Post-Quantum Cryptography-Based Multimedia Encryption Communication Scheme in IoT Consumer Electronics

K. B. Aneesh Kumar, *Member, IEEE*, L. S. Mohith, Kurunandan Jain, Prabhakar Krishnan, *Senior Member, IEEE*, Natarajan Venkatachalam, *Member, IEEE*, and Rajkumar Buyya, *Fellow, IEEE*

***Abstract*—Data, especially image data, is transmitted at an incredible rate due to the exponential growth in the number of connected devices brought about by the fast development of consumer electronics. Data transmission security remains fundamental in effective communication systems, especially with the emergence of the quantum era. Quantum advancements challenge traditional asymmetric cryptography, necessitating the requirement for new encryption schemes. The multimedia encryption schemes pose further challenges due to its large size, structural complexity, real-time requirements, and unique attack vectors specific to multimedia data. The current classical image encryption algorithms do not fully address the challenges posed by Quantum technology for securing the multimedia transmission. This paper proposes a hybrid framework combining Quantum Key Distribution (QKD), chaos-based encryption, and Post-Quantum Cryptography (PQC) to secure multimedia data, particularly images, in IoT consumer electronic networks. Integrating 2D-Logistic Sine Coupling Map (2D-LSCM), initialized with the Keys generated from QKD, and NTRU algorithm, this scheme achieves robust security and efficient performance. This new architecture improves processing speeds and enhances specificity and sensitivity values, fortifying chaotic map performance. Our experimental results and comprehensive security analysis demonstrate the security and performance of the framework. Correlation Analysis using Person correlation coefficient, with a nearing zero value, ensures the confidentiality of the encrypted image.**

***Index Terms*—Image encryption, chaos map, number theory research unit (NTRU), quantum key distribution (QKD), post quantum cryptography (PQC), key encapsulation method (KEM), Internet of Things (IoT), consumer electronics.**

I. Introduction

THE ADVANCEMENT of quantum technologies, particularly Shor's Algorithm, poses a significant threat to classical asymmetric cryptography, which is primarily based on the computational complexity of the prime factorization problem. The Shor's algorithm provides a quantum alternative that solves this problem in polynomial time, rendering asymmetric cryptographic algorithms like Diffie-Hellman, elliptic curve, and RSA insecure. With the exponential growth of consumer electronics in the IoT space, there is an increasing demand for data security to protect multimedia traffic, where traditional asymmetric encryption schemes are widely used for authentication, integrity protection, and key exchange. Quantum technologies can be used for man-in-the-middle interception of this traffic, which may result in integrity violations, fake authentication, and the exposure of exchanged keys. Additionally, multimedia encryption is challenging due to several factors. The large size of multimedia files demands significant computational resources, while their structural complexity—such as layers of metadata and encoded content—makes it difficult to apply standard encryption methods without disrupting file integrity. Real-time applications, like streaming and video conferencing, require encryption to be fast and efficient, adding pressure to balance security and performance. Furthermore, multimedia data has unique attack vectors, such as vulnerabilities in compression algorithms or patterns within content, which require encryption techniques tailored to protect against both general and content-specific threats. These complexities make multimedia encryption more difficult compared to traditional data encryption.

Quantum Key Distribution (QKD) offers a better alternative where quantum mechanical principles [6]—such as Heisenberg's uncertainty principle and the no-cloning theorem—to ensure secure and efficient exchange of security keys. However, QKD uses a combination of both quantum and classical channel for the final key derivation. Security lapses like lack of authentications or encryptions in traditional channels can open up users to multiple attacks including eavesdropping, man-in-the-middle attacks, and other security threats.

In addition to the QKD, there is another field that focus on the development of algorithms that are resistant to quantum

Received 21 December 2024; revised 19 February 2025 and 26 April 2025; accepted 17 May 2025. Date of publication 23 May 2025; date of current version 14 August 2025. *(Corresponding author: Kurunandan Jain.)*

K. B. Aneesh Kumar, L. S. Mohith, Kurunandan Jain, and Prabhakar Krishnan are with the Center for Cyber Security and Networks, Amrita Vishwa Vidyapeetham, Amritapuri Campus, Kollam 690525, India (e-mail: aneeshkb@am.amrita.edu; am.sc.p2mca24024@am.students.amrita.edu; kurunandanj@am.amrita.edu; kprabhakar@am.amrita.edu).

Natarajan Venkatachalam is with the Quantum Security Research Group, Society for Electronic Transactions and Security, Chennai 600113, India (e-mail: natarajan@setsindia.net).

Rajkumar Buyya is with the Quantum Cloud Computing and Distributed Systems Lab, School of Computing and Information Systems, The University of Melbourne, Melbourne, VIC 3010, Australia (e-mail: buyya@unimelb.edu.au).

Digital Object Identifier 10.1109/TCE.2025.3572949

computing attacks called Post Quantum Cryptography (PQC). These algorithms are designed to withstand the attacks from quantum algorithms like Shor's algorithm. In the context of multimedia encryption, PQC is particularly important as it ensures that sensitive multimedia content remains protected even in a post-quantum world. The key challenge in PQC is to create systems that can efficiently handle the large data sets associated with multimedia communications while remaining secure against future quantum threats

The Internet of Things (IoT) in consumer electronics refers to the network of devices, appliances, and gadgets that are connected to the Internet, allowing them to collect, exchange, and act on data. IoT technology enhances convenience, efficiency, and personalization, with applications in home automation, wearables, and smart entertainment. Devices like smartphones, wearables, smart home devices, and smart TVs are increasingly prevalent and handle sensitive data like health information and credit card details. If these devices use vulnerable cryptography, they could be at risk from quantum computers. Many IoT devices have long lifespans, meaning they could still be in use when quantum computers become powerful, raising concerns about data security in fields like homes, healthcare, finance, and education [32], [33]. As the number of connected devices grows exponentially over years, efficient data processing and management are crucial, prompting the development of better security solutions.

A new QKD framework with authentications and encryptions was proposed to handle conventional security issues associated with classical channel connecting QKD nodes. Hence, post quantum cryptographic algorithms are introduced for authentications and encryptions in classical channels. Authentication uses the Falcon [5] algorithm for the digital signature, while key encryption is done using the NTRU [2] algorithm. A digital signature is a cryptographic mechanism used to verify the authenticity and integrity of digital messages or documents. It provides assurance that the content has not been altered after it was signed and that it was indeed sent by the claimed sender. Unlike traditional algorithms such as RSA or ECC (Elliptic Curve Cryptography), NTRU uses mathematical problems based on lattice structures, which are believed to be hard even for quantum computers to solve. We propose a quantum-safe multimedia encryption scheme that utilizes the features of both NTRU and chaotic systems. The resulting scheme will enable the secured transmission of images in the Quantum world.

One of the most promising post quantum substitutes for the standard cryptography methods in terms of Key size, speed, ciphertext size for encryption, and key encapsulation mechanism, is a public key cryptosystem based on Nth-degree Truncated-polynomial Ring Units (NTRU) [2]. Similarly, Kyber, another lattice-based scheme, also provides strong security and fast encryption with compact key sizes, while schemes like McEliece (code-based cryptography) and SIDH (isogeny-based cryptography) are promising in offering quantum resistance, albeit with larger key sizes or slower speeds. Chaos-based encryption has emerged as a competitive alternative to conventional picture encryption algorithms thanks to developments in mathematical modeling and transformative techniques used on images. The chaotic system has several characteristics that make it suitable for encryption, including sensitivity, randomness, and ergodicity [19]. In chaos dependent encryption schemes, chaotic maps provide the sources of confusion and diffusion, which represent certain statistical measurements of the physical system.

However, encryption schemes based on chaotic maps are subject to certain drawbacks which include poorly chosen initial parameters applied to the chaos system which result in weak security due to less-than-optimal chaotic map. Secondly, insufficient integration of cryptographic primitives like confusion and diffusion necessitate additional transformative operations, which may reduce efficiency and security. Thirdly, when subjected to cryptanalysis, multiple chaos-based image encryption algorithms reveal deficiencies in their internal structure, thus lowering the algorithm's security [20]. Unfortunately, present picture encryption approaches do not consider image properties [13], and their corresponding algorithms also demand more system resources. The techniques suggested in the literature for the purpose of protecting images [35], [36] are not appropriate in the post quantum consumer electronics technology.

We make the following contributions to this research: We present a quantum-safe integrated chaos-based image encryption scheme that combines chaotic-map encryption with QKD communication protocols to ensure provable security and guarantee confidentiality in a zero-trust public cloud environment. By employing QKD authentications, we significantly reduce key consumption overheads. We also analyze the visual properties of encrypted images using this scheme and compare them with other notable chaotic system-based image encryption methods. In the context of universally composable security, we offer a thorough security analysis of the entire quantum key generation process, highlighting the role of randomness in ciphertext data and ensuring confidentiality.

In this paper, we make the following key contributions: (i) We propose a novel, hybrid multimedia encryption architecture that combines Quantum Key Distribution (QKD), the chaos-based 2D-Logistic Sine Coupling Map (2D-LSCM), and the lattice-based Post-Quantum Cryptography (PQC) algorithm NTRU, specifically tailored for secure image transmission in IoT consumer electronics. (ii) We introduce an authenticated encryption framework for classical QKD channels using Falcon digital signatures and NTRU encryption, effectively mitigating man-in-the-middle vulnerabilities. (iii) We demonstrate enhanced security against statistical and differential attacks, as verified by key sensitivity, entropy, and correlation coefficient analyses. (iv) We conduct extensive performance benchmarking against standard post-quantum encryption schemes, confirming the efficiency and scalability of our solution across various image resolutions. (v) We present a fully reproducible simulation framework using Python and QuNetSim, and validate our scheme on standard datasets from the USC-SIPI database.

The remaining of the paper is structured as follows: Section II provides a technological background and an overview of related works. In Section III, we propose our

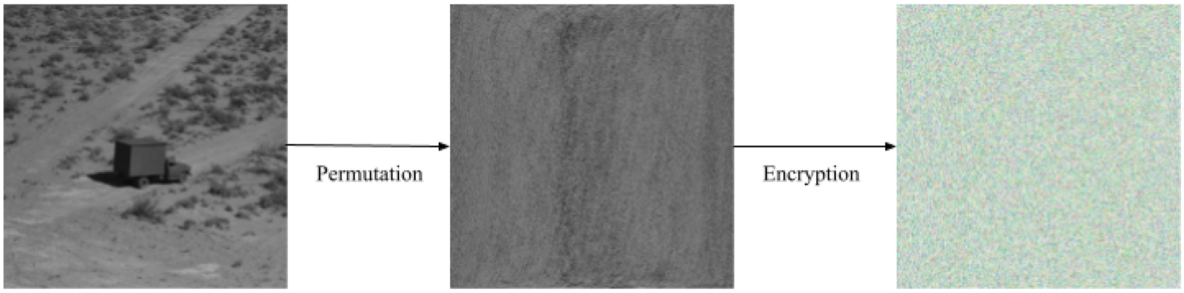


Fig. 1. Visualization of the stages of Chaos map-based encryption scheme.

novel architecture and chaos-map-integrated QKD scheme for image encryption. Section IV details the experimental data, performance evaluations, and analysis. Finally, Section V concludes with discussions of potential directions for further research.

II. Background and Literature Review

This section will give an overview of technologies and related works to solve the problem. We will look into chaotic map-based image encryption and discuss why a new algorithm is needed to overcome current security issues, followed by a brief overview of quantum communication and post-quantum cryptography. A detailed study of several papers on chaotic maps-based image encryption and NTRU is done to identify the security and performance aspects, and how we approach the problem will be discussed in this section.

A. Chaotic Map-Based Image Encryption

Chaotic systems are characterized by sensitivity, randomness, ergodicity, and non-periodicity. In cryptography, sensitivity is particularly valuable because it makes the system highly unpredictable. For instance, even small changes to a cryptographic key or initial parameters can lead to completely different ciphertexts. The randomness is essential for generating encryption keys, initialization vectors (IVs), and ciphertexts that are difficult to predict. It strengthens encryption systems by ensuring that even identical data encrypted multiple times will have different ciphertexts, preventing pattern recognition and attacks, and ensuring the confidentiality of the data. Without randomness, encryption systems would be vulnerable to attacks that exploit predictable patterns in the cipher text Ergodicity guarantees that chaotic systems can produce a broad range of unpredictable outputs, which is critical for creating diverse and secure keys or ciphertexts that are tough to break. Additionally, chaotic systems do not repeat their outputs, unlike periodic systems, which follow a fixed cycle. This non-periodicity ensures that the system's output is irregular and lacks discernible patterns, making it resistant to attacks such as frequency analysis or known-plaintext attacks that depend on pattern recognition.

One of the earliest image encryption schemes using chaotic systems was proposed by Fredrich [21], utilizing baker's chaotic maps on two-dimensional systems for confusion and diffusion (See Figure 1). The method employed "row-wise nonlinear feedback registers" to distribute pixel changes. However, subsequent cryptanalysis [20] revealed structural vulnerabilities, allowing recovery of image data from cipher images. Guan et al. [19] proposed a chaos-based image encryption technique combining Arnold's cat map for pixel shuffling and Chen's chaotic system [19] for encryption. This method integrates 1D and 3D chaotic systems to enhance randomness and achieve confusion and diffusion through repeated scrambling and rotation. The scheme demonstrated strong resistance to differential attacks, validated by high NPCR and UACI scores. Most existing chaotic image encryption algorithms focus on a single domain, such as diffusion or confusion, and often suffer from non-optimal initial conditions, leading to deterministic chaos maps. To overcome the security flaws in the existing techniques, we thus want an encryption scheme that adds uncertainty and diffusion to the algorithm.

B. Quantum Cryptography

Quantum cryptography was first proposed by Shor (1983) [29] and later by Bennett and Brassard (1984) [30]. As quantum computing threatens traditional public-key cryptography, various quantum cryptographic methods have emerged, including Quantum Digital Signatures for secure message authentication, Quantum Secret Sharing (QSS) for sharing secrets, and Quantum Public-Key Cryptography for quantum-resistant encryption. A prominent method, Quantum Key Distribution (QKD), securely generates and distributes symmetric keys between users, offering information-theoretic security (ITS) based on quantum physics. QKD has been demonstrated in real-world applications, such as satellite communication and fiber optic networks, and its scalability is improving. A typical QKD protocol involves encoding random binary bits into quantum states over a quantum channel, followed by post-processing to derive a symmetric key through a classical protocol, including key sifting, reconciliation, and error correction [31]. A generic QKD protocol contain two procedures (See Figure 2). In the first procedure random binary bits are encoded as quantum states and send it over a quantum channel. The second procedure is called post processing, where a classical post processing protocol is used to derive a symmetric key from the raw bits. The post processing message exchange happens through an authenticated classical channel. The post processing procedure in general include key sifting, key reconciliation, parameter estimation, error correction and privacy amplification [31].

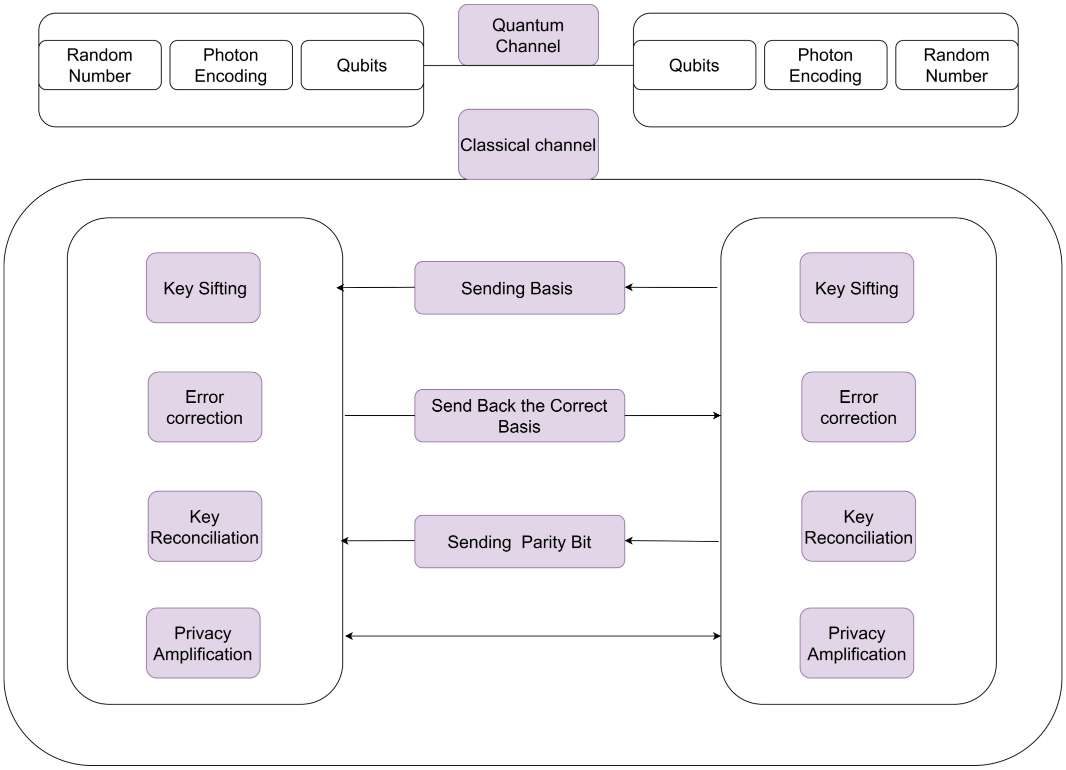


Fig. 2. Framework of quantum key distribution.

C. Post Quantum Cryptography

The implementation of quantum cryptography is necessary in order to ensure the safety of post-quantum computing systems [34]. Post-quantum cryptography (PQC), or quantum-safe encryption, resists quantum computers' cryptanalytic capabilities. PQC employs lattice-based, code-based, multivariate-based, supersingular isogeny-based, and hybrid algorithms within traditional cryptographic infrastructures [28]. NIST is standardizing PQC algorithms, focusing on security, cost, and implementation simplicity. These include public key encryption schemes [26] and digital signatures, with NTRU noted for its resistance to full-timing attacks and high performance [26]. NTRU also supports IoT devices, outperforming ECC and RSA in performance and energy efficiency for constrained environments [27].

Xu et al. proposed a Bit-Level Image Encryption technique using Piecewise Linear Chaotic Maps (PWLCM) [14]. Jain et al. [8] enhanced security for medical image transfer using multiple chaotic maps, while Naseer et al. [10] introduced colored image encryption via permutations and substitutions. Cowper et al. [3] developed a chaos-based multimedia encryption scheme using the BB84 protocol for quantum key generation. However, poor chaotic performance increases vulnerability to attacks, particularly in secure communications and chaos-based ciphers [22]. Ergodic chaotic maps mitigate risks by distributing outputs more broadly on the phase plane, highlighting the need for robust chaotic designs [23].

Efforts to improve chaotic systems often modify existing ones but achieve limited success [24]. For 1-dimensional maps, researchers proposed a dynamic parameter-control chaotic system (DPCCS) for enhanced performance [25]. In quantum image encryption, Wang et al. [13] suggested using polarized photons or quantum keys for data exchange, but this method is vulnerable due to classical channel security issues. Alternative approaches encrypt images by layering and encoding them in a binary tree structure [16], [17].

III. Proposed QKD Scheme

Lack of authentication and encryption are major security vulnerabilities in conventional channel communications, leading to various attacks, including eavesdropping and man-in-the-middle attacks. QKD includes both the classical channel, which processes post-data, and the quantum channel, which sends photons. There could be a man-in-the-middle attack if the classical channel is not verified. Eve serves as an intermediary (adversary) by pretending to be a trustworthy source. The attacker executes man-in-the-middle attack by interfering with the quantum channel and reestablishing connection between the two trusted parties. Basis sifting, error correction verification, sending random numbers for privacy amplification, and final key verification are QKD operations that need authentication. Both parties must mutually verify one another in QKD.

We designed a new QKD framework with PQC algorithms to address security concerns. Both QKD and PQC are emerging fields of research aimed at designing, developing, and implementing solutions for enterprise usage. Researchers are employing various methods to enhance key rates and security by combining QKD and PQC schemes. The integration of

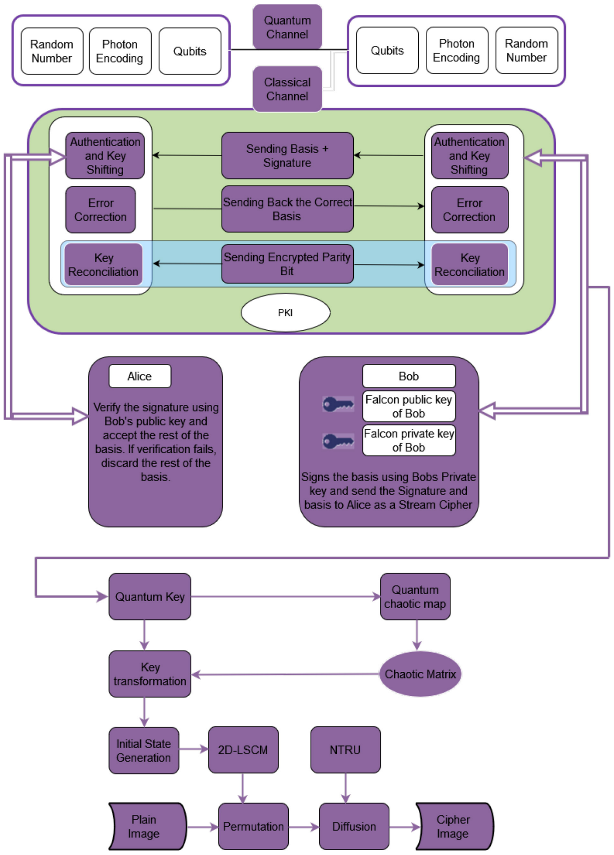

Random Number
Photon Encoding
Qubits
Quantum Channel
Classical Channel
Qubits
Photon Encoding
Random Number
Authentication and Key Shifting
Sending Basis + Signature
Authentication and Key Shifting
Error Correction
Sending Back the Correct Basis
Error Correction
Key Reconciliation
Sending Encrypted Parity Bit
Key Reconciliation
PKI
Alice
Verify the signature using Bob's public key and accept the rest of the basis. If verification fails, discard the rest of the basis.
Bob
Falcon public key of Bob
Falcon private key of Bob
Signs the basis using Bobs Private key and send the Signature and basis to Alice as a Stream Cipher
Quantum Key
Quantum chaotic map
Key transformation
Chaotic Matrix
Initial State Generation
2D-LSCM
NTRU
Plain Image
Permutation
Diffusion
Cipher Image

Fig. 3. Multimedia encryption Scheme.

these two schemes provides robust security and mitigates risks posed by quantum computers. Quantum-safe algorithms authenticate the QKD channel through PKI initially.

The study of NIST's final three encryption and digital signature schemes, both theoretical and practical, demonstrated that the Falcon Digital Signature Scheme offers the smallest private key size, the smallest public key size, and the fastest signing and verification times. Consequently, Falcon was used to provide authentication for the classical channel.

Additionally, NTRU is the oldest algorithm capable of replacing RSA while maintaining a manageable key size. Therefore, NTRU was selected to serve as the encryption provider for the classical channel. These considerations led to the adoption of the NTRU encryption scheme and the Falcon digital signature system to deliver authenticated encryption (See Figure 3) over the classical channel [11].

We implemented NTRU encryption in the Key Reconciliation step to address privacy issues arising during that phase. During this step, the transmitter, Alice, and the receiver, Bob, partition the qubits into several blocks and use the cascade protocol to compute the parity information for each block. Alice and Bob encrypt the data using each other's NTRU public keys before sending it to the receiving side. This ensures that the parity information is not sent in its raw form during the exchange. On the receiving end, the receiver decrypts the data using their NTRU private key.

During the key reconciliation process, this approach prevents information leakage. Moreover, Privacy Amplification is unnecessary for classical channel communication since the privacy of parity data can be secured during reconciliation, thereby eliminating the need for this phase. As a result, authentication and encryption in the classical channel significantly enhance its communication security. We have opted this improved QKD framework for the multimedia encryption technique which resulted in an increase in the overall level of security of the communication (See Figure 4(a)).

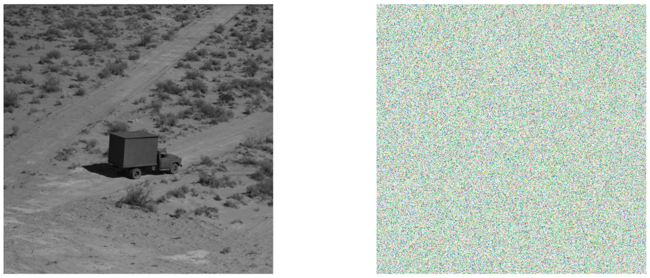

(a) Plain Image (b) Encrypted Image

Fig. 4. Plain and encrypted images.

A. Two-Dimensional Logistic Sine Coupling Map (2D-LSCM)

Logistic and Sine Maps are examples of 1D chaotic maps, that can be combined to produce 2D-chaotic maps. When these maps are considered individually, they both have some disadvantages like simple behavior and weak chaotic intervals. However, to overcome this a combination of these chaotic maps was introduced to develop a new chaotic map called 2D-LSCM, which produces quite a complex chaotic behavior [7]. The 2D-LSCM chaotic map is defined as follows where θ is the controlling parameter and has a range from 0 to 1.

$$x_i + 1 = sin(\pi(4\theta xi(1-xi)+(1-\theta)sin(\pi yi))) \tag{1}$$

$$y_i + 1 = sin(\pi(4\theta yi(1-yi)+(1-\theta)sin(\pi xi+1))) \tag{2}$$

The Quantum Chaotic Map can generate pseudo-random numbers sequences of high quality. Moreover, it is more sensitive compared to other chaotic maps and has a complex, chaotic behavior that can provide high security to the encrypted data [15]. It is defined as follows:

$$X_{n+1}+1 = r\Big(X_n - |X_n|^2\Big) - \text{ rY}_n \tag{3}$$

$$Y_{n+1} = -Ye^{-2\beta} + e^{-\beta} r\Big[\Big(2 - X_n - X_n{}^*\Big)Y_n\Big] \tag{4}$$

$$+e^{-\beta}r\Big[-X_nZ_n{}^* - X_n{}^*Z_n\Big] \tag{5}$$

$$Z_{n+1} = -Ze^{-2\beta}+e^{-\beta}r\Big[\Big(1-X_n{}^*\Big)Z_n - 2X_nY_n - X_n\Big] \tag{6}$$

Here r is the controlling parameter, and X_n* and Z_n* are defined as complex conjunction of X and Z. The value X ranges from $(0, 1)$, and Y ranges from $(0, 0.1)$. The value of Z ranges from $(0, 0.2)$ and β values is in the range of $[6, +\infty]$. The controlling parameter r can be in the range of $[0, 4]$.

Algorithm 1: Permutation Phase Using 2D-LSCM

```
Require: Image matrix $I$ of size $M \times N$, Key $K$
Ensure: Permuted image matrix $I'$
Generate 2D-LSCM chaotic map $C$ using key $K$
for each pixel $(x, y) \in I$ do
    Compute new positions $(x', y')$ using $C$
    Assign $I'(x', y') = I(x, y)$
end for
return $I' = 0$
```

Algorithm 2: NTRU Encryption Phase

```
Require: Permuted image matrix $I'$, NTRU public key $PK$
Ensure: Encrypted image matrix $E$
Initialize NTRU encryption
for each pixel $(x, y) \in I'$ do
    Convert pixel value to polynomial representation
    Encrypt using NTRU:
    $E(x, y) = \text{NTRU\_Encrypt}(I'(x, y), PK)$
end for
return $E = 0$
```

Algorithm 3: NTRU Decryption Phase

```
Require: Encrypted image matrix $E$, NTRU private key $SK$
Ensure: Decrypted image matrix $I'$
for each pixel $(x, y) \in E$ do
    Decrypt using NTRU:
    $I'(x, y) = \text{NTRU\_Decrypt}(E(x, y), SK)$
    Convert polynomial representation to pixel value
end for
return $I' = 0$
```

Algorithm 4: Reverse Permutation Phase Using 2D-LSCM

```
Require: Permuted image matrix $I'$, Key $K$
Ensure: Original image matrix $I$
Generate 2D-LSCM chaotic map $C$ using key $K$
for each pixel $(x', y') \in I'$ do
    Compute original position $(x, y)$ using $C$
    Assign $I(x, y) = I'(x', y')$
end for
return $I = 0$
```

IV. Proposed Algorithm

A. Multimedia Encryption Scheme

The proposed encryption scheme integrates Quantum Key Distribution (QKD), chaos-based encryption using the 2D-Logistic Sine Coupling Map (2D-LSCM), and Post-Quantum Cryptography (PQC) with NTRU encryption to secure multimedia data. The algorithm consists of three main phases:

- *Key Transformation:* Enhances randomness using chaotic sequences derived from quantum keys.
- *Permutation:* Employs 2D-LSCM to shuffle pixel values for confusion.
- *Diffusion:* Uses the NTRU encryption scheme to alter pixel values.

Let:

- Q: Raw quantum key from QKD,
- K: Chaotic sequence from Quantum Chaotic Map (QCM),
- $T(n)$: Transformed key stream,
- I: Original image matrix of size $M \times N$,
- P: Permuted image,
- E: Encrypted image matrix,
- $\mathcal{C}_{\text{2D-LSCM}}$: Permutation via 2D Logistic Sine Coupling Map,
- NTRU_{Enc}: NTRU encryption function,
- $\oplus$: Bitwise XOR operator.

Encryption is done by:

$$T(n) = (K(n) \cdot (K_i \oplus Q_i \bmod N)\ ) \oplus K(N-1) \quad (7)$$

$$P = \mathcal{C}_{\text{2D-LSCM}}(I, T) \quad (8)$$

$$E(x, y) = \text{NTRU}_{\text{Enc}}(P(x, y), \text{PK}) \quad (9)$$

The encrypted image is:

$$E = \left[E(x, y)\right]_{x=1, y=1}^{M,N} \quad (10)$$

Decryption is done by:

$$P(x, y) = \text{NTRU}_{\text{Dec}}(E(x, y), \text{SK}) \quad (11)$$

$$I = \mathcal{C}_{\text{2D-LSCM}}^{-1}(P, T) \quad (12)$$

Further explanation of each algorithm step can be found in the following section.

V. Methodology

A. Key Transformation

The key transformation phase enhances randomness in the quantum key, critical for secure image encryption. To address reduced randomness after classical channel communication, chaotic sequences from Quantum Chaotic Maps are used for key transformations. The map's initial condition is derived from the quantum key itself, as defined by the following equation:

$$T(n) = (K(n)(K_i \oplus Q_i \mod N)) \oplus K(N-1) \quad (13)$$

Here K indicates the random number sequence generated using a chaotic map, and Q indicates the quantum key. The variable N indicates the length of the key, and the length of the generated random number sequence is equal to the length of the quantum key.

B. Permutation Phase

To perform the Permutation, we use the chaotic matrix generated using 2D-LSCM. The key obtained from the key transformation phase is used as the initial condition of 2D-LSCM. Using 2D-LSCM, we generate a chaotic matrix that is used for performing the Permutation Phase.

The permutation phase works as follows:

- Consider a plain image of size $M \times N$, and we generate a chaos matrix $M \times N$.

Algorithm 5: Permutation Phase Using 2DLSCM

```
Function Permutation2DLSCM(image, Key):
    imwidth, imheight = get_dimensions(image)
    chaotic_map = generate_2DLSCM_map(imwidth,
      imheight, Key)
    for a in range(imwidth) do
        for b in range(imheight) do
            new_a, new_b = get_chaotic_map(a,
              b) permuted_image[new_a, new_b] =
              image[a, b]
        end
    end
return permuted_image
Function generate_2DLSCM_map(imwidth, imheight,
  Key):
    initialize_parameters(Key)
    map = create_empty_map(imwidth, imheight)
    for a in range(imwidth) do
        for b in range(imheight) do
            map[a, b] = logistic_sine_cosine_transform(a,
              b, Key)
        end
    end
return map
```

- Consider the plain image matrix as P and the chaotic matrix as S.
- Sort each column of S and obtain the index value to obtain matrix O
- The elements of O indicate the row position of the corresponding value; Fill the column position to obtain a position matrix PM.
- To shuffle the pixel values, choose the first row from PM and obtain the elements at these positions from S.
- Sort the selected values from S in ascending order and obtain the index value V.
- By using the newly obtained index value, shuffle the pixel values in P.
- Repeat steps from 6-8 for all rows of S to obtain the final permuted matrix.

C. NTRU Encryption

Diffusion is one of the most important steps in an encryption scheme in which, the actual alteration of the pixel values takes place. So, in the proposed image encryption scheme, diffusion is performed using the PQC algorithm NTRU. During the NTRU encryption, every pixel from the permuted matrix will be encrypted with the NTRU public key. The output from the NTRU encryption scheme is our final encrypted data. The fact that NTRU keys have a relatively larger key size than the classical encryption schemes make the encrypted data larger than the original image (Figure 4(b)). After the NTRU encryption, we convert the encrypted data to an RGB image which will add even more security to the encryption system.

- Generate the quantum Key with the QKD framework (authentication and encryption).
- Initialize the Chaotic Map using the quantum key.

Algorithm 6: NTRU Encryption Phase

```
Function NTRUEncrypt(image, Key):
    ntru_public_key, ntru_private_key =
      NTRU_KeyGen(Key)
    encrypted_image = empty_image(imwidth, imheight)
    for a in range(imwidth) do
        for b in range(imheight) do
            pixel_value = image[a, b] encrypted_pixel =
              NTRU_EncryptPixel(pixel_value,
              ntru_public_key)
            encrypted_image[a, b] = encrypted_pixel
        end
    end
return encrypted_image
Function NTRU_EncryptPixel(pixel_value,
  ntru_public_key):
    polynomial = encode_as_polynomial(pixel_value)
    encrypted_polynomial = NTRU_Encrypt_Polynomial
      (polynomial, ntru_public_key)
return encrypted_polynomial
```

- Generate the random number sequence using the Quantum Chaotic Map.
- Using the Quantum key and generated random number sequence perform the Key Transformation.
- The output from the Key Transformation phase is used to generate the initial condition of the chaotic map 2D-LSCM.
- Using the chaotic map 2D-LSCM, generate a chaotic matrix.
- Convert the input gray-scale image to an image matrix
- Using the chaotic matrix, perform permutation on the image pixel values.
- The output from the permutation box is provided as the input to the diffusion Phase.
- Encrypt the image pixels from the permutation phase using NTRU public key.
- The output from the NTRU encryption scheme is converted to an RGB image.

VI. Performance Evaluation

The system and simulation requirements that were utilised to implement the method have been detailed in this section. Along with the suggested scheme's time and space complexity in comparison to traditional pre-quantum encryption methods, several security assessments including key sensitivity analysis, Shannon entropy analysis, histogram analysis, and differential attack analysis have also been examined.

A. Testing Methodology and Data Availability

The framework of the proposed scheme was developed in Python. QuNetSim simulator was employed for simulating QKD network and integrating the chaos-map algorithm into the PQC quantum key generation algorithm. The quantum key generated from the QuNet simulator is used to perform

Algorithm 7: NTRU Decryption Phase

```
Function NTRUDecrypt(encrypted_image, ntru_private_key):
    imwidth, imheight = get_dimensions(encrypted_image)
    decrypted_image = empty_image(imwidth, imheight)
    for a in range(imwidth) do
        for b in range(imheight) do
            encrypted_pixel = encrypted_image[a, b] decrypted_pixel = NTRU_DecryptPixel(encrypted_pixel, ntru_private_key)
            decrypted_image[a, b] = decrypted_pixel
        end
    end
return decrypted_image
Function NTRU_DecryptPixel(encrypted_pixel, ntru_private_key):
    polynomial = NTRU_Decrypt_Polynomial(encrypted_pixel, ntru_private_key)
    pixel_value = decode_from_polynomial(polynomial)
return pixel_value
```

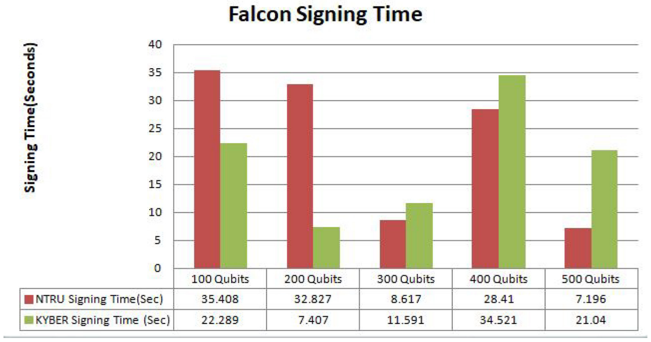


Fig. 5. Falcon signing time.

multimedia encryption [1], [4]. The images used for evaluating the proposed method are sourced from the USC-SIPI database. The datasets used and examined in this research work are accessible in the USC-SIPI database repository, https://sipi.usc.edu/database/ [12].

B. Falcon Signing Time and Verification Time

Falcon is used for authenticating both parties in the classical channel of QKD as a digital signature system for authenticated encryption (See Figure 3) [11]. Optimized for rapid signing and verification, Falcon is ideal for applications like financial transactions, with signing times in milliseconds to seconds and verification in microseconds to milliseconds. Its performance, influenced by message size, key size, implementation, and hardware, was compared with NTRU and Kyber in our research by measuring signing and verification times for different qubit sizes (See Figures 5 and 6).

Algorithm 8: Reverse Permutation Phase Using 2DLSCM

```
Function ReversePermutation2DLSCM(permuted_image, Key):
    imwidth, imheight = get_dimensions(permuted_image)
    chaotic_map = generate_2DLSCM_map(imwidth, imheight, Key)
    reversed_image = empty_image($im_width, im_height$)
    for a in range(imwidth) do
        for b in range(imheight) do
            original_a, original_b = find_original_position(a, b, imwidth, imheight, chaotic_map)
            reversed_image[original_a, original_b] = permuted_image[a, b]
        end
    end
return reversed_image
Function find_original_position(x, y, imwidth, imheight, chaotic_map):
    for i in range(imwidth) do
        for j in range(imheight) do
            if chaotic_map[i, j] == (x, y) then
                return (new_i, new_j)
            end
        end
    end
```

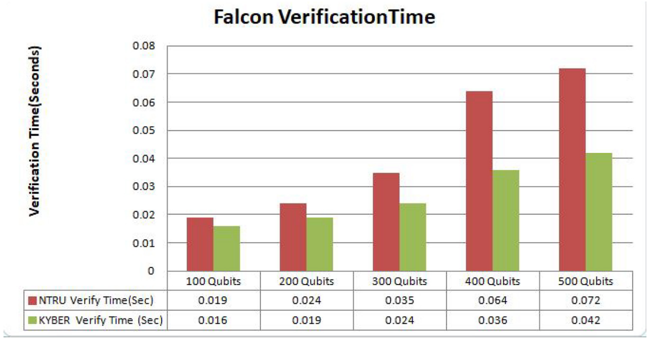


Fig. 6. Falcon verification time.

C. Security Analysis

To evaluate the proposed scheme's efficiency and security, we conducted comprehensive analyses and compared it with PWLCM and Logistic-Tent Chaotic Map encryption schemes due to the absence of quantum-safe alternatives.

Key Sensitivity Analysis: Testing with keys differing by a single bit (K1 and K2) showed less than 0.5% similarity between encrypted images (Table I), demonstrating superior sensitivity compared to PWLCM and Logistic-Tent schemes.

Shannon Entropy Analysis: The scheme achieved entropy values near the optimal 8-bit threshold for 8-bit images (Table II), confirming strong randomness and security comparable to traditional methods.

Histogram Analysis: Encrypted images exhibited uniform pixel distribution (Figures 7 and 8), indicating robustness

TABLE I
LITERATURE REVIEW

Citation	Author(s)	Title	Key Attributes
[5]	Pierre-Alain Fouque et al.	Falcon: Fast-Fourier lattice-based compact signatures over NTRU	Post-Quantum Signature scheme using Lattices
[7]	Zhongyun Hua et al.	2D Logistic-Sine-coupling map for image encryption	Chaotic map based Image encryption
[8]	Kurunandan Jain, Aravind Aji, and Prabhakar Krishnan	Medical image encryption scheme using multiple chaotic maps	Arnold's Cat map, 2DLSCM
[9]	Maithili S Jha et al.	A survey on quantum cryptography and quantum key distribution protocols	Analysis of BB84, BB92, SARG04 and other QKD protocols
[10]	Yasir Naseer et al.	A novel hybrid permutation substitution base colored image encryption scheme for multimedia data	RGB Image encryption using S-P boxes and 3D Mixed Chaotic maps.
[13]	Bo Wang et al.	Research on the improved algorithm for image quantum encryption in multimedia networks	Image diffusion using 2DLSCM, and scrambling using chaotic maps
[14]	Lu Xu et al.	A novel bit-level image encryption algorithm based on chaotic maps	Image encryption using Binary bitplane decomposition and PWLCM chaotic map
[15]	Jian Zhang and Da Huo	Image encryption algorithm based on quantum chaotic map and DNA coding	Logistic chaotic map, Quantum chaotic map, Lorenz chaotic map
[16]	Jinlei Zhang et al.	Quantum image encryption based on quantum image decomposition	Gray-scale Image to Quantum state and subsequent encryption
[17]	Ri-Gui Zhou et al.	Quantum image encryption and decryption algorithms based on quantum image geometric transformations	Translation of gray-scale images to quantum states, encryption and decryption
[18]	Zhongyun Hua et al.	Cosine-transform-based chaotic system for image encryption	Using CTBCS to generate chaotic maps such as LSC, STC and TLC
[19]	Zhi-Hong Guan et al.	Chaos-based image encryption algorithm	Combining Arnold's Cat Map & Chen's chaotic system
[20]	Eric Yong Xie et al.	On the cryptanalysis of fridrich's chaotic image encryption scheme	Cryptanalysis of [27], image recovery
[21]	Jiri Fridrich	Symmetric ciphers based on two-dimensional chaotic maps	Baker's chaotic map, row-wise nonlinear feedback registers

TABLE II
RESULT OF KEY SENSITIVITY ANALYSIS

Images (Pixels)	PWLCM Encryption (Percentage)	Logistic-Tent Map Encryption (Percentage)	Proposed Encryption Scheme (Percentage)
Cat	0.3914	0.3770	0.2578
Truck	0.3769	0.4101	0.2073
Aeroplane	0.3892	0.3986	0.4002
Landscape	0.3662	0.4132	0.2892
Moon	0.4883	0.3903	0.3423

against statistical cryptanalysis. Plain and encrypted image histograms were distinctly different.

As seen in Figures 7 and 8, the frequency spikes present in the plain image has been distributed across multiple color channels, effectively removing the chance of creating a mapping between plain and encrypted pixels.

$$NPCR = \frac{\sum_{i,j} D(i,j) \times 100}{W \times H} \tag{14}$$

$$UACI = \left(\sum_{i,j} \frac{|P(i,j) - Q(i,j)|}{W \times H \times M} \right) \times 100 \tag{15}$$

D. Encryption Time Analysis

The time taken to encrypt an image is a critical metric for evaluating the efficiency of encryption schemes, especially in real-time applications such as IoT and consumer electronics. The table below compares encryption times for different image sizes.

The proposed encryption scheme integrates NTRU and QKD, ensuring post-quantum security while maintaining competitive encryption times compared to other post-quantum cryptographic methods.

E. NPCR and UACI Analysis

The Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are two metrics used to evaluate resistance against differential attacks. Higher NPCR and UACI values indicate robustness against slight modifications in plaintext images.

The values in Table V confirm that the proposed encryption scheme achieves complete randomness in pixel distribution, making it highly resilient to differential attacks.

Resistance to Differential Attacks: Using NPCR (Number of Pixel Change Rate) and UACI (Unified Average Change Intensity) metrics, the scheme demonstrated resistance to differential attacks. The above formulae are used to compute the NPCR and UACI values. Let P and Q be two images

TABLE III
RESULT OF SHANNON ENTROPY ANALYSIS

Images (Pixels)	**PWLCM Encryption (bits)**	**Logistic-Tent Map Encryption (bits)**	**Proposed Method Encryption (bits)**
Cat	7.0505	7.9496	6.1358
Truck	7.9478	7.9478	6.9001
Aeroplane	7.9482	7.9482	5.7005
Landscape	7.9834	7.9279	7.0452
Moon	7.9234	7.9378	6.9039

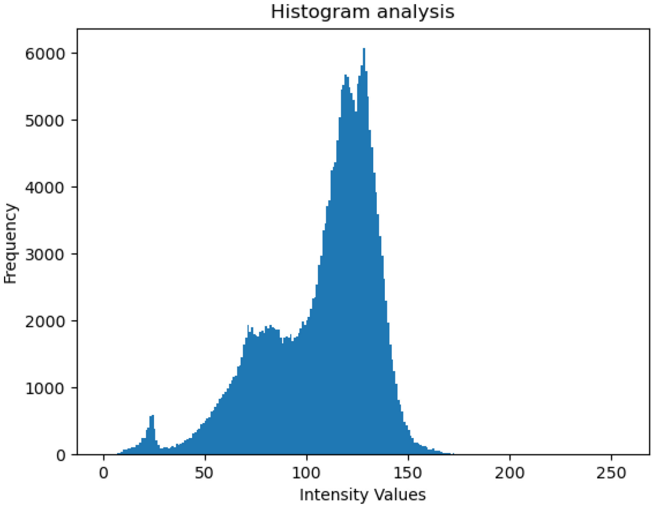


Fig. 7. Histogram of plain image.

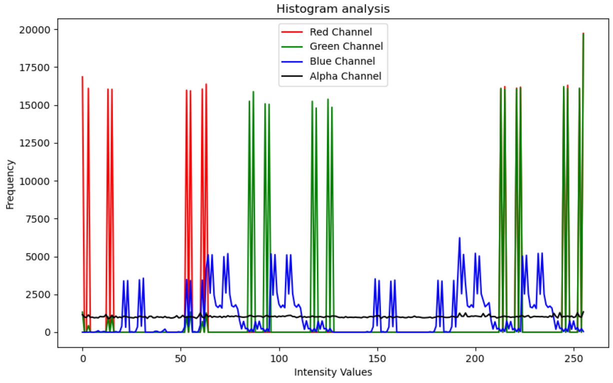


Fig. 8. Histogram of encrypted image.

the $P(i,j)$ and $Q(i,j)$ indicate the $(i,j)th$ pixels of the image P and Q. The values of W indicate the width H the height. Finally, M indicates the maximum value of an image pixel in the images P and Q, respectively. NPCR values reached 100%, with encrypted images in RGBA format entirely differing from grayscale plain images. UACI values exceeded 35%, affirming strong encryption noise. Results across various image sizes (128×128 to 1024×1024) are presented in Table III.

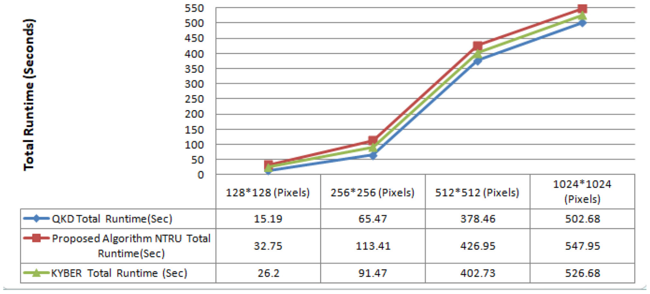
These findings confirm that the proposed scheme outperforms classical alternatives and is resistant to differential and statistical attacks.

TABLE IV
ENCRYPTION TIME COMPARISON

Image Size (Pixels)	Proposed Scheme (ms)	Kyber+QKD (ms)
128x128	1.35	1.21
256x256	2.49	2.30
512x512	4.87	4.56
1024x1024	9.85	9.20

TABLE V
NPCR AND UACI VALUES OF THE PROPOSED SCHEME

Image	NPCR (%)	UACI (%)
Cat	100.00	43.60
Truck	100.00	39.92
Aeroplane	100.00	45.68
Moon	100.00	41.55
Landscape	100.00	43.30



	128*128 (Pixels)	256*256 (Pixels)	512*512 (Pixels)	1024*1024 (Pixels)
QKD Total Runtime(Sec)	15.19	65.47	378.46	502.68
Proposed Algorithm NTRU Total Runtime(Sec)	32.75	113.41	426.95	547.95
KYBER Total Runtime (Sec)	26.2	91.47	402.73	526.68

Fig. 9. Comparison of performance for the proposed encryption scheme.

F. Performance Analysis

The performance of the suggested algorithm (utilizing NTRU) was evaluated by measuring the overall runtime for the image encryption and decryption of various sizes. The runtime was evaluated against various techniques, including standard Quantum Key Distribution (QKD) and Kyber combined with QKD throughout the encryption and decryption stages (Figure 9). The outcomes are promising, as the performance of Kyber and NTRU is nearly indistinguishable. However, the performance of both is slightly lower than standard QKD due to the minor overhead introduced by integrating NTRU into the QKD classical channel. Despite this, NTRU is an exceptional choice for applications necessitating both security and speed, as it can be integrated into the QKD classical channel with minimal performance degradation.

Correlation analysis was conducted to examine the relationship between adjacent pixel values in images to evaluate the effectiveness of the encryption scheme. In plaintext images, adjacent pixels typically exhibit a high degree of correlation

TABLE VI
RESULT OF DIFFERENTIAL ANALYSIS

Images (Pixels)	PWLCM NPCR (Percentage)	Logistic-tent map NPCR (Percentage)	Proposed Encryption scheme NPCR (Percentage)	PWLCM UACI (Percentage)	Logistic-tent map UACI (Percentage)	Proposed Encryption scheme UACI (Percentage)
Cat	99.6147	99.6185	100.00	33.4063	33.4361	43.6065
Truck	99.6399	99.6199	100.00	33.5850	33.5581	39.9261
Aeroplane	99.6012	99.6045	100.00	33.4935	33.4585	45.6885
Moon	99.5850	99.7020	100.00	32.6800	33.5750	41.5526
Landscape	99.5120	99.6790	100.00	33.7880	32.2020	43.3073

TABLE VII
PERFORMANCE OF THE PROPOSED ENCRYPTION SCHEME (MEMORY)

Image Size (Pixels)	Memory consumption of the proposed encryption scheme (Percentage)
128 × 128	40%
256 × 256	46%
512 × 512	62%
1024 × 1024	70%

due to natural continuity in visual data. In ciphertext images, an effective encryption algorithm disrupts this continuity, resulting in significantly lower correlation. This disruption indicates successful randomization of pixel values, enhancing the security of the encrypted image. The Pearson correlation coefficient is used to quantify this relationship, with values closer to zero in ciphertext images indicating a successful encryption process (Figures 10 and 11).

Table IV presents the memory consumption for different image sizes using the proposed encryption scheme. The memory required to store an encrypted image depends on several factors:

1) Image Size: Larger images require more memory.
2) Security Level: More secure encryption algorithms demand additional memory to store encrypted images.
3) Scheme Implementation: The proposed scheme typically requires less memory than RSA and AES, making it ideal for applications with limited memory, such as mobile devices and embedded systems.

In the simulated environment, the Python implementation of NTRU showed higher encryption times. However, this anomaly is unlikely to occur in real-world implementations, as NTRU is one of the fastest post-quantum cryptographic (PQC) schemes. Additionally, the scheme has an excellent security-to-performance ratio, which mitigates any performance depreciation. The slightly higher memory usage observed may be attributed to the lack of optimization in the code.

VII. CONCLUSION AND FUTURE WORK

The proposed quantum-safe multimedia encryption technique combines Chaos and the NTRU public key cryptosystem to develop a secure image encryption scheme. By integrating the proven security of chaotic encryption with NTRU's quantum-resistant properties, alongside a novel QKD framework with built-in authentication and encryption, the scheme ensures robust image transmission in quantum environments. Encoding encrypted grayscale images into RGB further strengthens data protection.

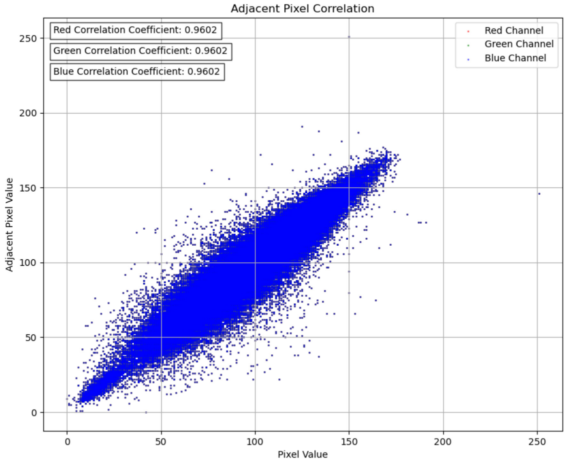


Fig. 10. Correlation of Plaintext Image.

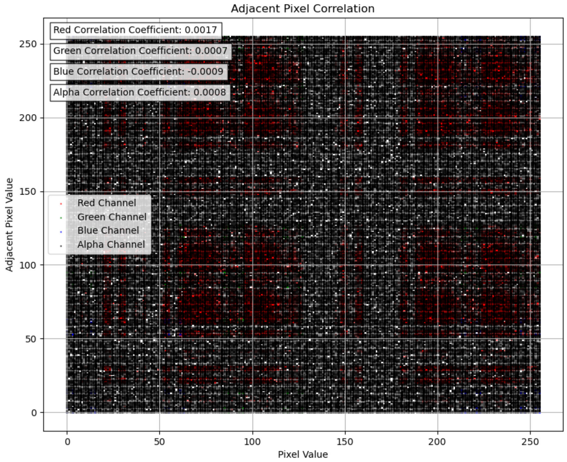


Fig. 11. Correlation of Ciphertext Image.

This implementation is practical and hardware-independent, making it suitable for real-world applications especially with the exponential growth in the consumer electronic devices. Beyond image encryption, it holds potential for securing other multimedia data, promoting the adoption of quantum-safe cryptography. As quantum technology advances, this scheme offers a reliable solution for secure multimedia transmission, supporting the widespread use of quantum-safe practices in the area of consumer electronics.

Although the proposed scheme demonstrates robust encryption performance, future research can explore several enhancement avenues. First, integration with emerging lightweight PQC primitives could reduce computational overhead, making the framework even more suitable for ultra-constrained IoT devices. Second, expanding the scheme to handle other multimedia formats—such as audio, video, and 3D models—could increase its utility in broader consumer electronic applications. Third, hardware implementations using FPGAs or ASICs should be explored to validate real-time feasibility and energy efficiency. Fourth, developing a decentralized quantum-safe key management framework for dynamic IoT environments could further strengthen end-to-end security. Finally, extending the scheme to support adaptive encryption—where security parameters change in real-time based on threat context—could be a promising direction in evolving quantum threat landscapes.

References

[1] A. Aji, K. Jain, and P. Krishnan, "A survey of quantum key distribution (QKD) network simulation platforms," in *Proc. 2nd Global Conf. Adv. Technol. (GCAT)*, 2021, pp. 1–8.

[2] B. Clark, *Understanding the NTRU Cryptosystem*, Williams Honors College, Akron, OH, USA, 2019.

[3] N. Cowper, H. Shaw, and D. Thayer, "Chaotic quantum key distribution," *Cryptography*, vol. 4, no. 3, p. 24, 2020.

[4] S. Diadamo, J. Nötzel, B. Zanger, and M. M. Beşe, "QuNetSim: A software framework for quantum networks," *IEEE Trans. Quant. Eng.*, vol. 2, pp. 1–12, Jun. 2021.

[5] P.-A. Fouque et al., "Falcon: Fast-Fourier lattice-based compact signatures over NTRU," Submission to the NIST's Post-Quantum Cryptography Standardization Process, 2018.

[6] A. B. Al-Ghamdi, A. Al-Sulami, and A. O. Aljahdali, "On the security and confidentiality of quantum key distribution," *Secur. Privacy*, vol. 3, no. 5, p. e111, 2020.

[7] Z. Hua, F. Jin, B. Xu, and H. Huang, "2D Logistic-Sine-coupling map for image encryption," *Signal Process.*, vol. 149, pp. 148–161, Aug. 2018.

[8] K. Jain, A. Aji, and P. Krishnan, "Medical image encryption scheme using multiple chaotic maps," *Pattern Recognit. Lett.*, vol. 152, pp. 356–364, Dec. 2021.

[9] M. S. Jha, S. K. Maity, M. K. Nirmal, and J. Krishna, "A survey on quantum cryptography and quantum key distribution protocols," *Int. J. Adv. Res. Ideas Innov. Technol*, vol. 5, pp. 144–147, Jan. 2019.

[10] Y. Naseer, T. Shah, and D. Shah, "A novel hybrid permutation substitution base colored image encryption scheme for multimedia data," *J. Inf. Secur. Appl.*, vol. 59, Jun. 2021, Art. no. 102829.

[11] A. Prakasan, K. Jain, and P. Krishnan, "Authenticated encryption in the quantum key distribution classical channel using post-quantum cryptography," in *Proc. 6th Int. Conf. Intell. Comput. Control Syst. (ICICCS)*, 2022, pp. 804–811.

[12] "USC-SIPI image database Website." 2021. Accessed: Aug. 8, 2022. [Online]. Available: http://sipi.usc.edu/ database/database.php

[13] B. Wang, J. Xu, and H. Song, "Research on the improved algorithm for image quantum encryption in multimedia networks," *Comput. Elect. Eng.*, vol. 62, pp. 414–428, Aug. 2017.

[14] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," *Optics Lasers Eng.*, vol. 78, pp. 17–25, Mar. 2016.

[15] J. Zhang and D. Huo, "Image encryption algorithm based on quantum chaotic map and DNA coding," *Multimedia Tools Appl.*, vol. 78, no. 11, pp. 15605–15621, 2019.

[16] J. Zhang, Z. Huang, X. Li, M. Wu, X. Wang, and Y. Dong, "Quantum image encryption based on quantum image decomposition," *Int. J. Theor. Phys.*, vol. 60, no. 8, pp. 2930–2942, 2021.

[17] R. G. Zhou, Q. Wu, M. Q. Zhang, and C. Y. Shen, "Quantum image encryption and decryption algorithms based on quantum image geometric transformations," *Int. J. Theor. Phys.*, vol. 52, no. 6, pp. 1802–1817, 2013.

[18] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Inf. Sci.*, vol. 480, pp. 403-419, Apr. 2019.

[19] Z. H. Guan, F. Huang, and W. Guan, "Chaos-based image encryption algorithm," *Phys. Lett. A*, vol. 346, no. 1–3, pp. 153–157, 2005.

[20] E. Y. Xie, C. Li, S. Yu, and J. Lü, "On the cryptanalysis of Fridrich's chaotic image encryption scheme," *Signal Process.*, vol. 132, pp. 150–154, Mar. 2017.

[21] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcat. Chaos*, vol. 8, no. 6, pp. 1259–1284, 1998.

[22] D. Arroyo, R. Rhouma, G. Alvarez, S. Li, and V. Fernandez, "On the security of a new image encryption scheme based on chaotic map lattices," *Chaos Interdiscipl. J. Nonlin. Sci.*, vol. 18, no. 3, 2008, Art. no. 33112.

[23] H. Hu, Y. Xu, and Z. Zhu, "A method of improving the properties of digital chaotic system," *Chaos Soliton. Fract.*, vol. 38, no. 2, pp. 439–446, 2008.

[24] R. Bose and S. Pathak, "A novel compression and encryption scheme using variable model arithmetic coding and coupled chaotic system," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 53, no. 4, pp. 848–857, Apr. 2006.

[25] Z. Hua and Y. Zhou, "Dynamic parameter-control chaotic system," *IEEE Trans. Cybern.*, vol. 46, no. 12, pp. 3330–3341, Dec. 2016, doi: 10.1109/TCYB.2015.2504180.

[26] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A ring-based public key cryptosystem," in *Proc. ANTS*, 1998, pp. 267–288.

[27] I. Upasana, N. Nandanavanam, A. Nandanavanam, and N. Naaz, "Performance characteristics of NTRU and ECC cryptosystem in context of IoT environment," in *Proc. IEEE Int. Conf. Distrib. Comput. VLSI Electr. Circuits Robot. (DISCOVER)*, 2020, pp. 23–28.

[28] R. Alleaume, "Using quantum key distribution for cryptographic purposes: A survey," 2007, *arXiv:quant-ph/0701168*.

[29] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, 1994, pp. 124–134, doi: 10.1109/SFCS.1994.365700.

[30] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst. Signal Process.*, 1984.

[31] M. Mehic, M. Niemiec, H. Siljak, and M. Voznak, "Error reconciliation in quantum key distribution protocols," in *Reversible Computation: Extending Horizons of Computing* (Lecture Notes in Computer Science 12070), I. Ulidowski, I. Lanese, U. Schultz, and C. Ferreira, Eds., Cham, Switzerland: Springer, 2020.

[32] K. N. Singh, N. Baranwal, O. P. Singh, and A. K. Singh, "SIELNet: 3-D chaotic-map-based secure image encryption using customized residual dense spatial network," *IEEE Trans. Consum. Electron.*, vol. 69, no. 4, pp. 862–868, Nov. 2023.

[33] H. K. Singh and A. K. Singh, "Using deep learning to embed dual marks with encryption through 3-D chaotic map," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 3056–3063, Feb. 2024.

[34] K. K. Singamaneni, G. Muhammad, and Z. Ali, "A novel multi-qubit quantum key distribution ciphertext-policy attribute-based encryption model to improve cloud security for consumers," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 1092–1101, Feb. 2024.

[35] R. Chaurasia and A. Sengupta, "Retinal biometric for securing jpeg-codec hardware ip core for ce systems," *IEEE Trans. Consum. Electron.*, vol. 69, no. 3, pp. 441–457, Aug. 2023.

[36] B. B. Gupta, A. Gaurav, and V. Arya, "Secure and privacy-preserving decentralized federated learning for personalized recommendations in consumer electronics using blockchain and homomorphic encryption," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 2546–2556, Feb. 2024.