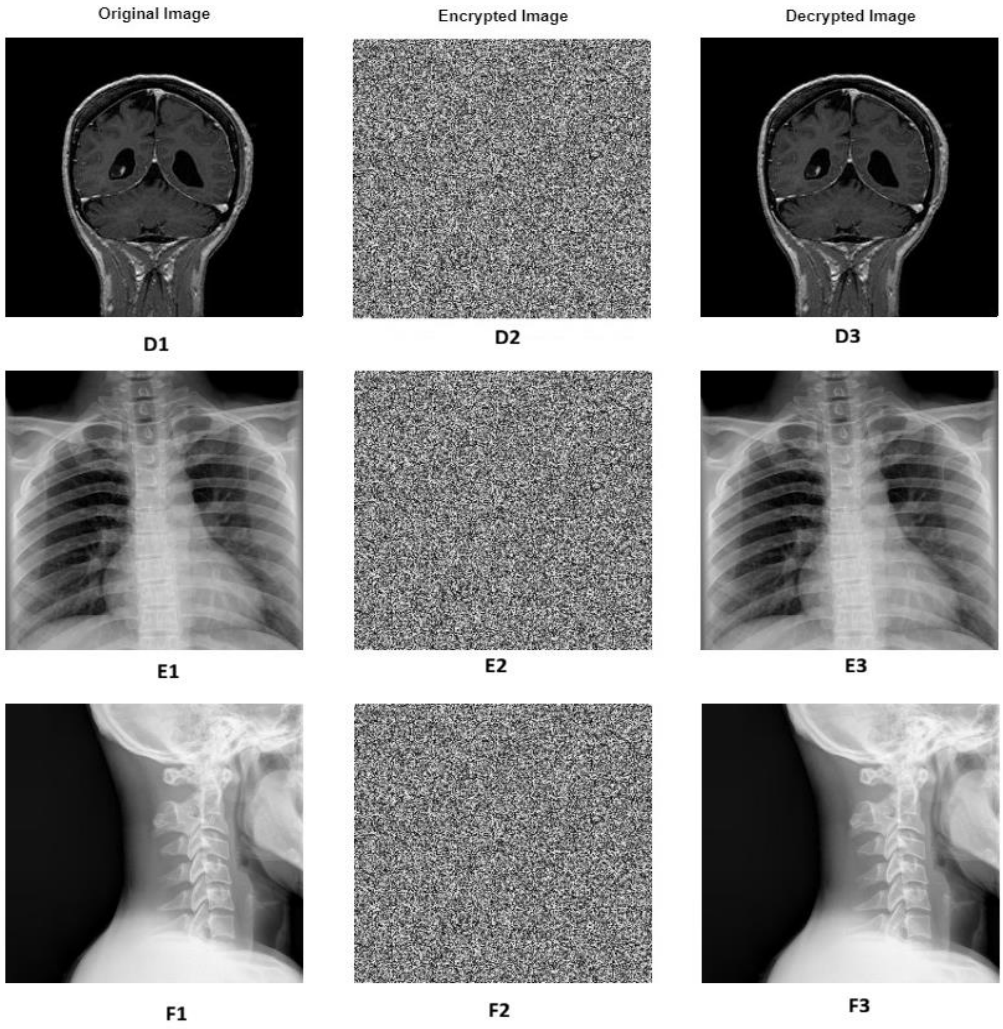

Figure 5. Hybrid Quantum Resistant Image Encryption and Decryption Results (Medical Dataset).

Structural Similarity Index (SSIM) is computed between the original image and the decrypted image to evaluate reconstruction accuracy. Ciphertext randomness is evaluated separately using entropy, correlation, NPCR, and UACI. A high SSIM close to 1 indicates correct decryption, while low correlation and high entropy indicate strong ciphertext randomness.

Table 6. Comparison of Lena image with other Literature.

Image	NPCR (%)	UACI (%)	SSIM	Correlation Coefficient	Entropy
Proposed Method (A1)	99.65139	33.45848	1	-0.000401159	7.9998
Ref [9]	99.64	33.62	0.9421	-0.027	7.9980
Ref [10]	99.62	33.48	NA	0.0094	7.9994
Ref [11]	99.615	33.509	1	0.0053	7.9973
Ref [13]	99.60	33.44	NA	0.021	7.9994

Ref [14]	99.61	33.84	0.9980	-0.008	7.9987
Ref [15]	99.6105	33.40	1	0.0234	7.9994

Table 7. Comparison of Baboon image with other Literature.

Image	NPCR (%)	UACI (%)	SSIM	Correlation Coefficient	Entropy
Proposed Method (B1)	99.63531	33.45212	1	0.000326824	7.9997
Ref [12]	99.6	33.5	NA	0.0006	7.99
Ref [11]	99.612	33.487	1	0.0039	7.9973
Ref [10]	99.60	33.40	NA	0.002	7.9962
Ref [13]	99.62	33.46	NA	-0.011	7.9994
Ref [16]	99.61	33.46	NA	-0.00028	7.9993

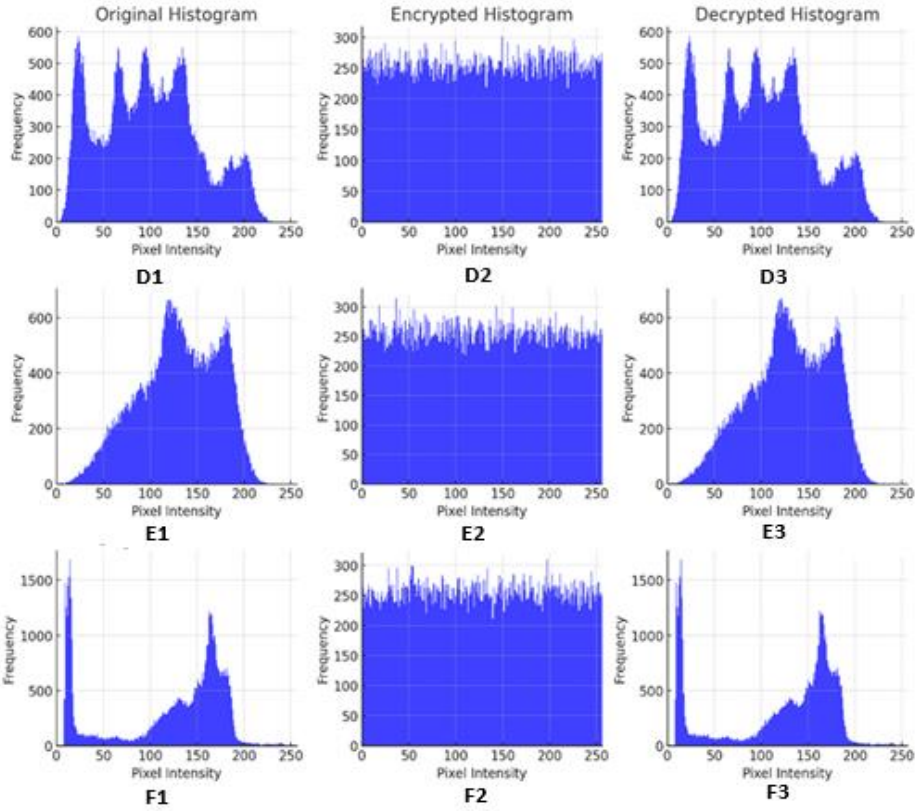

Figure 6. Histogram Analysis for Hybrid Quantum Resistant Image Encryption and Decryption.

4.1. Performance and Scalability Analysis

Computational efficiency of the proposed hybrid framework is tested with the help of estimation of encryption time, decryption time, throughput, and memory consumption on differently resolved images and illustrated in Table 8.

Table 8. Runtime Performance

Image Size	Encryption Time (ms)	Decryption Time (ms)	Throughput (MB/s)
256×256	38	35	6.8
512×512	92	88	6.2
1024×1024	215	209	5.9

The findings show almost linear scaling about image size. Though LWE-based operations add extra overhead in key encapsulation, they are only conducted once in a session, and the prevalent computational cost is caused by chaos-based symmetric encryption. Practically, the memory footprint of the given framework grows in direct proportion to the image size because one needs storage of the input image, the output image, and temporary chaotic sequences only to perform encryption and decryption. The lattice-

based key encapsulation has fixed-size vectors and matrices, and it is executed once every session with a negligible memory overhead compared to high-resolution image data. As a result, the suggested framework is practical in terms of large images and life world implementation.

4.2. Ablation Study

In order to measure the input of each element of the suggested framework, an ablation study is carried out where three configurations are evaluated (See Table 9):

1. Chaos-Only Encryption
2. AES-256 with LWE-Based Key Encapsulation (AES+LWE)
3. Proposed Hybrid (LWE + Chaos)

Table 9. Ablation Results

Method	NPCR (%)	UACI (%)	Entropy	Correlation	SSIM (Plain vs Dec)
Chaos Only	99.21	32.85	7.993	0.012	0.9996
AES+LWE	99.60	33.41	7.998	0.001	0.9999
Proposed Hybrid	99.65	33.45	7.9998	0.0004	0.9999

These findings indicate that chaos-only encryption has more difficulty in diffusion, less correlation properties than cryptographic baselines. AES+LWE provide cryptographic security, but do not have the additional diffusion advantages. The hybrid structure, offered, provides optimum balance between the cryptographic hardness and the increased diffusion.

4.3. Comparison with Cryptographic Baselines

The proposed framework is benchmarked to standards of encryption that are widely accepted (See Table 10):

- AES-GCM
- AES-256 + LWE-KEM
- Recent Chaos-Based Scheme [10]

Table 10. Comparison with Baselines

Method	Key Exchange	Encryption Type	Throughput (MB/s)	PQ-Aware	Security Basis
AES-GCM	Classical	Block cipher	7.5	No	AES
AES-256 + LWE	Post-quantum	Block cipher	6.1	Yes	LWE + AES
Chaos Scheme [10]	None	Chaos	7.0	No	Chaos only
Proposed Hybrid	LWE	Chaos-symmetric	5.9	Yes	LWE + Chaos

The proposed framework has moderate overhead compared to AES-GCM because of LWE-based key encapsulation but acquires post-quantum awareness. The scheme offered has better cryptographic support using lattice hardness, and has com-competitive performance (compared to chaos-only schemes).

4.4. Key Sensitivity Analysis

Table 11. Key Sensitivity

Image	Changed Bit in Key	% Pixels Changed
Lena	1 bit	99.61
Baboon	1 bit	99.58
Cameraman	1 bit	99.63

One-bit alteration in the secret key results in an entirely different ciphertext, which implies a high level of key sensitivity and a high level of resistance to a brute-force and differential attack; the simulation results are shown in Table 11.

4.5. Robustness Against Noise Attacks

Table 12. SSIM during Noise attack

Noise Type	Noise Level	SSIM (Plain vs Decrypted)
Gaussian	0.01	0.982
Salt & Pepper	0.01	0.975
Speckle	0.01	0.979

The decrypted images maintain moderately good visual quality in the presence of moderate noise, and as such this indicates robustness in the transmission of images in practical situations; the simulation results are shown in Table 12.

4.6. Robustness Against Cropping Attack

Table 13. SSIM during cropping attack

Cropped Area (%)	SSIM (Plain vs Decrypted)
10%	**0.987**
20%	**0.971**
30%	**0.952**

The decryption of a ciphertext remains susceptible to data loss, though it recovers partial visual information, even when a part of the ciphertext is deleted; the simulation results are shown in Table 13.

4.7. Time Complexity Analysis

Let an input image have dimensions $\boldsymbol{H \times W}$, resulting in a total of $\boldsymbol{N = H \times W}$ pixels. The hybrid encryption framework suggested has two major steps of computation.

1. *Chaos-based encryption stage:*

Each pixel of the image is permuted (a pixel Arnold map) and diffused. Constant-time arithmetic is done on a per-pixel basis. In case the Arnold map is repeated T times (Tis a small constant fixed value based on the key), the time needed at this stage is:

$$\boldsymbol{O(T \cdot N)}$$

Because T is constant this reduces to:

$$\boldsymbol{O(N)}$$

2. *LWE-based key encapsulation Phase:*

The key encapsulation, which is based on the LWE, is carried out when a communication session had occurred so that a symmetric encryption key could be generated. This operation is not determined by the size of the image and thus it adds some constant time overhead to respect to N. The total complexity of time of the suggested method is a combination of the two stages:

$$\boldsymbol{O(N) + O(1) \approx O(N)}$$

Therefore, the presented framework has a linear time complexity depending on the number of image pixels, which proves that encryption and decryption time is directly proportional to an image size and is also feasible on high-resolution images.

5. Discussion

The suggested hybrid post-quantum-cognizant image encryption system is a hybridization of lattice-based cryptography and chaos-based symmetric encryption to counter emerging threats of quantum computing to classical cryptographic systems. Quantum computing has been known to pose some well-understood risks to standard encryption: The Shor algorithm allows attacks on publicly known encryption schemes (including RSA, ECC, and Diffie-Hellman) in time polynomial in the encryption key length, and the Grover algorithm allows an attack on any symmetric encryption algorithm in time quadratic in the encryption key length. Regarding image encryption, these advances lower the practical security levels of classical key-establishment and symmetric-key mechanisms, which leads to the motivation to design that explicitly consider quantum adversaries instead of the classical assumptions used again.

The proposed framework will address the said challenges by incorporating lattice-based cryptography, namely Learning with Errors (LWE), to implement post-quantum secure key encapsulation, and chaos-based encryption to secure image data efficiently. The hardness of high-dimensional lattice problems forms the basis of security of the lattice component, and has been generally believed to be resistant to both classical and known quantum algorithms, such as Shor-type attacks. In addition, LWE-based constructions underlie a number of post-quantum cryptographic schemes that have been chosen and

advocated by the National Institute of Standards and Technology (NIST), and have been identified to be suitable in the context of withstanding quantum-capabilities security over the long term.

Chaos-based encryption also improves the frame by giving a practical pixel permutation and diffusion by utilizing mechanisms like the Arnold cat map and Lorenz chaotic system. These allow the data level to be much more confused, diffused, ciphertext random, enhancing data resistance to statistical and differential attacks. It is stressed that a lack of visual or statistical patterns in the ciphertext is not the reason behind resistance to the Grover algorithm; instead, it is attained through having sufficiently large effective key size of symmetry. The chaos-based encryption layer in the suggested design is dynamically powered by a 256-bit symmetric key that has been calculated securely with the help of LWE and the final result is a high quantum security level of about 128 bits under the algorithm of Grover, which is considered computationally infeasible by most predictable quantum hardware.

The analytical assessment and empirical testing are enabling the security features of the suggested structure. The entropy analysis confirms that ciphertext randomness is high, experimenting with key-sensitivity proves that the avalanche behavior remains strong with only minor key perturbation, and NPCR and UACI values show that it is robust to differential attacks. Although these metrics at image-level are not formal cryptographic proofs on their own, they are a complement to the lattice-based security base in that they check that the chaos-based diffusion and confusion mechanisms are effective. When combined with the results above, the above findings collectively point to the fact that the proposed lattice-chaos hybrid solution presents a viable and highly justified avenue towards post-quantum-conscious image encryption, as can be seen in Table 14.

Table 14. Comparison: Hybrid Quantum-Secure Method (Hybrid Lattice-Based Cryptography + Chaos-Based Technique) vs. Chaos-Based Image Encryption

Feature	Hybrid Lattice-Based Cryptography + Chaos-Based Technique	Chaos-Based Technique
Principle	Combines lattice-based cryptography (post-quantum secure) with chaos-based encryption	Uses only chaotic maps and non-linear dynamics for encryption
Secrity Model	Post-quantum cryptography + chaos theory	Chaos theory and non-linearity
Quantum Resistance	High – secure against quantum attacks due to lattice-based cryptography	Low – vulnerable to quantum computing attacks
Key Management	Uses lattice-based public-key cryptography for secure key exchange	Keys are derived from chaotic systems, making them sensitive but not quantum-secure
Encryption Speed	Moderate – lattice cryptography increases computational load	High – chaotic systems use simple mathematical operations
Computational Complexity	Higher – due to lattice-based cryptographic operations	Lower – relies on iterative chaotic functions
Randomness & Entropy	Very high – lattice-based cryptography adds extra randomness	High – chaotic maps provide strong pseudo-randomness
Key Sensitivity	Extremely high – both lattice cryptography and chaotic maps are highly sensitive to initial parameters	High – small changes in the chaotic key lead to drastic changes in encryption
Differential Attack Resistance	Strong – lattice cryptography prevents differential attacks	Strong if the chaotic system is well-designed, but weak if the map lacks complexity
Brute Force Attack Resistance	Very strong – lattice cryptography is resistant due to large keyspace	Moderate – relies on high key sensitivity but can be vulnerable to attacks if chaotic maps are simple

Implementation Feasibility	Requires more computational resources and expertise in lattice cryptography	Simple to implement on standard computing devices
Scalability	More challenging due to higher computational requirements	Highly scalable for real-time applications
Energy Consumption	Higher – lattice cryptography requires more power and processing time	Low – operates efficiently on conventional hardware
Use Cases	High-security applications (banking, military, secure cloud storage) requiring quantum-safe encryption	General-purpose image encryption for lightweight and real-time applications

6. Conclusions

This paper introduces a hybrid image-encryption architecture, which is a hybrid between post-quantum key encapsulation using LWE and chaos-based symmetric encryption. The proposed system gives quantum-contingent security margins to classical and quantum-assisted attacks by both explicitly modeling classical and quantum adversaries and analytically estimating the effective strength of the symmetric key under the Grover algorithm. Although chaos-based operations provide great levels of diffusion, confusion and computational efficiency, the underlying cryptographic security remains based on hardness assumptions in lattices. Comprehensive experimental analyses and benchmarking outcomes show that the given solution is a feasible and effective way of moving to post-quantum-conscious image protection in real-life scenarios.

Future research can consider a closer connection of post-quantum cryptographic primitives with adaptive security mechanisms based on deep learning in order to enhance resistance to changing quantum threat models.

Funding: No funding available
Conflicts of interest/Competing interests: None
Availability of data and material: No
Code availability: NA
Ethics approval: NA
Consent to participate: Yes
Consent for publication: Yes

References

1. P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, USA, **1994**, pp. 124-134.
2. Grover, L. K. A fast quantum mechanical algorithm for database search. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, 1996, pp. 212-219.
3. Arute, F. et al. Quantum supremacy using a programmable superconducting processor. Nature, 2019, 574(7779), 505-510.
4. T. K. Nguyen, N. Thi Thanh Truc and V. T. Hai. AKQ: A Hybrid Quantum-Classical Image Encryption System. RIVF International Conference on Computing and Communication Technologies (RIVF), Hanoi, Vietnam, 2023, pp. 527-532
5. Z. Qu and H. Sun. A Secure Information Transmission Protocol for Healthcare Cyber Based on Quantum Image Expansion and Grover Search Algorithm. IEEE Transactions on Network Science and Engineering, 2023, 10(5), pp. 2551-2563.
6. R. W. Wardhani, D. S. C. Putranto, T. -T. -H. Le, J. Ji and H. Kim. Toward Hybrid Classical Deep Learning-Quantum Methods for Steganalysis. IEEE Access, 2024, 12, pp. 45238-45252.
7. Amirkhanova, D. S., Iavich, M., & Mamyrbayev, O. Lattice-Based Post-Quantum Public Key Encryption Scheme Using ElGamal's Principles. Cryptography, 2024, 8(3), 31.
8. Rajan, A. A. QMedShield: A Novel Quantum Chaos-based Image Encryption Scheme for Secure Medical Image Storage in the Cloud. arXiv preprint arXiv:2405.09191, 2024.
9. Karmakar, J., Nandi, D. & Mandal, M.K. A novel hyper-chaotic image encryption with sparse-representation based compression. Multimedia Tools Application, 2020, 79, 28277–28300.
10. Y. Wang, L. Chen, K. Yu and T. Fu. A Secure Spatio-Temporal Chaotic Pseudorandom Generator for Image Encryption. IEEE Transactions on Circuits and Systems for Video Technology, 2024, 34(9), pp. 8509-8521.
11. C. He, Z. Chen, X. Sun and L. Wang. An Algorithm Based on Hodgkin-Huxley Model and Latin Square for Image Encryption. IEEE Access, 2023, 11, pp. 34163-34174.
12. M. Shahbaz Khan et al. Chaotic Quantum Encryption to Secure Image Data in Post Quantum Consumer Technology. IEEE Transactions on Consumer Electronics, 2024, 70(4), pp. 7087-7101.
13. T. Zhang and Y. Ma. Stable Image Encryption Algorithm Based on Expanded One-Dimensional Chaotic Jumping and Parallel Encoding Operation Grouping. IEEE Access, 2023,11, pp. 108746-108760.
14. M. Gong, X. Chai, Y. Lu and Y. Zhang. Exploiting Four-Dimensional Chaotic Systems With Dissipation and Optimized Logical Operations for Secure Image Compression and Encryption. IEEE Transactions on Circuits and Systems for Video Technology, 2024, 34 (8) pp. 7628-7642.
15. Zhang T, Ma Y. Stable image encryption algorithm based on expanded one-dimensional chaotic jumping and parallel encoding operation grouping. IEEE Access. 2023, 11, pp. 108746-60.
16. Abd El-Latif, A. A., Almousa, M., & Abd-El-Atty, B. A robust image encryption scheme based on quantum walks and dynamic DNA for secure cloud applications. IEEE Access, 2025.