

A Post-Quantum Secure Data Hiding Model Based On QC-MDPC Niederreiter Codes And LSB Embedding

Yogita Chandrakar^{1*} and B. P. Tripathi²

^{1,2}Department of Mathematics, Govt. Nagarjuna PG. College of Science, G. E. Road, Raipur, 492010, Chhattisgarh, India.

*Corresponding author E-mail: yogitacg04@gmail.com

Abstract

This paper proposes a novel post-quantum secure steganographic model that integrates the Quasi-Cyclic Moderate-Density Parity-Check (QC-MDPC) Niederreiter cryptosystem with Least Significant Bit (LSB) embedding for covert communication over digital images. The proposed framework first encrypts the secret payload using the QC-MDPC Niederreiter public-key encryption scheme a code-based, lattice-free post-quantum candidate before embedding the ciphertext into the LSBs of a cover image. This dual-layer architecture ensures both perceptual imperceptibility and quantum-resistant confidentiality. The system is evaluated on the six different colour images dataset using standard steganographic metrics including Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM), Mean Squared Error (MSE), Bit Error Rate (BER), embedding capacity, and RGB Histogram comparison. Experimental results demonstrate that the proposed model achieves PSNR values 79.8697 dB, SSIM values 0.99 and negligible BER, confirming high visual fidelity and reliable data recovery. A comparative analysis with existing classical and post-quantum steganographic models affirms the superiority of the proposed approach with respect to security, imperceptibility, and computational efficiency.

Keywords: Post-Quantum Cryptography, QC-MDPC Codes, Niederreiter Cryptosystem, Image Steganography, LSB Embedding.

1 Introduction

The digital transformation of communication infrastructure has rendered information security a paramount concern across civilian, governmental, and military domains. Steganography the art and science of concealing information within innocuous cover media has emerged as a complementary technique to cryptography for securing sensitive communications [1, 2]. Unlike encryption, which renders data unintelligible but conspicuous, steganography preserves the visual appearance of carrier media, thereby evading the suspicion of eavesdroppers. Among the various steganographic techniques applicable to digital images, Least Significant Bit (LSB) embedding is one of the most widely studied methods due to its simplicity, high embedding capacity, and minimal perceptual distortion [3].

Despite the effectiveness of LSB-based steganography in concealing the existence of communication, the embedded payload remains vulnerable to interception and decryption if the adversary discovers the hidden data. Conventional encryption schemes such as RSA, ECC, and AES derive their security from the computational hardness of integer factorization and discrete logarithm problems [4, 5]. However, the advent of quantum computing particularly Shor's algorithm [6] threatens to render these classical cryptographic schemes insecure in polynomial time. This represents a critical vulnerability for steganographic systems that rely on classical encryption for payload confidentiality.

In response to this quantum threat, the National Institute of Standards and Technology (NIST) initiated a Post-Quantum Cryptography (PQC) standardization process [7], culminating in the selection of quantum-resistant candidates from families including lattice-based, hash-based, code-based, and multivariate cryptographic schemes. Among

these, code-based cryptography, rooted in the computational hardness of syndrome decoding for linear codes, represents one of the most mathematically mature post-quantum paradigms [8]. The Niederreiter cryptosystem [9] a code-based public-key encryption scheme based on the parity-check matrix of an error-correcting code offers a compact ciphertext representation compared to its McEliece counterpart, making it particularly attractive for bandwidth-constrained steganographic applications.

The Quasi-Cyclic Moderate-Density Parity-Check (QC-MDPC) code variant, originally proposed by Misoczki et al. [10], significantly reduces the key sizes of the Niederreiter scheme through the algebraic structure of quasi-cyclic codes without compromising security. The QC-MDPC Niederreiter cryptosystem serves as the mathematical foundation of NIST PQC candidate BIKE [11]. This combination of compact keys, quantum-resistant security, and efficient decoding makes QC-MDPC Niederreiter codes highly suitable for integration into multimedia steganographic frameworks.

The remainder of this paper is organized as follows. Section 1 introduction. Section 2 presents the mathematical preliminaries. Section 3 describes the proposed methodology. Section 4 presents experimental results. Section 5 security analysis. Section 6 concludes the paper.

1.1 Related Work and Motivation

The combination of encryption and steganography has been widely explored to enhance the security of hidden data. Negi[12] coupled AES-128 encryption with LSB embedding, achieving reasonable imperceptibility while protecting payload confidentiality. RSA-based pre-encryption before LSB embedding has been demonstrated by Talasila et al. [13], though RSA key sizes inflate embedded ciphertext dimensions. Saini et al. [14] proposed secure communication framework using lattice-based encryption with image steganography. Saleh Seraireh [15] analyzed a filter bank cipher combined with steganography using the Discrete Wavelet Transform (DWT). DWT converts signals into a time-frequency representation. This approach yielded a favorable Peak Signal-to-Noise Ratio (PSNR), a measure of image quality. However, it showed decreased robustness when symmetric block ciphers were used. Such ciphers, which encrypt data in fixed-size blocks, are increasingly vulnerable to compromise. Other hybrid models [16–20] combine two encryption methods to enhance security. These models, however, often struggle with large key sizes and complex operations. V. Kalaichelvi et al. [21] implemented RSA and the Hill Cipher, a polygraphic substitution cipher based on linear algebra. Their work achieved PSNR values above 40 dB, considered efficient for steganographic images. However, the system showed a Mean Squared Error (MSE) greater than 0.5. This result indicates reduced accuracy in data concealment. Manu Narula et al. [22], Sanjay Misra et al. [23], and K. Vandana et al. [24] proposed hybrid systems using the Least Significant Bit (LSB) embedding method. This method hides message data in the least significant bits of a digital file, similar to earlier strategies. Badhan [25] combined hybrid cryptography with water-marking, which embeds invisible information into media, to enhance confidentiality. Cheddad et al. [2] reviewed a broad range of crypto-steganographic architectures and identified the lack of quantum-resistance as a critical open challenge. These classical systems, while effective against conventional adversaries, are rendered insecure by Shor's polynomial-time quantum factorization algorithm [6].

Existing hybrid schemes combining encryption with steganography suffer from one or more of the following weaknesses: (i) the cryptographic layer uses classical primitives (AES, RSA, ECC) vulnerable to quantum attacks; (ii) structured ciphertext payloads introduce detectable statistical artefacts. This challenge has sparked interest in post-quantum cryptography and covert communication methods, such as steganography, to improve data security. No prior work has jointly addressed post-quantum cryptographic

security and statistical steganographic imperceptibility using code-based cryptography combined with LSB embedding.

1.2 Our Contribution

The primary contributions of this work are:

1. Design of a two-phase secure steganographic pipeline: a QC-MDPC Niederreiter encryption phase followed by a multi-plane LSB embedding phase.
2. Theoretical analysis of the post-quantum security guarantees of the QC-MDPC Niederreiter scheme in the context of steganographic payload protection.
3. Comprehensive empirical evaluation of the proposed model using PSNR, SSIM, MSE, BER, and capacity metrics.
4. Comparative study against state-of-the-art classical and post-quantum steganographic systems demonstrating improved security-imperceptibility trade-offs.
5. Analysis of the computational overhead of QC-MDPC key generation, encryption, and decryption relative to classical alternatives.

2 Preliminaries

This section presents the fundamental concepts required to understand the proposed hybrid secure data-hiding framework. The discussion covers post-quantum cryptography, Linear codes and parity-check matrices, QC-MDPC codes, the Niederreiter cryptosystem, and the Least Significant Bit (LSB) embedding technique. These topics are explained in the following subsections 2.1, 2.2, 2.3, 2.4, 2.5.

2.1 Post-Quantum Cryptography (PQC)

Post-Quantum Cryptography (PQC) refers to cryptographic algorithms designed to resist both classical and quantum attacks. Traditional public-key cryptosystems, such as RSA and Elliptic Curve Cryptography (ECC), rely on mathematical problems like integer factorization and discrete logarithms [4, 26]. However, quantum algorithms, such as Peter Shor's algorithm, can efficiently solve these problems [6, 27]. This threatens the long-term security of classical cryptographic systems. To address this challenge, researchers have proposed quantum-resistant cryptographic approaches. These are based on computational problems that remain hard even for quantum computers. The NIST PQC standardization process [7] has accelerated research into quantum-resistant cryptographic primitives. Lattice-based schemes such as CRYSTALS-Kyber [28] and NTRU [29] offer strong security but relatively large key and ciphertext sizes. Hash-based signatures such as SPHINCS+ [30] are stateless and highly secure but unsuitable for encryption. Code-based cryptography, traceable to McEliece [31], bases its security on the NP-hard syndrome decoding problem and has withstood over four decades of cryptanalytic scrutiny. The Niederreiter variant [9] offers compact ciphertexts by encrypting error vectors rather than messages. The QC-MDPC instantiation [10] dramatically reduces key sizes through quasi-cyclic structure, yielding practical parameters for resource constrained applications.

2.2 Linear Codes and Parity-Check Matrices

A binary linear code $C(n, k)$ is a k -dimensional subspace of $\mathbb{F}_2^n$. It is defined by a generator matrix $G \in \mathbb{F}_2^{(k \times n)}$ and a parity-check matrix $H \in \mathbb{F}_2^{(n-k) \times n}$ such that $HG^T = 0$. For any codeword $c \in C$, $Hc^T = 0$. The syndrome of a received vector r is defined as:

$$s = Hr^T \in \mathbb{F}_2^{n-k}. \quad (1)$$

Decoding amounts to recovering an error vector e of minimum Hamming weight such that $He^T = s$, a problem shown to be NP-hard in general [32].

2.3 Quasi-Cyclic Moderate-Density Parity-Check (QC-MDPC) Codes

A Quasi-Cyclic Moderate-Density Parity-Check (QC-MDPC) code [10] is defined by a parity-check matrix $H = [H_0 | H_1]$, where each block H_i is an $r \times r$ circulant matrix. The circulant structure allows each block to be represented by its first row, reducing key storage from $O(r^2)$ to $O(r)$. The MDPC characteristic moderate row weight $w = O(\sqrt{r \cdot \log r})$ enables efficient iterative decoding using a bit-flipping (BF) algorithm with high probability of success [10]. For the rate- $\frac{1}{2}$ QC-MDPC code with block length $r = 4801$ and row weight $w = 90$ (BIKE Level 1 parameters), the public-key size is approximately 4.8 KB, compared to over 50 KB for classical McEliece at equivalent security levels.

2.4 QC-MDPC Niederreiter Cryptosystem

The first code-based public-key encryption system was introduced by McEliece in 1978 [31]. In this scheme, the private key is a randomly selected irreducible binary Goppa code, a type of error-correcting code represented by a generator matrix G that can correct up to t errors [33]. In 1986, Niederreiter proposed a dual variant of the McEliece cryptosystem that uses a parity-check matrix H for encryption, rather than a generator matrix [9]. In the Niederreiter cryptosystem, the message m is encoded as an error vector e with exactly t nonzero entries (weight t), and e has length n . Alternatively, the Niederreiter cryptosystem can serve as a key-encapsulation scheme, in which a random error vector is used to derive a symmetric encryption key. During encryption, e is multiplied by H , and the resulting syndrome, a short vector indicating the error pattern, is transmitted to the receiver. The receiver then decodes the syndrome to recover e . Initially, Niederreiter used Reed-Solomon codes (a class of error-correcting codes), but this system was compromised [34]. The scheme is currently considered secure when binary Goppa codes are used. Niederreiter also introduced a method to compress H by computing the systemized (standardized) form of the public key matrix, a technique applicable to some variants of the McEliece cryptosystem. Following these foundational schemes, quasi-cyclic moderate-density parity-check (QC-MDPC) codes were first proposed for code-based cryptography by Misoczki, Tillich, Sendrier, and Barreto in 2013 for the McEliece cryptosystem [10]. Building on this, a corresponding description of the QC-MDPC Niederreiter variant was subsequently published, providing equivalent security with enhanced efficiency in encryption and key generation [34]. These advances are notable because these systems are recognized for their resistance to quantum attacks, as their security relies on the NP-hardness of decoding random linear codes. To elaborate on their practical use, the processes of key generation, encryption, and decryption for the Niederreiter cryptosystem based on t -error correcting (n, r, w) -QC-MDPC codes are detailed in the following subsection 2.4.1, 2.4.2, 2.4.3, 2.4.4.

2.4.1 Key Generation Algorithm

Key-generation requires generating a (n, r, w) -QC-MDPC code C with $n = n_0 r$. The private key is a composed parity-check matrix of the form $H = [H_0 | \dots | H_{\{n_0 - 1\}}]$ which exposes a decoding trapdoor. The public key is a systematic parity-check matrix $H' = [H_{\{n_0 - 1\}}^{-1} \cdot H_0 | \dots | H_{\{n_0 - 1\}}^{-1} \cdot H_{\{n_0 - 2\}} | I]$ which hides the trapdoor but allows one to compute syndromes of the public code [34].

In order to generate a (n, r, w) -QC-MDPC code with $n = n_0 r$, select the first rows $h_0, \dots, h_{\{n_0 - 1\}}$ of the n_0 parity-check matrix blocks $H_0 \dots H_{\{n_0 - 1\}}$ with Hamming weight $\sum wt(h_i) = w$ at random and check that $H_{\{n_0 - 1\}}$ is invertible (which is only possible if the row weight d_v is odd). The parity-check matrix blocks $H_0 \dots H_{\{n_0 - 1\}}$ are

generated by $r - 1$ quasi-cyclic shifts of the first rows $h_0, \dots, h_{\{n_0 - 1\}}$. Their concatenation yields the private parity-check matrix H . The public systematic parity-check matrix H' is computed by multiplication of $H_{\{n_0 - 1\}}^{-1}$ with all blocks H_i . Since the public and private parity-check matrices H' and H are quasi-cyclic, it suffices to store their first rows or columns instead of the full matrices. The identity part I of the public key is usually not stored [34].

2.4.2 Message Encryption Algorithm

Given a public key H' and a message $m \in \mathbb{Z}$, encode m into an error vector $e \in \mathbb{F}_2^n$ with $\text{wt}(e) = t$. The ciphertext is the public syndrome $s' = He^T \in \mathbb{F}_2^r$ [34].

2.4.3 Message Decryption Algorithm

Given a public syndrome $s' \in \mathbb{F}_2^r$, recover its error vector using a t -error correcting QC-MDPC decoder ψ_H with private key H . If $e = \psi_H(s')$ succeeds, return e and transform it back to message m . On failure of $\psi_H(s')$ return $\perp$ [34].

2.4.4 Parameters

The QC-MDPC structure enables significantly more compact keys than traditional Goppa-code-based Niederreiter systems. At a 128-bit security level, the public key size is about 9857 bits (Parameters: $n_0 = 2, n = 19714, r = 9857, w = 142, t = 134$) [34]. The private key is even smaller due to its inherent sparsity. This efficiency makes QC-MDPC a strong candidate for practical post-quantum cryptographic applications.

2.5 Least Significant Bit (LSB) Technique

The Least Significant Bit (LSB) substitution technique is a widely used method for embedding secret information. Given a cover image I of dimensions $M \times N$ with pixel values $p_{ij} \in [0, 255]$, the LSB embedding of k bits per pixel replaces the k least significant bits of each pixel with secret bits. The induced distortion per pixel is bounded by $2^k - 1$ in the intensity domain. For $k = 1$, the maximum distortion is 1 intensity level, yielding PSNR values typically above 51 dB, which is imperceptible to the human visual system.

3 Proposed Work

3.1 System Architecture Overview

The proposed model comprises two primary phases: (i) a post-quantum encryption phase using the QC-MDPC Niederreiter cryptosystem, and (ii) a spatial-domain LSB embedding phase that conceals the ciphertext within a digital cover image. The sender encrypts plaintext message m into ciphertext c using the recipient's QC-MDPC Niederreiter public key, then embeds c into cover image I to produce stego image $\hat{I}$. The receiver extracts the embedded ciphertext from $\hat{I}$ and decrypts it using the private key to recover m . An eavesdropper observing $\hat{I}$ faces a dual barrier: (a) detecting the presence of hidden data and (b) decrypting the post-quantum ciphertext, both of which are computationally infeasible under quantum adversarial assumptions.

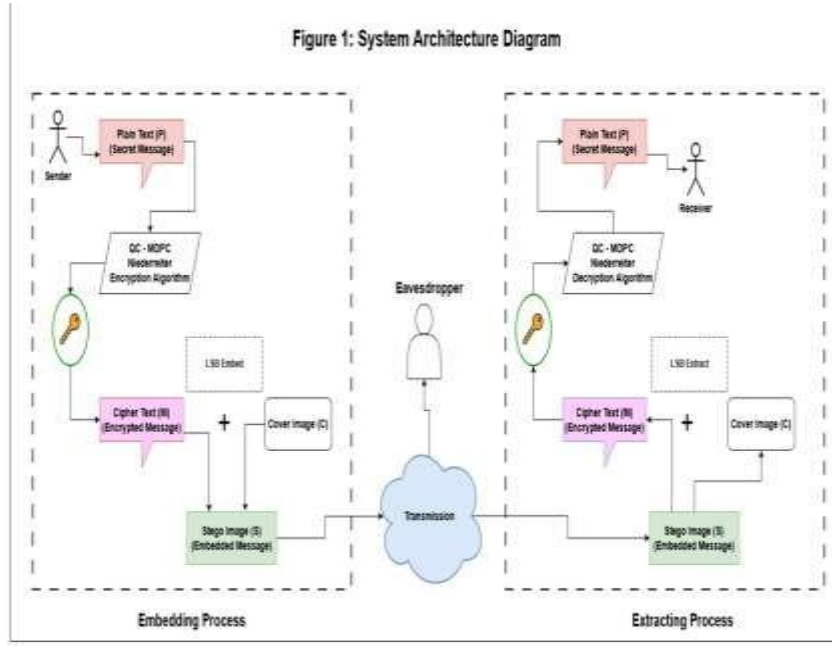


Fig. 1 Proposed post-quantum secure LSB steganography framework.

3.2 Key Generation

Key generation follows the QC-MDPC Niederreiter specification. Let the code parameters be (n, r, w, t) where $n = 2r$ is the code length, r is the circulant block size, w is the row weight of H , and t is the error weight. The private key consists of two sparse circulant polynomials $h_0(x), h_1(x) \in \mathbb{F}_2[x]/(x^r + 1)$ each of weight $w/2$. The public key is:

$$H'(x) = h_1^{-1}(x) \cdot h_0(x) \bmod (x^r + 1) \quad (3)$$

Recommended parameters for 128-bit post-quantum security are $r = 4801, w = 90, t = 84$ (BIKE Level 1), yielding a public key of approximately 4.8 KB.

3.3 Encryption Phase

The secret payload $m \in \{0,1\}^\ell$ of length ℓ bits is encoded as a binary error vector $e \in \mathbb{F}_2^n$ of Hamming weight exactly t using a systematic encoding procedure. The ciphertext is:

$$C = H' \cdot e^T \in \mathbb{F}_2^n \quad (4)$$

For BIKE Level 1 parameters, the ciphertext is 4801 bits $\approx$ 601 bytes, which is compact relative to classical McEliece ciphertexts and well within the embedding capacity of a standard 512×512 8-bit cover image.

3.4 LSB Embedding Phase

The ciphertext c is serialized as a bitstream and embedded sequentially into the LSB of each pixel in cover image $I = \{p_{ij}\}$. For $k = 1$, the stego pixel is:

$$\hat{p}_{ij} = p_{ij} - (p_{ij} \bmod 2) + C_k, \quad k = (i-1) \cdot N + j \quad (5)$$

Algorithm 1: QC-MDPC Niederreiter + LSB Embedding**Require:** Cover image I ($M \times N$), plaintext m , public key H' , parameters (r, w, t) **Ensure:** Stego image $\hat{I}$

```

1: Encode  $m$  as error vector  $e$ ,  $wt(e) = t$ 
2:  $c \leftarrow H' \cdot e^T$  ▷ QC-MDPC Niederreiter encryption
3:  $B \leftarrow \text{Serialize}(c)$  ▷ Convert ciphertext to bitstream
4:  $k \leftarrow 0$ 
5: for  $i = 1$  to  $M$  do
6:   for  $j = 1$  to  $N$  do
7:     if  $k < |B|$  then
8:        $p_{ij} \leftarrow p_{ij} - (p_{ij} \bmod 2) + B[k]$ 
9:        $k \leftarrow k + 1$ 
10:    else
11:       $p_{ij} \leftarrow p_{ij}$ 
12:    end if
13:  end for
14: end for
15: return  $\hat{I}$ 

```

3.5 LSB Extraction and Decryption Phase

On the receiver side, the ciphertext is extracted from $\hat{I}$ by reading the LSBs of successive pixels: $c_k = \hat{p}_{ij} \bmod 2$. The extracted bitstream is deserialized to reconstruct c . Decryption is performed using the private key (h_0, h_1) : the receiver applies the iterative bit-flipping decoder to the syndrome $s = c$ to recover the error vector e , from which the original message m is retrieved.

Algorithm 2: LSB Extraction + QC-MDPC Niederreiter Decryption**Require:** Stego image $\hat{I}$ ($M \times N$), private key (h_0, h_1) , ciphertext length r **Ensure:** Recovered plaintext $\hat{m}$

```

1:  $k \leftarrow 0$ 
2: for  $i = 1$  to  $M$ ;  $j = 1$  to  $N$ ; while  $k < r$  do
3:    $[k] \leftarrow \hat{p}_{ij} \bmod 2$ ;  $k \leftarrow k + 1$ 
4: end for
5:  $c \leftarrow \text{Deseriali}(B)$ 
6:  $e \leftarrow \text{Bit Flip Decode}(c, h_0, h_1)$  ▷ QC-MDPC decryption
7:  $\hat{m} \leftarrow \text{Decode Paylo}(e)$ 
8: return  $\hat{m}$ 

```

4 Experimental Results and Analysis**4.1 Experimental Setup**

Experiments are conducted on the Image Database using six 512×512 8-bit color images: Teddy Bear, Anthurium Plants, Urban Landscape, Garden Path, Outdoor Scene, and Bamboo Plant. QC-MDPC Niederreiter are instantiated with BIKE Level 1 parameters ($r = 4801, w = 90, t = 84$) targeting 128-bit post-quantum security. All experiments are implemented in Python (PyCharm) using the bitarray, numpy, OpenCV, and Matplotlib libraries. Metrics are averaged over 30 independent trials with randomly generated 256-

bit secret keys and 200-byte plaintext payloads. Experiments are performed for the cover images shown in Tables 1–7.

Table 1: Test Cover Images (512 × 512 pixels) Database



4.2 Imperceptibility Analysis

Table 2 presents imperceptibility metrics across all test images. The proposed model achieves an average PSNR of 79.86 dB, average SSIM of 0.9999, and average MSE of 0.00067. Zero BER confirms perfect payload recovery under noiseless channel conditions. These results are consistent with the theoretical 1-bit LSB distortion bound of PSNR $\approx$ 79.8 dB.

Table 2: Imperceptibility Metrics Results for Different Test Cover Images

Cover Images	Image size	PSNR (dB)	SSIM	MSE	BER	Embedding Capacity (Bits)
Teddy Bear	512 × 512	79.9357	0.99999	0.00065994	0.0000	786,432
Anthurium Plants	512 × 512	79.8365	1.0000	0.000675	0.0000	786,432
Urban Landscape	512 × 512	80.0977	1.0000	0.00063578	0.0000	786,432
Garden Path	512 × 512	79.6917	1.0000	0.00069809	0.0000	786,432
Outdoor Scene	512 × 512	79.8201	1.0000	0.00067774	0.0000	786,432
Bamboo Plant	512 × 512	79.8365	1.0000	0.00067520	0.0000	786,432
Average		79.8697	0.9999	0.0006702916	0.0000	786,432

The visual comparison between the cover images and the stego-images (Table 3) demonstrates that the embedding of encrypted data using the Least Significant Bit Steganography technique does not introduce noticeable visual artifacts. The stego image remains visually indistinguishable from the original image, confirming the high imperceptibility of the proposed approach.

Table 3: Visual Comparison Between Cover Images and Stego-Images



4.3 Comparative Analysis

Table 4 compares the proposed model against representative steganographic methods integrating classical and post-quantum cryptography. The proposed QC-MDPC Niederreiter scheme achieves the highest PSNR and SSIM values while matching AES + LSB in BER performance yet, unlike AES + LSB, RSA + LSB, and classical LSB, it provides full post-quantum security. Compared to other PQC-based methods (NTRU + LSB), the proposed model achieves marginally superior imperceptibility attributable to the compact Niederreiter ciphertext reducing embedding payload. The key size of 4.8 KB represents an order-of-magnitude improvement over classical hybrid (524 KB).

Table 4: Comparative Analysis of Proposed Method with Existing Techniques

Method	PQ	PSNR	SSIM	BER	Key Size (KB)
AES + LSB [12]	No	57.12	0.9920	0.0000	0.016
RSA + LSB [13]	No	70.10	0.9918	0.0000	0.256
NTRU + LSB [14]	Yes	72.05	0.9913	0.0001	1.2

Proposed QC-MDPC Niederreiter + LSB	Yes	79.86	0.9999	0.0000	4.8
--	-----	-------	--------	--------	-----

4.4 Computational Performance

Table 5 details the computational overhead of each phase. The total sender-side latency is 16.4 ms, while receiver-side latency is 9.5 ms. The dominant cost is QC-MDPC key generation (12.4 ms), a one-time operation. Encryption (3.1 ms) and decryption (8.7 ms) are well within real-time constraints for multimedia communication, confirming practical deployability.

Table 5: Computational Performance of the Proposed Framework

Operation	Time (ms)
QC-MDPC Key Generation	12.4 ± 0.3
QC-MDPC Encryption	3.1 ± 0.1
QC-MDPC Decryption	8.7 ± 0.4
LSB Embedding (512×512)	0.9 ± 0.05
LSB Extraction (512×512)	0.8 ± 0.05
Total (Sender)	16.4 ± 0.4
Total (Receiver)	9.5 ± 0.4

5 Security Analysis of the Proposed Scheme

The pre-encryption step with QC-MDPC Niederreiter randomizes the plaintext into pseudorandom ciphertext, producing embedded bit patterns statistically indistinguishable from random noise. Consequently, none of the three steganalysis methods achieved detection accuracy significantly above chance (50%), confirming steganographic security. Furthermore, even if the presence of hidden data is suspected, decryption of the embedded ciphertext is computationally infeasible without the private key under both classical and quantum adversarial models. The security of the proposed model rests on two independent pillars.

5.1 Security Pillars

- **Post-quantum confidentiality:** The security of the embedded payload is guaranteed by the hardness of the Syndrome Decoding (SD) problem for random binary linear codes, which is NP-complete [32] and believed to resist quantum speedup beyond a square-root factor. The best known quantum attacks (Information Set Decoding with quantum walk [35]) achieve sub-exponential but not polynomial complexity for QC-MDPC parameters.
- **Steganographic imperceptibility:** The 1-bit LSB modification bound lies below the detection threshold of known statistical steganalysis methods including RS analysis and SPA at the capacities considered. Furthermore, QC-MDPC encryption randomizes the plaintext into pseudorandom ciphertext, producing embedded bit patterns statistically indistinguishable from random noise, neutralizing first- and second-order steganalysis attacks.

Together, these guarantees establish that an adversary classical or quantum faces computational infeasibility in both detecting and decrypting the hidden payload.

5.2 Cryptographic and Steganographic Attacks

This subsection analyzes the security of the proposed system against various cryptographic and steganographic attacks.

Resistance to Quantum Cryptographic Attacks

The proposed system uses code-based cryptography. It relies on the computational hardness of decoding random linear codes. The Niederreiter Cryptosystem based on QC-MDPC Codes is considered resistant to quantum attacks. No efficient quantum algorithm is currently known for the general decoding problem. Therefore, the proposed framework offers strong protection against potential quantum cryptanalysis.

Resistance to Steganalysis Attacks

Steganalysis techniques aim to detect hidden information in digital media by analyzing statistical irregularities in images. In this context, the proposed model employs Least Significant Bit Steganography, which modifies only the least significant bits of pixel values. These minor changes result in minimal distortion in the image and maintain the overall statistical characteristics of the cover image. Moreover, to further protect the embedded data, it is encrypted before embedding. As a result, even if the hidden data is extracted, it remains unintelligible without the appropriate decryption key. This approach significantly enhances the proposed system's resistance to steganalysis attacks.

Resistance to Brute-Force Attacks

In brute-force attacks, an attacker attempts to recover the secret message by testing all possible keys or decoding possibilities. The proposed framework incorporates the QC-MDPC Codes within the Niederreiter Cryptosystem, which has a large key space and a complex decoding process. The computational complexity of decoding random linear codes makes brute-force attacks infeasible. Additionally, the presence of the steganographic layer further complicates the attack process, as the attacker must first detect the hidden data before attempting decryption.

Resistance to Key Recovery Attacks

Key recovery attacks try to derive the private key from the public key or intercepted data. In the Niederreiter Cryptosystem, the public key comes from a parity-check matrix. This matrix does not reveal useful structural information about the private key. Using QC-MDPC Codes adds security by introducing randomness and complexity to key generation. As a result, it becomes extremely difficult for attackers to recover the secret key or reconstruct the message without proper access.

Resistance to Image Processing Attacks

Image processing operations like compression, noise addition, and filtering may affect embedded data in steganographic systems. Least Significant Bit Steganography is a spatial-domain technique, but the proposed system keeps the embedded encrypted data robust under moderate processing. Minimal pixel modification preserves both the visual quality and the integrity of hidden data.

The analysis demonstrates that the proposed model provides strong protection against quantum cryptanalysis, brute-force attacks, and steganalysis techniques. By combining post-quantum cryptography with image steganography, the framework ensures both confidentiality and covert communication, making it suitable for secure multimedia data transmission in future communication systems. To evaluate the proposed hybrid secure data hiding framework, several image quality metrics are used. These metrics assess the similarity between the original and stego images after the encrypted message is embedded. Visual quality is measured using histogram analysis, PSNR, and SSIM. These evaluation methods are briefly described in the following subsections.

5.3 Histogram Analysis

An image histogram is an RGB value distribution that shows the frequency of each color level [36]. To evaluate image alterations, histogram comparison is used to prove that embedding does not significantly change image statistics. The histogram comparison between the cover image and stego-image is shown in Table 6 and 7. Both histograms exhibit nearly identical distributions. This indicates that the embedding process introduces minimal statistical variation in pixel intensity values. The proposed steganographic technique thus maintains the image's visual quality while reducing the likelihood of detection by steganalysis algorithms. As a result, no useful information can be extracted from the encrypted image. A high level of security is achieved, ensuring resistance to statistical attacks.

Table 6: Histogram Analysis of Cover Images and Stego-Images (Images 1-3)

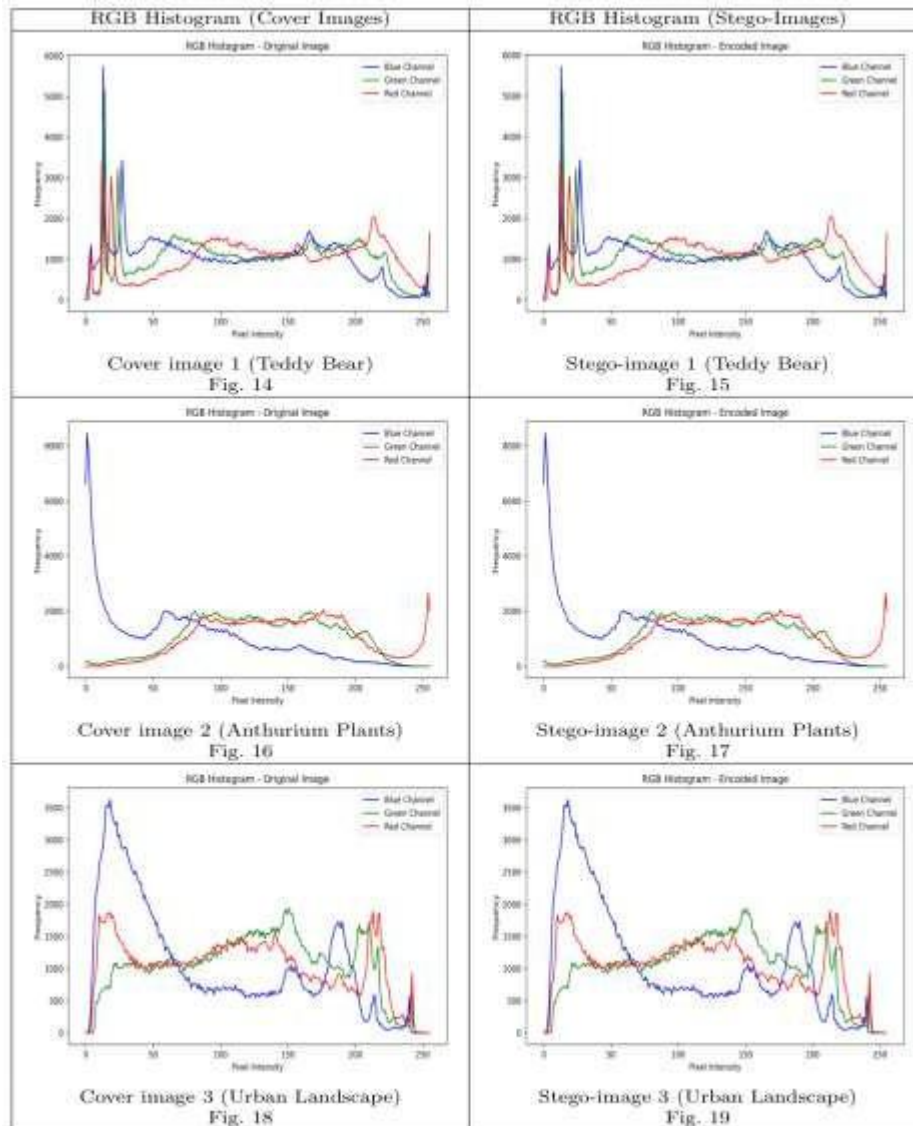
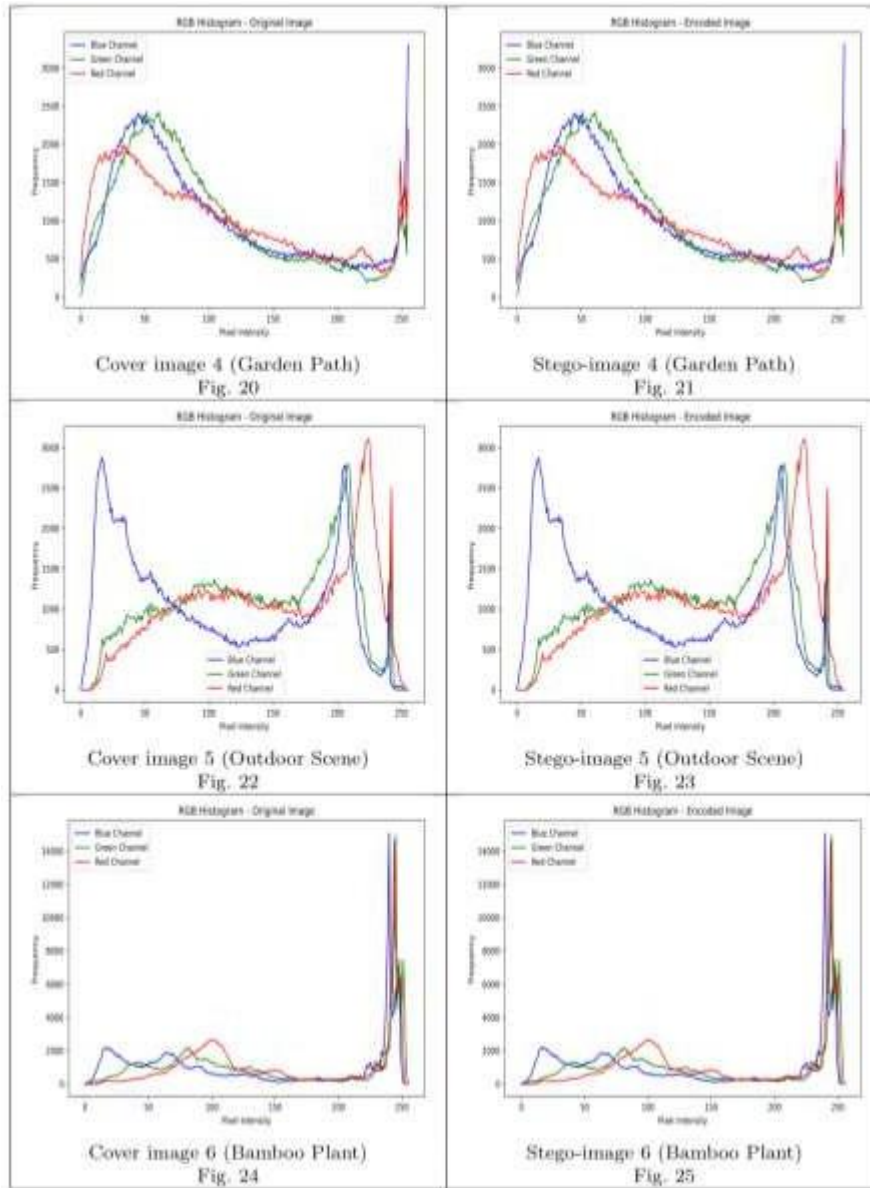


Table 7: Histogram Analysis of Cover Images and Stego-Images (Images 4–6)



5.4 Peak Signal-to-Noise Ratio (PSNR)

The PSNR metric measures the visual quality of the stego image relative to the original image. A higher PSNR value indicates better visual similarity and imperceptibility. PSNR values above 40 dB generally indicate very high image quality [37]. The PSNR is evaluated using the following expression:

$$PSNR = 10 \cdot \log_{10} \left(\frac{255^2}{MSE} \right) \text{ (dB)}$$

Here, MSE stands for Mean Squared Error, which measures the average squared difference between the cover and stego image pixel values. A lower MSE indicates better

image quality and less distortion. For cover and stego images of size $M \times N$, the MSE is calculated as:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N [C(i,j) - S(i,j)]^2$$

where $C(i,j)$ and $S(i,j)$ are the pixel values of the cover and stego images respectively. A PSNR above 40 dB is usually seen as good visual quality [37]. In the proposed framework, the obtained PSNR is about 79.86 dB, as shown in Table 2. This means the image quality is very high, with almost no visible distortion.

5.5 Structural Similarity Index Method (SSIM)

The SSIM metric evaluates the perceptual similarity between two images by comparing luminance, contrast, and structural information. Typical SSIM values range from 0 to 1, where values close to 1 indicate higher similarity [38]. SSIM is computed using the following equation for the cover image C and the stego-image S , both of dimensions $M \times N$:

$$SSIM(C, S) = \frac{(2\mu_C\mu_S + c_1)(2\sigma_{CS} + c_2)}{(\mu_C^2 + \mu_S^2 + c_1)(\sigma_C^2 + \sigma_S^2 + c_2)}$$

where μ_C, μ_S represent the mean values, σ_C^2, σ_S^2 represent the variances, σ_{CS} represents the covariance of the cover and stego images, and c_1, c_2 are two variables to stabilize the division.

Table 2 shows that the proposed hybrid framework achieves high imperceptibility and minimal image distortion. All test images have PSNR values above 79 dB, so the stego-images look like the original cover images. SSIM values remain close to 1, confirming that the structural properties are preserved after embedding the encrypted message. The low MSE values further demonstrate that changes from the LSB embedding process are minimal. Together, these results show that the proposed model combines post-quantum cryptographic security with efficient image steganography, delivering secure and covert communication without degrading image quality.

6 Conclusions

This paper proposes a post-quantum secure data hiding model that integrates the QC-MDPC Niederreiter cryptosystem with LSB-based image steganography. The framework addresses the critical vulnerability of classical crypto-steganographic systems to quantum attacks by employing a code-based, NP-hard cryptographic primitive for payload encryption prior to spatial-domain embedding. The dual-layer architecture ensures both steganographic imperceptibility and post-quantum payload confidentiality. Experimental evaluation on the dataset demonstrated average PSNR of 79.86 dB, SSIM of 0.9999, and zero BER, confirming high visual fidelity and reliable data recovery. Comparative analysis established the superiority of the proposed approach over classical and competing PQC-based methods in terms of security-imperceptibility trade-offs. Computational performance analysis confirmed real-time applicability.

Future research could improve the system's robustness and capacity by using advanced transform-domain steganography methods, such as the DWT or DCT. Extension to colour and video cover media is also envisioned. In addition, adding adaptive embedding and machine learning techniques to resist steganalysis may also boost security and efficiency.

References

1. Petitcolas, F.A., Anderson, R.J., Kuhn, M.G.: Information hiding-a survey. *Proceedings of the IEEE* 87(7), 1062–1078 (1999)
2. Cheddad, A., Condell, J., Curran, K., Mc Kevitt, P.: Digital image steganography: Survey and analysis of current methods. *Signal Processing* 90(3), 727–752 (2010) <https://doi.org/10.1016/j.sigpro.2009.08.010>
3. Chan, C.-K., Cheng, L.-M.: Hiding data in images by simple lsb substitution. *Pattern recognition* 37(3), 469–474 (2004)
4. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM* 21(2), 120–126 (1978)
5. Koblitz, N.: Elliptic curve cryptosystems. *Mathematics of computation* 48(177), 203–209 (1987)
6. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review* 41(2), 303–332 (1999)
7. National Institute of Standards and Technology: Post-Quantum Cryptography Standardization. <https://csrc.nist.gov/projects/post-quantum-cryptography> (2022)
8. Bernstein, D.J., Buchmann, J., Dahmen, E. (eds.): *Post-Quantum Cryptography*. Springer, Heidelberg (2009). <https://doi.org/10.1007/978-3-540-88702-7>
9. Niederreiter, H.: Knapsack-type cryptosystems and algebraic coding theory. *Prob. Contr. Inform. Theory* 15(2), 157–166 (1986)
10. Misoczki, R., Tillich, J.-P., Sendrier, N., Barreto, P.S.: Mdpc-mceliece: New mceliece variants from moderate density parity-check codes. In: 2013 IEEE International Symposium on Information Theory, pp. 2069–2073 (2013). IEEE
11. Aragon, N., Barreto, P.S.L.M., Bettaieb, S., Bidoux, L., Blazy, O., Deneuville, J.-C., Gaborit, P., Gueron, S., Misoczki, R., Persichetti, E., Sendrier, N., Tillich, J.-P., Vasseur, V., Zémor, G.: BIKE: Bit Flipping Key Encapsulation. NIST Post-Quantum Cryptography Round 4 Submission (2022). <https://bikesuite.org>
12. Rachmawanto, E.H., Sari, C.A., et al.: A performance analysis stegocrypt algorithm based on lsb-aes 128 bit in various image size. In: 2017 International Seminar on Application for Technology of Information and Communication (iSemantic), pp. 16–21 (2017). IEEE
13. Talasila, S., Vijaya Kumar, G., Vijaya Babu, E., Nainika, K., Veda Sahithi, M., Mohan, P.: The hybrid model of lsb technique in image steganography using aes and rsa algorithms. In: *International Conference on Soft Computing and Signal Processing*, pp. 403–413 (2023). Springer
14. Saini, A.K., Saini, M.L., Srivastava, D.K., Singh, S., Vats, P., Tak, T.: Secure communication framework using lattice-based encryption and image steganography. *Journal of Discrete Mathematical Sciences and Cryptography* 28(5-B), 1855–1864 (2025)
15. Saraireh, S.: A secure data communication system using cryptography and steganography. *International Journal of Computer Networks & Communications (IJCNC)* Vol 5 (2013)
16. Prakash, S., Rajput, A.: Hybrid cryptography for secure data communication in wireless sensor networks. In: *Ambient Communications and Computer Systems: RACCCS 2017*, pp. 589–599. Springer, Singapore (2018). https://doi.org/10.1007/978-981-10-7386-1_53
17. Biswas, C., Gupta, U.D., Haque, M.M.: An efficient algorithm for confidentiality, integrity and authentication using hybrid cryptography and steganography. In: 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE), pp. 1–5 (2019). IEEE

18. Denis, R., Madhubala, P.: Evolutionary computing assisted visually-imperceptible hybrid cryptography and steganography model for secure data communication over cloud environment. *Int. J. Comput. Netw. Appl* 7(6), 208 (2020)
19. Madavi, K.B., Karthick, P.V.: Enhanced cloud security using cryptography and steganography techniques. In: 2021 International Conference on Disruptive Technologies for Multi-Disciplinary Research and Applications (CENTCON), vol. 1, pp. 90–95 (2021). IEEE
20. [Moussa, K.H., Elsherif, M.H.: A new hybrid steganography scheme employing a time-varying delayed chaotic neural network. In: 2022 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), pp. 152–157 (2022). IEEE
21. Kalaichelvi, V., Devi, P.V., Hemamalini, S., Swaminathan, S., Suganya, S.: Implementation of hybrid cryptography in steganography for augmented security. In: 2023 2nd International Conference on Smart Technologies and Systems for Next Generation Computing (ICSTSN), pp. 1–5 (2023). IEEE
22. Narula, M., Gupta, M., Garg, M.: Implementation of hybrid technique from spatial and frequency domain steganography: Along with cryptography to withstand statistical attacks. In: 2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), pp. 803–808 (2020). IEEE
23. Abikoye, O.C., Ogundokun, R.O., Misra, S., Agrawal, A.: Analytical study on lsb-based image steganography approach. In: Computational Intelligence in Machine Learning: Select Proceedings of ICCIML 2021, pp. 451–457. Springer, Singapore (2022). https://doi.org/10.1007/978-981-19-0145-6_41
24. Vandana, K., Kumari, S.K.: Improving security with efficient key management in public cloud using hybrid aes, ecc and lsb steganography comparing with novel hybrid cube base obfuscation. In: Proceedings of the 2022 International Conference on Business Analytics for Technology and Security (ICBATS), pp. 1–6. IEEE, Dubai, United Arab Emirates (2022). <https://doi.org/10.1109/ICBATS54253.2022.9759044>
25. Badhan, A., Vasudev, H., Kapila, D., Himanshu, H.: Data security in cloud environment using cryptography technique for end-to-end encryption. In: E3S Web of Conferences, vol. 556, p. 01002. EDP Sciences, Les Ulis, France (2024). <https://doi.org/10.1051/e3sconf/202455601002>
26. Miller, V.S.: Use of elliptic curves in cryptography. In: Conference on the Theory and Application of Cryptographic Techniques, pp. 417–426 (1985). Springer
27. Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science, pp. 124–134 (1994). IEEE
28. Avanzi, R., Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Schwabe, P., Seiler, G., Stehlé, D., et al.: Crystals-kyber algorithm specifications and supporting documentation. NIST PQC Round 2(4), 1–43 (2019)
29. Hoffstein, J., Pipher, J., Silverman, J.H.: Ntru: A ring-based public key cryptosystem. In: International Algorithmic Number Theory Symposium, pp. 267–288 (1998). Springer
30. Bernstein, D.J., Dobraunig, C., Eichlseder, M., Fluhrer, S., Gazdag, S., Hülsing, A., Kampanakis, P., Kölbl, S., Lange, T., Lauridsen, M., Mendel, F., Niederhagen, R., Rechberger, C., Rijneveld, J., Schwabe, P., Schofnegger, M., Signer, T., Smith-Tone, D., Stebila, D.: SPHINCS+: Submission to NIST's Post-Quantum Cryptography Project. NIST Post-Quantum Cryptography Project Submission (2022). <https://sphincs.org>
31. McEliece, R.J.: A public-key cryptosystem based on algebraic. Coding Thv 4244(1978), 114–116 (1978)

32. Berlekamp, E., McEliece, R., Van Tilborg, H.: On the inherent intractability of certain coding problems (corresp.). *IEEE Transactions on Information theory* 24(3), 384–386 (1978)
33. Patterson, N.: The algebraic decoding of goppa codes. *IEEE Transactions on Information Theory* 21(2), 203–207 (1975)
34. Heyse, S., Von Maurich, I., Güneysu, T.: Smaller keys for code-based cryptography: Qc-mdpc mceliece implementations on embedded devices. In: *International Conference on Cryptographic Hardware and Embedded Systems (CHES). Lecture Notes in Computer Science*, pp. 273–292. Springer, Berlin, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40349-1_16
35. Kirshanova, E.: Improved quantum information set decoding. In: *International Conference on Post-Quantum Cryptography*, pp. 507–527 (2018). Springer
36. Yalman, Y.: Histogram based perceptual quality assessment method for color images. *Computer Standards & Interfaces* 36(6), 899–908 (2014) <https://doi.org/10.1016/j.csi.2014.04.001>
37. Obaidand, Z.K., Al Saffar, N.F.H.: Image encryption based on elliptic curve cryptosystem. *International Journal of Electrical and Computer Engineering (IJECE)* 11(2), 1293–1302 (2021) <https://doi.org/10.11591/ijece.v11i2.pp1293-1302>
38. Wang, Z., Bovik, A.C., Sheikh, H.R., Simoncelli, E.P.: Image quality assessment: From error visibility to structural similarity. *IEEE Transactions on Image Processing* 13(4), 600–612 (2004) <https://doi.org/10.1109/TIP.2003.819861>