Journal of Future Artificial Intelligence and Technologies

E-ISSN: 3048-3719

Research Article

Quantum Key Distribution-Assisted Image Encryption Using 7D and 2D Hyperchaotic Systems

Zahrah Asri Nur Fauzyah [1], Aceng Sambas [2,3,4], Prajanto Wahyu Adi [5], and De Rosal Ignatius Moses Setiadi [6,*]

[1] Faculty of Computer Science, Universitas Dian Nuswantoro, Semarang, 50131, Central Java, Indonesia; e-mail : itszaraaa317@gmail.com
[2] Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Campus Besut, 22200 Terengganu, Malaysia; e-mail : acengsambas@unisza.edu.my
[3] Artificial Intelligence for Sustainability and Islamic Research Center (AISIR), Universiti Sultan Zainal Abidin, Gongbadak 21300, Malaysia; e-mail : acengsambas@unisza.edu.my
[4] Department of Mechanical Engineering, Universitas Muhammadiyah Tasikmalaya, Tamansari Gobras 46196 Tasikmalaya, Indonesia; e-mail : acengs@umtas.ac.id
[5] Faculty of Science and Mathematics, Universitas Diponegoro, Semarang, Central Java 50275, Indonesia; e-mail : prajanto@live.undip.ac.id
[6] Research Center for Quantum Computing and Materials Informatics, Faculty of Computer Science, Dian Nuswantoro University, Semarang, 50131, Indonesia; e-mail : moses@dsn.dinus.ac.id
* Corresponding Author : De Rosal Ignatius Moses Setiadi

Abstract: Secure image transmission is increasingly vital in the digital era, especially against emerging quantum threats. This study proposes a hybrid image encryption scheme that integrates Quantum Key Distribution (QKD) using the BB84 protocol with a combination of 7-dimensional (7D) and 2-dimensional (2D) hyperchaotic systems to achieve robust security. The BB84 protocol facilitates quantum-assisted key exchange, ensuring resistance to eavesdropping, while the hyperchaotic systems provide high entropy and complex randomness, utilized in a layered permutation-substitution encryption framework. The initial seeds for chaotic sequences are derived using a SHA-512 hash of both the input image and quantum-generated key, ensuring uniqueness and sensitivity. Experimental validation was conducted using several benchmark images. The information entropy values of the ciphered images reached up to 7.9993, indicating excellent randomness. Differential analysis showed high resistance to small perturbations, with NPCR exceeding 99.61% and UACI averaging around 33.47%, which meet standard security thresholds. Histogram and chi-square tests confirmed the uniform pixel distribution, with chi-square values below 280, satisfying the randomness criterion for 8-bit images. Furthermore, correlation coefficients of adjacent pixels dropped to near zero, evidencing effective decorrelation. The encryption scheme also demonstrated robustness to data loss, as shown by the successful decryption of partially corrupted cipher images. Robustness testing under partial data loss (200×200-pixel blocks) also demonstrated visual recoverability and algorithm resilience. Overall, the proposed BB84-assisted dual-hyperchaotic encryption scheme offers a secure and computationally effective solution for protecting sensitive image data, making it suitable for post-quantum secure communications.

Keywords: 2D Hyperchaotic Map; 7D Hyperchaotic System; BB84 Protocol; Fisher-Yates permutations; Post-Quantum Security; Quantum Image Encryption; Quantum Key Distribution.

Received: March, 21st 2025
Revised: April, 20th 2025
Accepted: April, 21st 2025
Published: April, 22nd 2025
Curr. Ver.: April, 22nd 2025

Copyright: © 2025 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY SA) license (https://creativecommons.org/licenses/by-sa/4.0/)

1. Introduction

In this modern era, the rapid development of Internet technology has significantly impacted human lifestyles, making information exchange (text, audio, images, video) easy and efficient[1]. However, this also raises the risk of cyber-attacks, including data theft and information interception [2]–[4]. Cryptography involves techniques for encoding and protecting data from unauthorized access and alteration[5], [6]. However, the conventional cryptographic methods commonly used today, which rely heavily on computational complexity, are

becoming increasingly vulnerable due to advances in quantum computing. Specifically, widely used cryptographic algorithms such as RSA and AES are at risk from quantum algorithms like Shor's and Grover's, significantly weakening their effectiveness [7]–[9]. This vulnerability necessitates integrating quantum-based solutions, notably Quantum Key Distribution (QKD), for secure and reliable key exchange[10].

Quantum Key Distribution, specifically through protocols like BB84, utilizes quantum mechanical principles to distribute cryptographic keys securely [11]–[15]. The strength of BB84 lies in its inherent quantum nature, enabling detection of any eavesdropping attempts, thus ensuring secure key distribution[16]–[18]. However, the direct use of QKD-generated keys alone is insufficient to guarantee security against certain classical cryptographic attacks, such as differential and statistical analysis, particularly in image encryption contexts. Therefore, hybrid approaches integrating quantum and classical cryptography are required to achieve robust protection.

Recent image encryption approaches have shown that incorporating chaotic or hyperchaotic systems can significantly enhance security by generating highly unpredictable random sequences for encryption processes[19]–[21]. Due to their sensitive dependence on initial conditions, multi-dimensional chaotic dynamics, and complex trajectory patterns, hyperchaotic systems are especially promising for robust encryption schemes[22], [23].

Previous studies have explored various hyperchaotic models, including the 2D system proposed by Yu et al.[24] proposed an image encryption technique utilizing a hyperchaotic system and fractional Fourier transform, although it fails to recover images after statistical attacks on encrypted images. Lu et al.[25] introduced a 4D conservative hyperchaotic system to generate chaotic key sequences combined with image DNA encoding for protection, which is very secure but requires faster DNA encoding operations. Tsafack et al. [26] developed a four-dimensional chaotic circuit for image encryption, providing a large key space but remaining vulnerable to noise attacks. Shenli Zhu et al. [27] created a new 2D hyperchaotic system with improved chaotic performance. Despite being two-dimensional, the system has two positive Lyapunov exponents, indicating its potential application in higher-dimensional systems. Naemah [28] proposed a robust 7D hyperchaotic model combined with the Pascal matrix. Alongside hyperchaotic qualities, substitution, and permutation techniques are vital for image encryption. Generally, combining appropriate hyperchaotic-based substitution and permutation techniques can result in high security for image encryption.

Motivated by limitations in previous studies, such as vulnerability to statistical and noise attacks, this research integrates the BB84 quantum key distribution protocol with hybrid 7D and 2D hyperchaotic systems. The BB84 protocol ensures secure key exchange resistant to quantum attacks while combining 7D and 2D hyperchaotic systems balances cryptographic strength and computational efficiency. Thus, this method addresses key vulnerabilities in conventional and existing hyperchaotic-based encryption approaches. The main contributions are:

1. Utilizing quantum mechanics principles for secure key distribution with BB84.
2. Designing a hybrid cryptography model combining classical encryption with QKD.
3. Combining 7D and 2D hyperchaotic systems with robust substitution and permutation techniques for secure image encryption.

The paper is structured as follows: Preliminaries cover QKD (BB84), 2D and 7D hyperchaotic systems, and related work. The proposed scheme combines 7D and 2D hyperchaotic maps with BB84 for improved image encryption. Results and Discussion evaluate the method using various metrics. The paper concludes with final remarks

2. Preliminaries

2.1. Quantum Key Distribution BB84

BB84 is a quantum key exchange protocol that uses qubits, the fundamental units of quantum computing, to transmit secure keys. Alice converts random bits into qubits using two random bases (rectilinear and diagonal). Bob measures these qubits with his random bases. If Bob's measurement basis matches Alice's sending basis, the qubits can be used as a shared key, typically around 50% of the total qubits due to quantum randomness[12], [29]. The protocol is secure because any interference causes the qubit values to become chaotic,

indicating a potential attack if the shared key length deviates significantly from 50%. A qubit in the BB84 protocol is represented as Equation (1).

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1}$$

where $|0\rangle$ and $|1\rangle$ are the fundamental states of the qubit, and α and β are complex coefficients representing the probabilities of these states, ensuring $\alpha^2 + \beta^2 = 1$.

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} \tag{2}$$

$$Rx(\theta) = \frac{1}{\sqrt{2}}\begin{bmatrix} cos\left(\frac{\theta}{2}\right) & -i\ sin\left(\frac{\theta}{2}\right) \\ -i\ sin\left(\frac{\theta}{2}\right) & cos\left(\frac{\theta}{2}\right)\end{bmatrix} \tag{3}$$

In practical BB84 implementations on quantum hardware, Hadamard (H) and Rx (x-axis rotation) gates manage qubits in the x-basis or regulate photon polarization to achieve the necessary angles. The H and Rx gates' mathematical representations in the context of manipulating qubits for the BB84 protocol are shown in Equations (2) and (3). In this formula, θ denotes the rotation angle, with $-i$ representing the complex imaginary unit, where $i^2 = -1$. The $Rx(\theta)$ gate is an x-axis rotation gate that manipulates the qubit phase by θ (in radians) along the x-axis in its matrix representation. The Hadamard gate (H) in BB84 aims to prepare the qubits on an x basis before the sending or measurement process.

2.2. The 2D Hyperchaotic Map

Hyperchaotic 2D maps were introduced by Zhu et al. [27]. The mathematical model analysis of the 2D hyperchaotic map has been analyzed to determine its dynamic properties numerically. Searches of attractor trajectories, bifurcation diagrams, Lyapunov exponents (LE), approximate entropy, and permutation entropy have confirmed the superior complexity of chaos. In this way, the 2D hyperchaotic method can generate quality chaotic sequences, which are statistically random and have a high and balanced convergence speed. The mathematical formula for the new 2D Hyperchaotic model can be seen in Equation (4).

$$\begin{aligned} x_{n+1} &= sin^2\left(\frac{a\pi}{x_n} + by_n\right) \\ y_{n+1} &= sin^2(b\pi y_n + ax_n) \end{aligned} \tag{4}$$

In this system, a and b are the controlling parameters. x_n and y_n are the state variables at the n-th discrete time point, while x_{n+1} and y_{n+1} are at the $(n+1)$-th point. If $x_n \in R$ and $y_n \in R$, then $x_{n+1} \in R$ and $y_{n+1} \in R$, making Equation (4) a mapping of $R \to R$. The 2D hyperchaotic system's trajectory with x_n and y_n when $a \in [0, 40]$ and $b = 30$, with the initial state initial state $(x_0, y_0) = (0{,}2, 0{,}3)$, is shown in Figure 1.

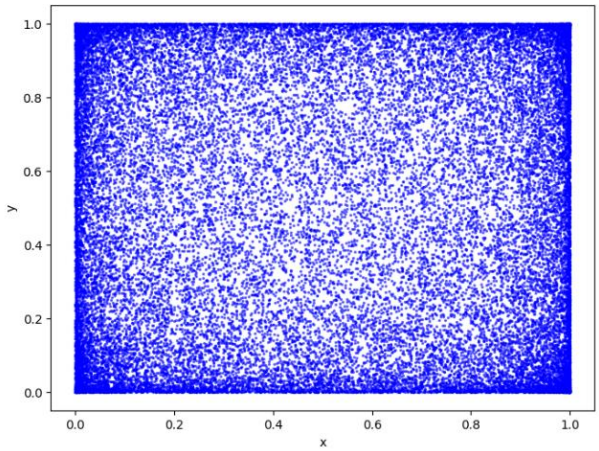

Figure 1. Sample of trajectory diagram of 2D Hyperchaotic

2.3 The 7D Hyperchaotic Map

The seven-dimensional hyperchaotic system introduced in [28], consists of seven interconnected differential equations with eight parameters (a, b, c, d, e, f, g, h). This system generates chaotic sequences exhibiting complex and highly unpredictable behaviors, enhancing encryption security. The formula for the 7D hyperchaotic system is shown in Equation (5).

$$\begin{cases} \dot{x}_1 = -ax_1 + ax_5 - bx_5x_6x_7 \\ \dot{x}_2 = -cx_2 - dx_6 + x_1x_6x_7 \\ \dot{x}_3 = -ax_3 + ax_5 - gx_1x_2x_7 \\ \dot{x}_4 = -ax_4 + ex_1 + x_1x_2x_3 \\ \dot{x}_5 = -ax_5 + ex_7 - x_2x_3x_4 \\ \dot{x}_6 = -ex_6 + ex_5 + x_3x_4x_5 \\ \dot{x}_7 = -bx_7 + fx_2 - hx_4x_5x_6 \end{cases} \tag{5}$$

Here a, b, c, d, e, f, g, h are the parameters of the system, while x_1, x_2, x_3, x_4, x_5, x_6, x_7 are the initial values. In this system, the selected parameter values are $a = 15$, $b = 5$, $c = 0.5$, $e = 10$, $f = 4$, $g = 0.1$, and $h = 1.5$. The parameter d acts as the control parameter, while the other values remain constant. The trajectory diagram of system $d \in [7.6, 27.4]$ is shown in Figure 2.

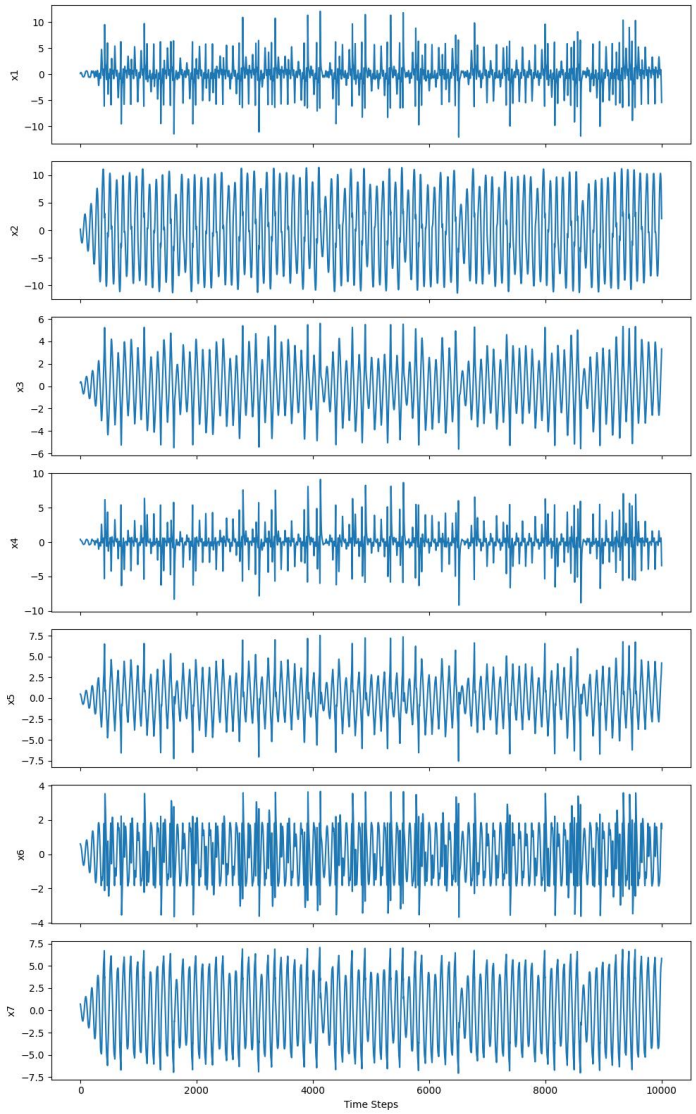

Figure 2. Sample of the trajectory of each sequence of 7D hyperchaotic system.

2.4. Related Works

The BB84 protocol as a QKD has gained attention due to its robustness against quantum computing threats. Bennett and Brassard's [30] implementation combined BB84 with post-quantum cryptographic approaches to enhance security. Vest et al. [31] developed a portable BB84 unit suitable for short-range applications, and Shu [32] proposed an optimal quantum key distribution protocol based on BB84 principles. BB84's quantum nature makes it superior to classical cryptographic methods by leveraging quantum mechanics' inherent unclonability and probabilistic characteristics, significantly enhancing resistance to interception.

After quantum key generation using BB84, encryption often involves XOR operations between the quantum-generated key and plaintext bits. Kuang and Chan [33] explored quantum encryption using shift operators for XOR operations in phase space, while Abdullah and Mahdi [34] combined geometric transformations with XOR operations using quantum random numbers.

Hyperchaotic systems enhance encryption security due to their sensitive dependence on initial conditions, multi-dimensional dynamics, and complexity. Previous studies include Winarno et al. [23], who proposed combining two hyperchaotic systems and unified confusion-diffusion patterns, demonstrating good resistance to differential and statistical attacks [23]. Benaissi et al. [35] integrated hybrid chaos maps with key images for robust sequence generation. Setiadi and Rijati [5] used 2D chaos logistic maps combined with permutation-substitution operations for secure encryption. Meanwhile, Andono and Setiadi [36] combined pixel and bit confusion using mixed chaos systems and hash operations.

Motivated by limitations identified in previous research, particularly vulnerabilities to statistical analysis, differential attacks, and insufficient randomness quality, this study integrates the BB84 protocol with hybrid 7D and 2D hyperchaotic systems. The combination strategically leverages the secure key distribution properties of BB84, the superior complexity of 7D hyperchaotic maps, and the efficient randomness generation from 2D hyperchaotic maps. Therefore, this hybrid approach addresses the critical gaps of previous encryption methods, achieving enhanced security against statistical and differential cryptographic attacks while maintaining high-quality randomness.

3. Proposed Method

This research proposes an encryption scheme that integrates QKD BB84 with classical cryptographic techniques and 7D and 2D hyperchaotic systems to improve the security of image encryption. The scheme leverages quantum keys generated via the BB84 protocol and classical cryptography techniques to strengthen security. In addition, applying the 7D hyperchaotic and 2D hyperchaotic systems aims to randomize image data effectively, increasing the level of chaos and security of the encryption process. In this scheme, substitution and XOR encryption techniques add complexity to the encryption process, thereby increasing the difficulty level for those trying to carry out cryptanalysis attacks. An illustration of the proposed method can be seen in Figure 3, and the stages of the proposed method are explained in detail in sections 3.1 to 3.2.

3.1. Preparation and Generate Initial Seed

1. Read the input image, then perform a SHA-512 hash operation on the input image, thus obtaining $\mathrm{hash1}$. This will uniquely represent the image used as one part of forming chaotic parameters.
2. Generate quantum keys using the BB84 protocol. So that the input key has a uniform length, a SHA-512 hash operation on the quantum key is performed to get $\mathrm{hash2}$.
3. Each $\mathrm{hash1}$ and $\mathrm{hash2}$ has 128 hexa numbers converted into 64 ASCII characters.
4. The combination of both hashes becomes hybrid_hash using Equation (6).

$$\mathrm{hybrid_hash} = (\mathrm{hash2} + \mathrm{hash2}) \bmod 256 \tag{6}$$

5. Form the initial seed for 7D hyperchaotic and 2D hyperchaotic using hybrid_hash. Use the standard deviation (σ) function. Next, carry out normalization by dividing 10 by the power of the value rounded down from the base 10 logarithm of the standard deviation results. The Equation (7) calculates the initial seed formula for 7D 2D hyperchaotic.

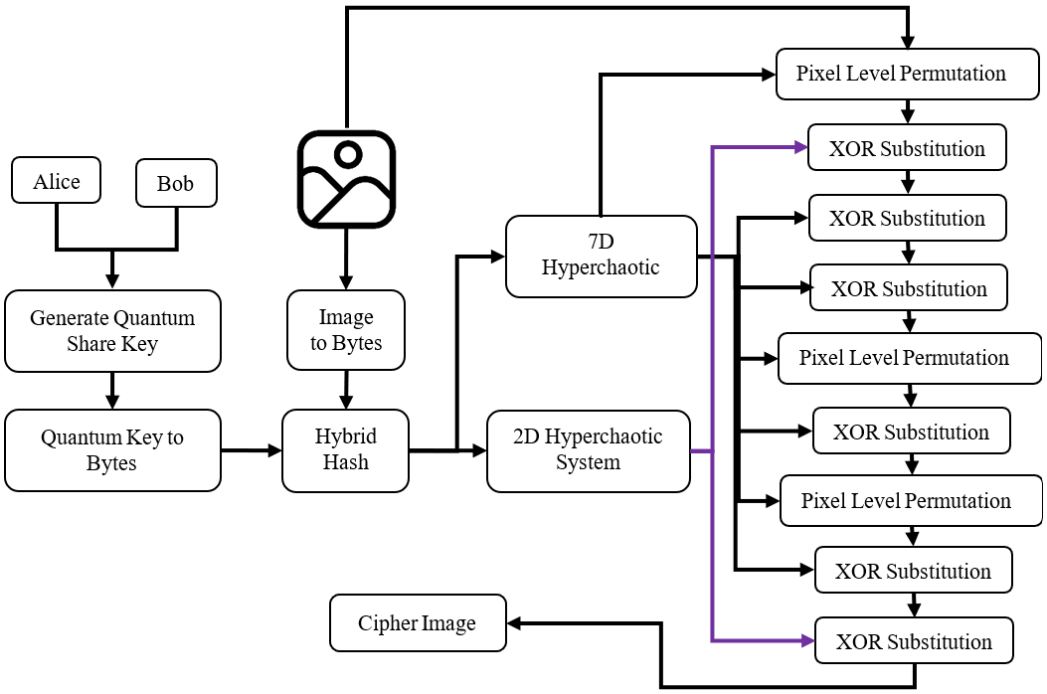

Figure 3. Purposed Method

$$is_i = \frac{\sigma(\text{hybrid_hash}_j, \ldots, \text{hybrid_hash}_{j+n-1})}{10^{\lfloor \log_{10}(\text{std}(\text{hybrid_hash}_j,\ldots,\text{hybrid_hash}_{j+n-1}) \rfloor}} - 1 \quad (7)$$

Where is_i is i^{th} initial seed values; hybrid_hash_j denotes the j^{th} character of the hybrid_hash; j and n are indices defining segments of the hash utilized to generate each seed. To clearly illustrate the assignment of indices (i, j, and n), Table 1 summarizes the indexing for each initial seed calculation.

6. The output of this stage is to obtain nine initial seeds for 7D and 2D hyperchaotic.

Table 1. Indexing of the hybrid hash for initial seed generation.

Initial Seed (is_i)	Start Index (j)	Length of Segment (n)
is_1 (7D Seed-1)	1	9
is_2 (7D Seed-2)	10	9
is_3 (7D Seed-3)	19	9
is_4 (7D Seed-4)	28	9
is_5 (7D Seed-5)	37	9
is_6 (7D Seed-6)	46	9
is_7 (7D Seed-7)	55	9
is_8 (2D Seed-1)	1	32
is_9 (2D Seed-2)	33	32

3.2. Image Encryption using 7+2 Dimensional Hyperchaotic map

1. The image encryption stage begins by generating a chaotic sequence based on the initial seed and specified parameters. For 2D hyperchaotic, parameter values a=0.9 and b=0.4 were adopted from Zhu et al. [27], while for the 7D hyperchaotic system, the parameters a = 15, b = 5, c = 0.5, d = 25, e = 10, f = 4, g = 0.1, and h = 1.5 were chosen based on Naemah's work [28]. These parameter choices ensure optimal chaotic behavior and randomness quality. Thus, after execution, nine chaotic sequences are obtained: seven sequences are $\dot{x}_1(t)$, $\dot{x}_2(t)$, $\dot{x}_3(t)$, $\dot{x}_4(t)$, $\dot{x}_5(t)$, $\dot{x}_6(t)$, $\dot{x}_7(t)$ from 7D hyperchaotic and two chaotic sequences $\dot{x}(t)$, $\dot{y}(t)$ from 2D hyperchaotic.
2. Change the image to a one-dimensional format.

3. The first layer is carried out using a pixel permutation technique using the chaotic sequence $\dot{x}_6(t)$. Permutation is performed using the Fisher-Yates algorithm by normalizing the chaotic sequence. Suppose the normalized chaotic sequence $\dot{x}_6(t)$ is represented by $A \in \{a_1, a_2, \ldots, a_n\}$. The permutation operation is then executed on the one-dimensional image array using Algorithm 1, producing the first encrypted layer output, denoted as $encL1$.

Algorithm 1. Fisher-Yates Notation
INPUT: $\dot{x}_6(t)$
OUTPUT: $encL1$
1: for $i \leftarrow n-1$ to do 1
2: $j \leftarrow$ random integer such that $0 \le j \le i$
3: Swap $A[i]$ with $A[j]$

4. Subsequent encryption layers (layers 2 to 9) alternately apply XOR substitution and permutation operations to increase encryption complexity. Each encryption layer is denoted as $encL_i$, where i represents the layer number. XOR substitutions use chaotic sequences from the 7D and 2D hyperchaotic systems, while permutation layers again utilize the Fisher-Yates algorithm with specified chaotic sequences. The detailed operations for each encryption layer are summarized in Table 2.

Table 2. Encryption steps for layers 2 to 9.

Layer ($encL_i$)	Operation Type	Chaotic Sequence
2	XOR substitution	$\dot{x}(t)$
3	XOR substitution	$\dot{x}_1(t)$
4	XOR substitution	$\dot{x}_3(t)$
5	Permutation (Fisher-Yates)	$\dot{x}_5(t)$
6	XOR substitution	$\dot{x}_4(t)$
7	Permutation (Fisher-Yates)	$\dot{x}_7(t)$
8	XOR substitution	$\dot{x}_2(t)$
9	XOR substitution	$\dot{y}(t)$

Note: XOR substitution is performed by applying bitwise XOR operations between the previous encryption output $encL_{i-1}$ and the respective chaotic sequence. Fisher-Yates permutation is performed as shown in Algorithm 1.
The final output after the ninth encryption layer is the cipher image. Decryption involves reversing these encryption steps in the opposite order, using identical sequences.

4. Results and Discussion

This section presents the experimental results. The proposed method was implemented using Python and Google Collab, with the Qiskit simulator version 0.46.1 for QKD BB84 simulation. The experiment used a standard 512×512pixel image commonly employed in image encryption studies and full black and white images to test robustness, as shown in Figure 4. Various security analyses, detailed with visualizations, are presented in sections 4.1 to 4.8.

4.1 Generate Quantum Key Distribution

This section illustrates the BB84 protocol's process to generate a secure cryptographic key, following the theory described in Section 2.1. Before encryption, the key generation process ensures that Alice and Bob agree on a secure key by using the same measurement bases. The experiment used 512 bits, split into batches of 8 qubits due to Qiskit simulator limitations. Below is an example from one batch:

1. Alice sends a message and measures the first 8 bits: "110011100", using two bases: Z ($|1\rangle|0\rangle$) and Y ($|-i\rangle \mid +i\rangle$).
2. For the first bit (1), Alice uses the Z basis and creates a qubit in state $|1\rangle$.
3. Alice uses the Y basis for the second bit (0) and creates a qubit in state $|-i\rangle$.

4. These qubits are sent to Bob, who measures them using the same or different bases from Alice.

Sample key generation results for an 8-bit batch are presented in Table 3, while the circuit used is shown in Figure 5.

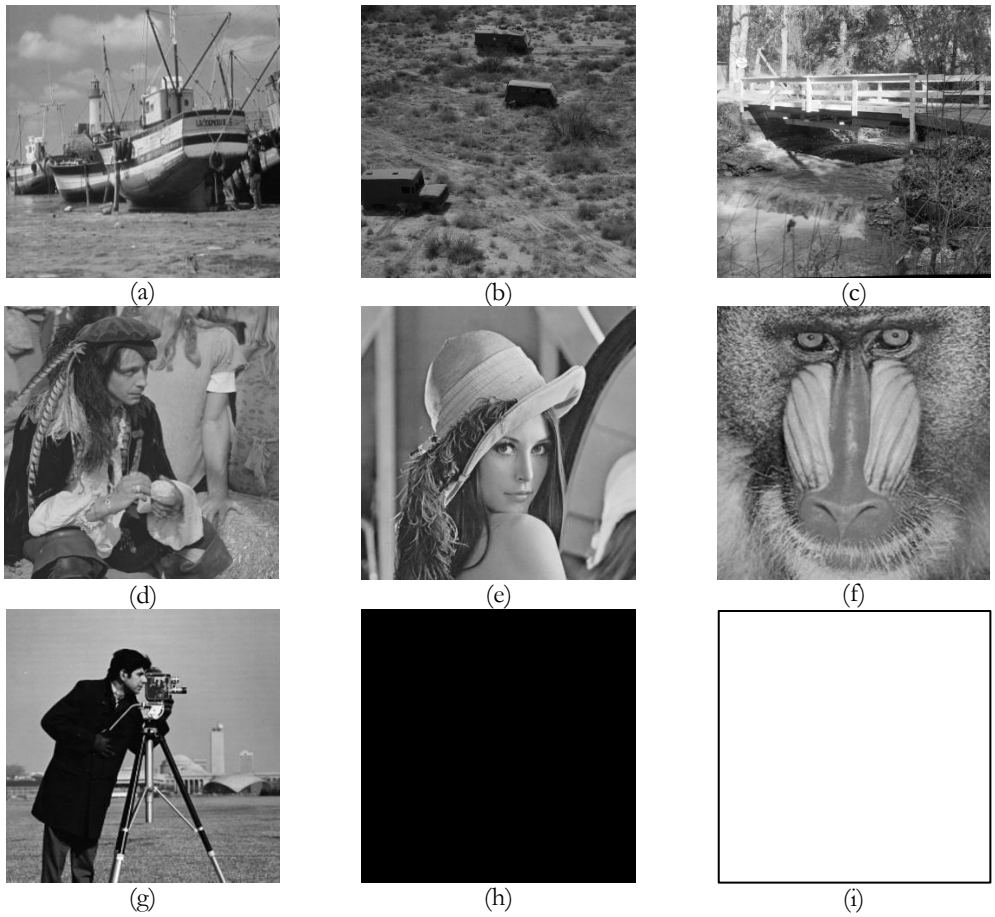

Figure 4. Standard image used for testing. (**a**) Boats; (**b**) Trucks; (**c**) Stream and bridge; (**d**) Pirates; (**e**) Lena; (**f**) Baboons; (**g**) Cameraman; (**h**) full black; (**i**) full white.

Table 3. Key generation using BB84 distribution protocol.

Bits	Alice Base	Alice Qubit	Bob Base	Measurement
1	Z	$\|1\rangle$	Z	Match
1	Y	$\| +i\rangle$	Y	Match
0	Z	$\|0\rangle$	Z	Match
0	Z	$\| 0\rangle$	Y	Not match
1	Y	$\|+i\rangle$	Z	Not match
1	Z	$\|1\rangle$	Z	Match
1	Y	$\|+i\rangle$	Z	Not match
0	Z	$\|0\rangle$	Y	Not match

4.2. Information Entropy

Information Entropy (IE) measures a data source's uncertainty or confusion level. In image encryption, IE indicates the degree of randomness or uncertainty in the distribution of pixel values of the image. A good-quality encrypted image should have a high IE value (close to eight), indicating that the encryption has succeeded in scrambling the image data well and minimizing information leakage. Conversely, if the IE value is low, it will indicate that the encryption is not strong enough, and there may still be patterns or information that can be identified in the encrypted image. The IE calculation is

carried out using Equation (8), and the measurement results and comparison with related methods are presented in Table 4.

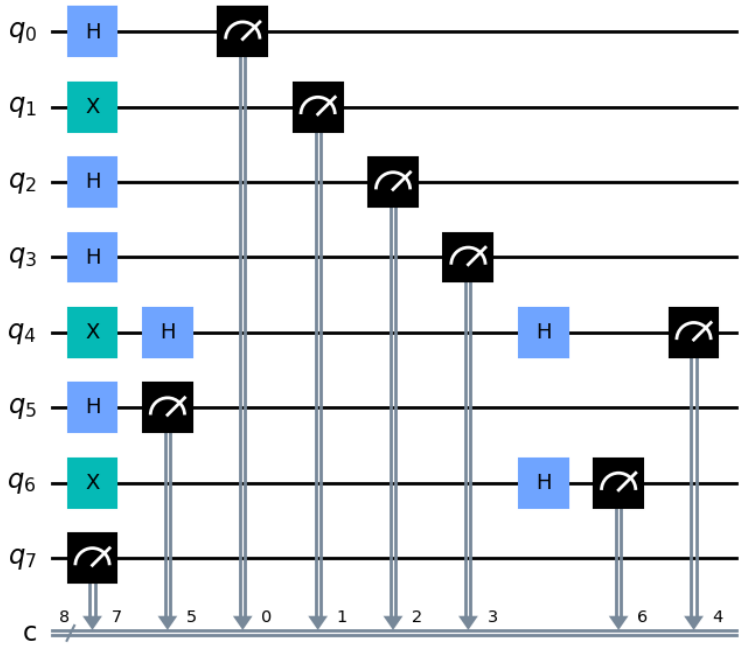

Figure 5. Sample Quantum Circuit Used

$$H(x) = -\sum_{i=1}^{n} P(x_i) \log_2 P(x_i) \tag{8}$$

In the Equation (8), $H(x)$ represents the IE value of random variable x; $P(x_i)$ shows the probability of the appearance of value x_i in random variable x; n is the total number of possible values of random variable x. The negative sign in front of the sum is used because the information entropy is expected to be positive. The more possible values there are in the random variable x and the more evenly distributed the probability of their occurrence, the higher the value of the IE. On the other hand, if there is one dominant value with a very high probability of occurrence, then the information entropy will be low.

Table 4. Information entropy results and comparison.

Image	Ref [34]	Ref[22]	Ref[37]	Ref [38]	Proposed
Boat	-	7.9993	-	7.9993	7.9993
Truck	-	-	-	-	7.9993
Stream and bridge	-	-	-	-	7.9993
Pirate	-	-	-	-	7.9992
Lena	7.599	7.9993	7.9993	7.9991	7.9993
Cameraman	-	-	7.9993		7.9993
Baboon	7.6232	7.9993	7.9993	7.9992	7.9993
Black	-	-	-	-	7.9992
White	-	-	-	-	7.9992

4.3. Differential Analysis

Normalized Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are two metrics widely used to evaluate the performance of encryption algorithms against differential analysis. NCPCR measures the percentage of pixel changes between two encrypted images whose keys are only slightly different. In comparison, UACI measures the average intensity of pixel changes between the two images. According to [39], a good image

encryption algorithm must have an NCPCR value above 99% and a UACI value between 33% and 34%. Suppose the NCPCR and UACI values are outside this range. In that case, the encryption algorithm is considered less effective in producing encrypted images that are genuinely random and sensitive to key changes. Equation (9) measures NPCR, while UACI is in Equation (10).

$$NPCR = \left[\frac{1}{N \times M}\sum_{i=1}^{N}\sum_{j=1}^{M}\delta(i,j)\right] \times 100\%, \delta(i,j)\begin{cases}0 \; if \; E_1(i,j) = E_2(i,j)\\1 \; if \; E_1(i,j) \neq E_2(i,j)\end{cases} \quad (9)$$

$$UACI = \left[\frac{1}{N \times M}\sum_{i=1}^{N}\sum_{j=1}^{M}\frac{|E_1(i,j) - E_2(i,j)|}{255}\right] \times 100\% \quad (10)$$

Where $E1$ is the encrypted image, while $E2$ describes the encrypted image with 1-bit modification in the plaintext, N refers to the number of column pixels, and M refers to the number of row pixels. The variables i and j represent the coordinates of each pixel individually, with 255 being the maximum pixel intensity value in the image.

Table 5. NPCR results and comparison.

Image	Ref [34]	Ref[22]	Ref[37]	Ref [38]	Proposed
Boat	-	99.61	99.59	99.60	99.59
Truck	-	-	99.59	-	99.60
Stream and bridge	-	-	99.60	-	99.59
Pirate	-	-	-	-	99.62
Lena	99.62	99.62	99.59	99.60	99.61
Cameraman	-	-	99.60	-	99.59
Baboon	99.58	99.61	99.61	99.61	99.60
Black	-	-	-	-	99.61
White	-	-	-	-	99.59

Table 6. UACI results and comparison.

Image	Ref [34]	Ref[22]	Ref[37]	Ref [38]	Proposed
Boat	-	33.46	33.48	33.46	33.47
Truck	-	-	33.45	-	33.47
Stream and bridge	-	-	33.49	-	33.48
Pirate	-	-	-	-	33.45
Lena	33.62	33.43	33.46	33.46	33.46
Cameraman	-	-	33.50	-	33.49
Baboon	33.45	33.47	33.48	33.49	33.47
Black	-	-	-	-	33.47
White	-	-	-	-	33.46

4.4 Histogram Analysis

A histogram is a graphical representation showing pixel intensity distribution in a digital image. On the horizontal axis (x), the histogram displays the range of pixel intensity values, starting from 0 (black) to 255 (white) for images with a bit depth of 8. Meanwhile, the vertical axis (y) shows the number or frequency of pixels with a certain intensity value. In the context of image encryption, histograms play an important role as indicators of the success of the encryption process. Before encrypting, the initial image histogram usually has an uneven distribution, with several pixel intensity values dominating and forming certain peaks. However, the pixel intensity distribution should become evener and more uniform after an effective encryption process. The proposed method successfully does this, as shown in Figure 6.

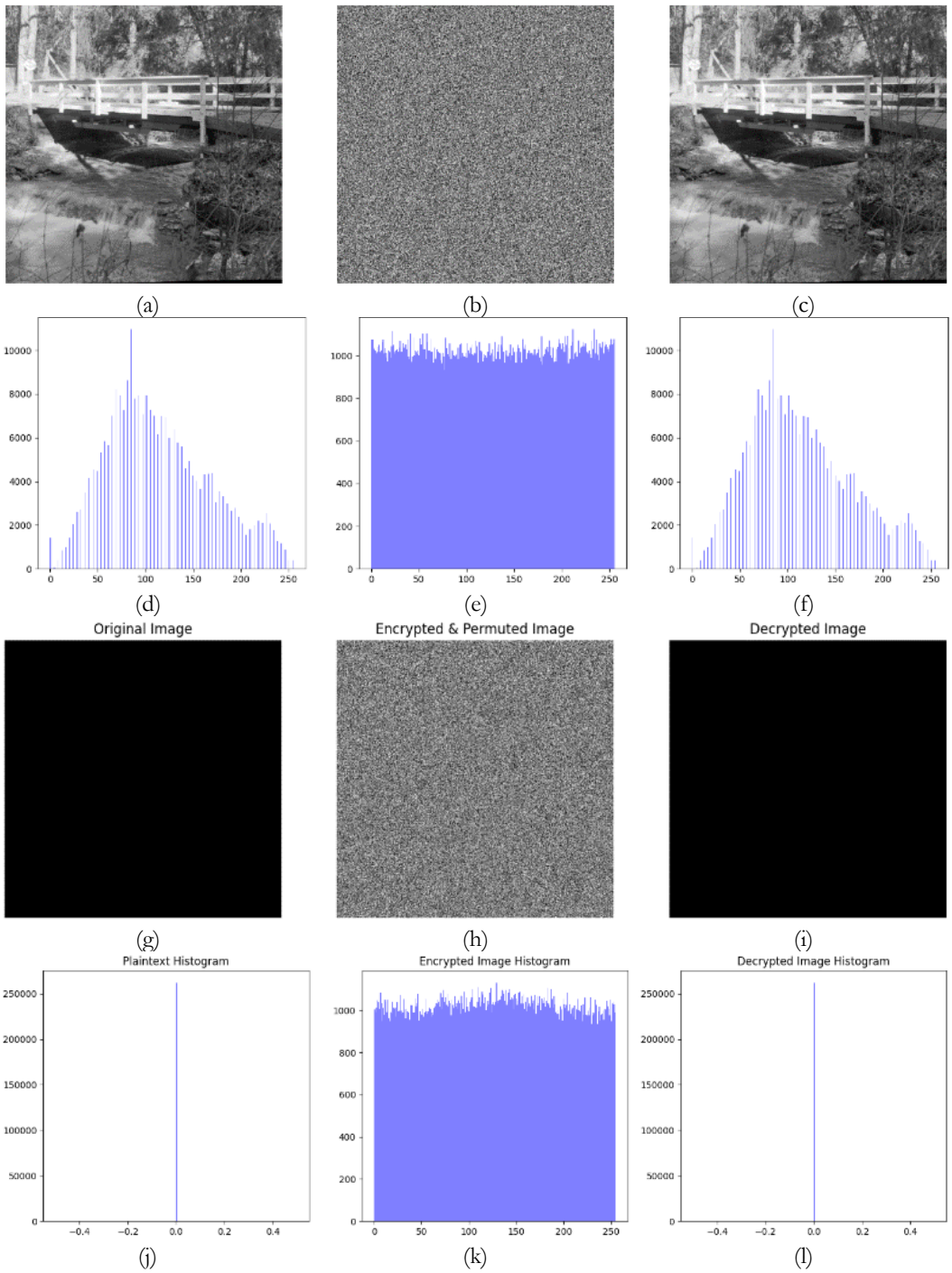

Figure 6. Sample encryption results and its histogram (**a**) Stream and bridge; (**b**) Encrypted Stream and bridge; (**c**) Decrypted Stream and bridge; (**g**) Black image; (**h**) Encrypted black image; (**i**) Decrypted black image; (**d,j**) Original histogram; (**e,k**) encrypted histogram; (**f,l**) decrypted histogram.

4.5. Chi-Square (χ^2)Analysis

Chi-square is a statistical tool often used to measure the level of randomness of pixel distribution in encrypted images and the uniformity of the histogram. The more random the pixel distribution, the lower the chi-square value and the more uniform the histogram. A good chi-square value for 8-bit image encryption is at least less than 293.2478. Chi-square can be calculated mathematically using Equation (11).

$$\chi^2 = \sum_{i=1}^{256} \frac{(O_i - E_i)^2}{E_i} \tag{11}$$

Where the χ^2 value is calculated from the difference between the number of pixels in each value of the original image (O_i) and encrypted image (E_i), which is the expected frequency with the theoretical probability distribution of pixel value i.

The results of the χ^2 calculation is shown in Table 7.

Table7. Chi-square results and comparison.

Image	Ref[22]	Ref[37]	Proposed
Boat	259.4941	244.456	236.8339
Truck	-	-	240.9355
Stream and bridge	-	-	249.2519
Pirate	-	-	256.4570
Lena	242.9590	244.125	243.6640
Cameraman	-	247.285	249.7480
Baboon	255.6563	246.271	245.9042
Black	-	-	280.0195
White	-	-	272.7148

4.6. Correlation Coefficient of Adjacent Pixels (CCAP)

The Correlation Coefficient of Adjacent Pixels (CCAP) measures how well an encryption algorithm disrupts the correlation between adjacent pixels in an image. Original images usually correlate highly with adjacent pixels, but effective encryption should reduce this, making the encrypted image appear random. CCAP is measured in three directions: horizontal, vertical, and diagonal, to ensure randomness across all patterns. CCAP values range from 1 to -1, with values near 0 indicating effective encryption. The results of CCAP measurements are shown in Table 8, and a sample plot is presented in Figure 7.

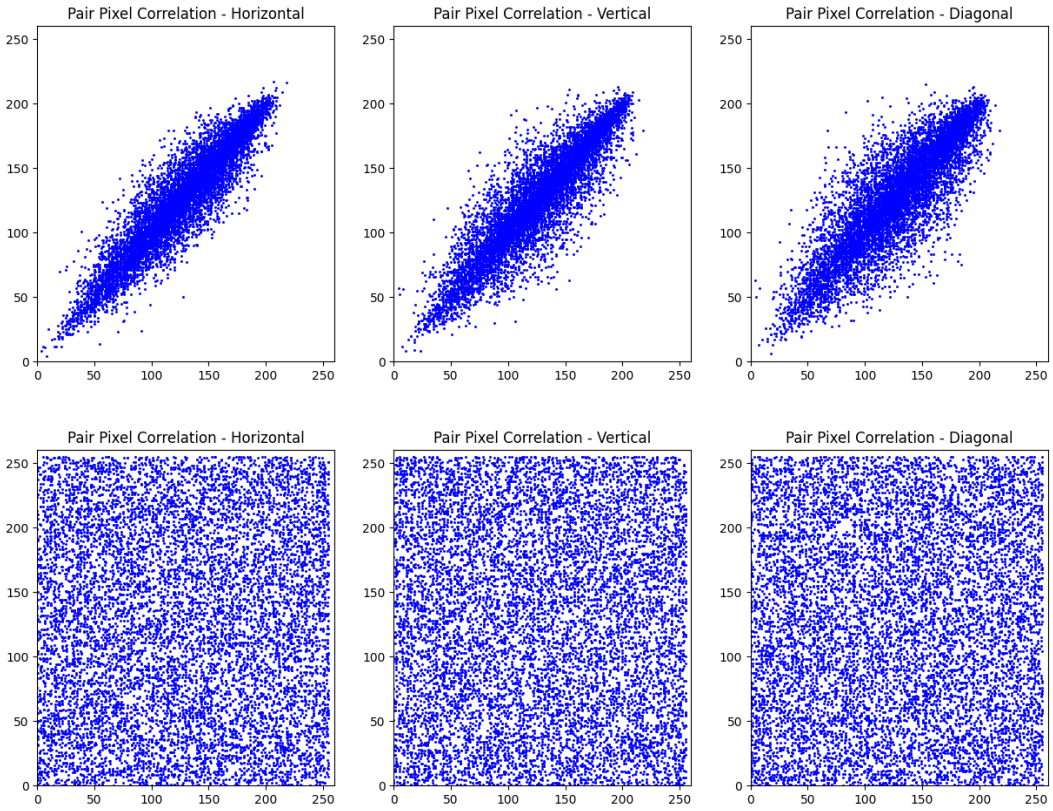

Figure 7. The correlation coefficient of adjacent pixels of plain(top) and encrypted image (under).

Table 8. UACI results and comparison.

Image	Direction	Ref [34]	Ref[22]	Ref[37]	Ref [38]	Proposed
Boat	H	-	0.0041	0.0018	0.0048	0.0003
	V	-	0.0011	0.0004	-0.0022	-0.0003
	D	-	0.0113	0.0014	0.0013	-0.0001
Truck	H	-	-	-	-	-0.0009
	V	-	-	-	-	0.0005
	D	-	-	-	-	0.0004
Stream and bridge	H	-	-	-	-	0.0009
	V	-	-	-	-	0.0003
	D	-	-	-	-	-0.0002
Pirate	H	-	-	-	-	0.0006
	V	-	-	-	-	0.0003
	D	-	-	-	-	-0.0001
Lena	H	0.0021	0.0019	0.0016	0.0033	-0.0003
	V	- 0.0113	0.0069	0.0013	0.0022	0.0006
	D	0.0029	0.0200	0.0005	-0.0035	0.0001
Cameraman	H	-	-	0.0010	-	-0.0002
	V	-	-	0.0016	-	0.0003
	D	-	-	0.0011	-	-0.0006
Baboon	H	- 0.0203	0.0251	0.0011	0.0012	-0.0003
	V	0.0038	0.0040	0.0014	0.0014	0.0002
	D	0.0032	0.0231	0.0007	0.0039	0.0009
Black	H	-	-	-	-	-0.0006
	V	-	-	-	-	-0.0004
	D	-	-	-	-	-0.0003
White	H	-	-	-	-	-0.0002
	V	-	-	-	-	-0.0008
	D	-	-	-	-	-0.0006

4.7 Robustness Test

The robustness test in image encryption aims to assess how well the encryption algorithm can maintain image integrity when some of the data is lost or damaged. This is important because encrypted images can lose some of their data in real situations, such as poor data transmission or storage corruption. In this test, encrypted image data is intentionally deleted or partially destroyed, then decrypted again to see how well the original image can be recovered. A robust encryption algorithm must produce images that are still recognizable or have minimal distortion, demonstrate resistance to data loss, and ensure data security and reliability even in imperfect conditions. This research also tested the proposed method with robustness test sample results presented in Figure 8.

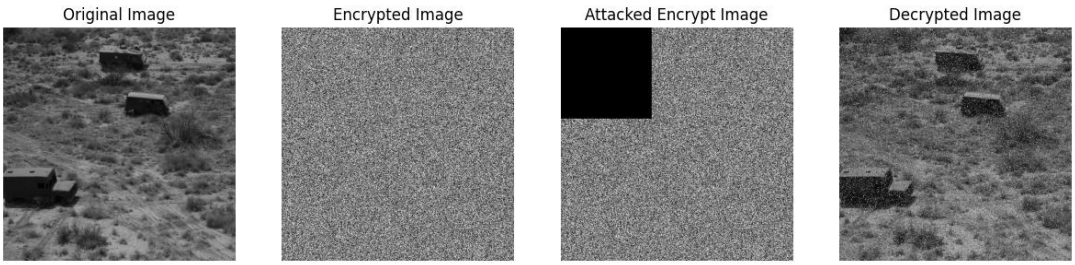

Figure 8. Sample of Robustness test using 200×200 pixels attack

4.8. Discussion

Based on the results presented in sub-chapters 4.1 to 4.6, it can be concluded that 1) The information entropy value almost reaches 8 for all test images, indicating a high degree of randomness in the encrypted images, on par with or better than other methods. 2) NCPCR values above 99% and UACI between 33% and 34% indicate that the method is susceptible to small changes in the encryption key, indicating high security and resistance to attacks. 3) The histogram of the encrypted image shows a uniform and unrecognizable pixel distribution, indicating effective encryption in disguising the original pattern. This is confirmed by the chi-square value lower than the threshold of 293.2478. Moreover, compared with other methods described in [22] and [37]**,** this method performs comparable or even better in creating unpredictable pixel distributions. 4) CCAP values close to zero for all directions indicate that this method effectively eliminates correlation between adjacent pixels. The results of measuring the CCAP value in the proposed method also prove significant superiority compared to related research. 5) Based on the robustness test, the proposed method also shows good results, maintaining image integrity even though some data is lost during transmission or storage, showing good durability in real conditions. Overall, this discussion highlights that the combination of 7D and 2D hyperchaotic systems with quantum key distribution using the BB84 protocol proposed in this research shows excellent performance in various aspects of security evaluation.

5. Conclusions

This research has succeeded in proposing a secure image transmission scheme by integrating the BB84 protocol and classical cryptographic techniques, namely the hyperchaotic system. The BB84 protocol is tasked with distributing keys securely based on the principles of quantum mechanics, and these keys are used to carry out image encryption based on 7D and 2D hyperchaotic models. On the classical side, all the resulting sequences are used for the XOR substitution process and Fisher-Yates permutation to produce high encryption complexity, making it difficult for cryptanalysts to carry out attacks. Experimental results show that the proposed method succeeds in encrypting images well. Some measurements, including histogram, chi-square, information entropy, adjacent pixel correlation coefficient, NPCR, and UACI, confirm that the proposed method meets the security criteria for effective image encryption. However, despite its strong encryption capabilities, the proposed method has limitations. The implementation currently relies on the Qiskit simulator for BB84-based key distribution, meaning real-world deployment on quantum hardware is yet to be tested. Further refinements and optimizations may also be explored to enhance computational efficiency and adaptability in different practical scenarios. By leveraging the combination of the BB84 protocol and dual hyperchaotic systems, the proposed encryption scheme offers high security and resistance to various cryptographic attacks. This research contributes to developing secure and efficient image encryption methods, leveraging quantum and hyperchaotic principles to protect sensitive information in modern communications.

Author Contributions: Conceptualization: ZANF and DRIMS.; Methodology: ZANF and DRIMS; Software: ZANF and PWA; Validation: AS, PWA, and DRIMS; Formal analysis: AS and PWA; Investigation: AS and DRIMS; Resources: ZANF; Data curation: ZANF; Writing—original draft preparation: ZANF; Writing—review and editing: AS, PWA, and DRIMS; Visualization: ZANF; Supervision: DRIMS; Project administration: ZANF; Funding acquisition: All. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

[1] A. K. Jain, S. R. Sahoo, and J. Kaubiyal, "Online social networks security and privacy: comprehensive review and analysis," *Complex Intell. Syst.*, vol. 7, no. 5, pp. 2157–2177, Oct. 2021, doi: 10.1007/s40747-021-00409-7.

[2] A. Çetin and S. Öztürk, "Comprehensive Exploration of Ensemble Machine Learning Techniques for IoT Cybersecurity Across Multi-Class and Binary Classification Tasks," *J. Futur. Artif. Intell. Technol.*, vol. 1, no. 4, pp. 371–384, Feb. 2025, doi: 10.62411/faith.3048-3719-51.

[3] J. P. Ntayagabiri, Y. Bentaleb, J. Ndikumagenge, and H. El Makhtoum, "OMIC: A Bagging-Based Ensemble Learning Framework for Large-Scale IoT Intrusion Detection," *J. Futur. Artif. Intell. Technol.*, vol. 1, no. 4, pp. 401–416, Feb. 2025, doi: 10.62411/faith.3048-3719-63.

[4] D. R. I. M. Setiadi, S. K. Ghosal, and A. K. Sahu, "AI-Powered Steganography: Advances in Image, Linguistic, and 3D Mesh Data Hiding – A Survey," *J. Futur. Artif. Intell. Technol.*, vol. 2, no. 1, pp. 1–23, Apr. 2025, doi: 10.62411/faith.3048-3719-76.

[5] D. R. I. M. Setiadi and N. Rijati, "An Image Encryption Scheme Combining 2D Cascaded Logistic Map and Permutation-Substitution Operations," *Computation*, vol. 11, no. 9, p. 178, Sep. 2023, doi: 10.3390/computation11090178.

[6] A. Singh, K. B. Sivangi, and A. N. Tentu, "Machine Learning and Cryptanalysis: An In-Depth Exploration of Current Practices and Future Potential," *J. Comput. Theor. Appl.*, vol. 1, no. 3, pp. 257–272, Feb. 2024, doi: 10.62411/jcta.9851.

[7] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pp. 124–134. doi: 10.1109/SFCS.1994.365700.

[8] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96*, 1996, pp. 212–219. doi: 10.1145/237814.237866.

[9] D. R. I. M. Setiadi, N. Rijati, A. R. Muslikh, B. V. Indriyono, and A. Sambas, "Secure Image Communication Using Galois Field, Hyper 3D Logistic Map, and B92 Quantum Protocol," *Comput. Mater. Contin.*, vol. 81, no. 3, pp. 4435–4463, 2024, doi: 10.32604/cmc.2024.058478.

[10] M. A. Nielsen and I. L. Chuang, "Quantum information theory," in *Quantum Computation and Quantum Information*, Cambridge University Press, 2012, pp. 528–607. doi: 10.1017/CBO9780511976667.016.

[11] B. Qi, L. Qian, and H. Lo, "Quantum Encryption," in *Optical and Digital Image Processing*, Wiley, 2011, pp. 769–787. doi: 10.1002/9783527635245.ch34.

[12] C. Bernhardt, *Quantum Computing for Everyone*. Fairfield University: The MIT Press, 2019. doi: 10.7551/mitpress/11860.001.0001.

[13] S. K. Sehgal and R. Gupta, *SOA Based BB84 Protocol for Enhancing Quantum Key Distribution in Cloud Environment*, vol. 130, no. 3. Springer US, 2023. doi: 10.1007/s11277-023-10354-y.

[14] N. Sinha, "Quantum Computation and Quantum Information by Michael E. Nielson and Isaac L. Chuang," *Mapana - J. Sci.*, vol. 1, no. 2, pp. 120–121, Apr. 2003, doi: 10.12723/mjs.2.10.

[15] A. M. A. A. Al-muqarm, F. Abedi, and A. S. Abosinnee, "Quantum Computing Cryptography and Lattice Mechanism," *J. Inf. Commun. Converg. Eng.*, vol. 20, no. 4, pp. 242–249, Dec. 2022, doi: 10.56977/jicce.2022.20.4.242.

[16] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *J. Cryptol.*, vol. 5, no. 1, pp. 3–28, 1992, doi: 10.1007/BF00191318.

[17] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, Aug. 1991, doi: 10.1103/PhysRevLett.67.661.

[18] J. G. Sekar, E. Periyathambi, and A. Chokkalingam, "Hybrid chaos-based image encryption algorithm using Chebyshev chaotic map with deoxyribonucleic acid sequence and its performance evaluation," *Int. J. Electr. Comput. Eng.*, vol. 13, no. 6, p. 6952, Dec. 2023, doi: 10.11591/ijece.v13i6.pp6952-6963.

[19] Y. Zhang, R. Li, Y. Shi, and F. Luo, "The Probabilistic Image Encryption Algorithm Based on Galois Field GF(257)," *IETE J. Res.*, pp. 1–14, Nov. 2023, doi: 10.1080/03772063.2023.2284956.

[20] T. Gopalakrishnan and S. Ramakrishnan, "Chaotic Image Encryption with Hash Keying as Key Generator," *IETE J. Res.*, vol. 63, no. 2, pp. 172–187, Mar. 2017, doi: 10.1080/03772063.2016.1251855.

[21] M. Devipriya, M. Sreenivasan, and M. Brindha, "Reconfigurable Architecture for Image Encryption Using a Three-Layer Artificial Neural Network," *IETE J. Res.*, vol. 70, no. 1, pp. 473–486, Jan. 2024, doi: 10.1080/03772063.2022.2127940.

[22] K. M. Hosny, S. T. Kamal, M. M. Darwish, and G. A. Papakostas, "New image encryption algorithm using hyperchaotic system and fibonacci q-matrix," *Electron.*, vol. 10, no. 9, 2021, doi: 10.3390/electronics10091066.

[23] E. Winarno, K. Nugroho, P. W. Adi, and D. R. I. M. Setiadi, "Combined Interleaved Pattern to Improve Confusion-Diffusion Image Encryption Based on Hyperchaotic System," *IEEE Access*, vol. 11, pp. 69005–69021, 2023, doi: 10.1109/ACCESS.2023.3285481.

[24] S.-S. Yu, N.-R. Zhou, L.-H. Gong, and Z. Nie, "Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system," *Opt. Lasers Eng.*, vol. 124, p. 105816, Jan. 2020, doi: 10.1016/j.optlaseng.2019.105816.

[25] Q. Lu, L. Yu, and C. Zhu, "A New Conservative Hyperchaotic System-Based Image Symmetric Encryption Scheme with DNA Coding," *Symmetry (Basel).*, vol. 13, no. 12, p. 2317, Dec. 2021, doi: 10.3390/sym13122317.

[26] N. Tsafack, J. Kengne, B. Abd-El-Atty, A. M. Iliyasu, K. Hirota, and A. A. Abd EL-Latif, "Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption," *Inf. Sci. (Ny).*, vol. 515, pp. 191–217, Apr. 2020, doi: 10.1016/j.ins.2019.10.070.

[27] S. Zhu, X. Deng, W. Zhang, and C. Zhu, "Construction of a New 2D Hyperchaotic Map with Application in Efficient Pseudo-Random Number Generator Design and Color Image Encryption," *Mathematics*, vol. 11, no. 14, p. 3171, Jul. 2023, doi: 10.3390/math11143171.

[28] A. A. Neamah, "An image encryption scheme based on a seven-dimensional hyperchaotic system and Pascal's matrix," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 35, no. 3, pp. 238–248, Mar. 2023, doi: 10.1016/j.jksuci.2023.02.014.

[29] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of the International Conference on Computers, Systems & Signal Processing*, 1984, pp. 175–179.

[30] F. Cavaliere, J. Mattsson, and B. Smeets, "The security implications of quantum cryptography and quantum computing," *Netw. Secur.*, vol. 2020, no. 9, pp. 9–15, Sep. 2020, doi: 10.1016/S1353-4858(20)30105-7.

[31] G. Vest *et al.*, "Quantum key Distribution with a Hand-Held Sender Unit," *Phys. Rev. Appl.*, vol. 18, no. 2, p. 024067, Aug. 2022, doi: 10.1103/PhysRevApplied.18.024067.

[32] H. Shu, "Asymptotically Optimal Prepare-Measure Quantum Key Distribution Protocol," *Int. J. Theor. Phys.*, vol. 62, no. 8, pp. 1–13, 2023, doi: 10.1007/s10773-023-05447-0.

[33] R. Kuang and A. Chan, "Quantum encryption in phase space with displacement operators," *EPJ Quantum Technol.*, vol. 0, 2023, doi: 10.1140/epjqt/s40507-023-00183-0.
[34] A. A. Abdullah and S. S. Mahdi, "Implementing Quantum Image Security Algorithm Based on Geometric Transformation and Quantum Random Number Generation," *J. Eng. Sci. Technol.*, vol. 17, no. 5, pp. 3570–3582, 2022.
[35] S. Benaissi, N. Chikouche, and R. Hamza, "A novel image encryption algorithm based on hybrid chaotic maps using a key image," *Optik (Stuttg).*, vol. 272, no. November 2022, p. 170316, Feb. 2023, doi: 10.1016/j.ijleo.2022.170316.
[36] P. N. Andono and D. R. I. M. Setiadi, "Improved Pixel and Bit Confusion-Diffusion Based on Mixed Chaos and Hash Operation for Image Encryption," *IEEE Access*, vol. 10, no. November, pp. 115143–115156, 2022, doi: 10.1109/ACCESS.2022.3218886.
[37] S. Bhowmik and S. Acharyya, "Image encryption approach using improved chaotic system incorporated with differential evolution and genetic algorithm," *J. Inf. Secur. Appl.*, vol. 72, no. December 2022, p. 103391, 2023, doi: 10.1016/j.jisa.2022.103391.
[38] X. Wang, W. Xue, and J. An, "Image encryption algorithm based on Tent-Dynamics coupled map lattices and diffusion of Household," *Chaos, Solitons and Fractals*, vol. 141, p. 110309, 2020, doi: 10.1016/j.chaos.2020.110309.
[39] M. Khan and T. Shah, "A novel image encryption technique based on Hénon chaotic map and S8 symmetric group," *Neural Comput. Appl.*, vol. 25, no. 7–8, pp. 1717–1722, Dec. 2014, doi: 10.1007/s00521-014-1663-4.