mathematics

Article

Quantum Color Image Encryption Scheme Based on Geometric Transformation and Intensity Channel Diffusion

Xianhua Song [1,*], Guanglong Chen [1] and Ahmed A. Abd El-Latif [2,3]

1 School of Science, Harbin University of Science and Technology, Harbin 150080, China
2 EIAS Data Science Lab, College of Computer and Information Sciences, Prince Sultan University, Riyadh 11586, Saudi Arabia
3 Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Shebin El-Koom 32511, Egypt
* Correspondence: songxianhua@hrbust.edu.cn

Abstract: A quantum color image encryption algorithm based on geometric transformation and intensity channel diffusion was designed. Firstly, a plaintext image was transformed into a quantum state form using the quantum image representation based on HSI color space (QIRHSI) representation as a carrier. Next, a pseudo-random sequence was generated using the generalized logistic map, and the pixel positions permuted multiple two-point swap operations. Immediately afterward, the intensity values were changed by an intensity bit-plane cross-swap and XOR, XNOR operations. Finally, the intensity channel of the above image was diffused in combination with the pseudo-confusion sequence as produced by the quantum logistic map to perform a diffusion operation on the intensity bit-plane to obtain the ciphertext image. Numerical simulations and analyses show that the designed algorithm is implementable and robust, especially in terms of outstanding performance and less computational complexity than classical algorithms in terms of security perspective.

Keywords: quantum computation; quantum image encryption; intensity channel diffusion; geometric transforms; chaotic systems; plane permutation

MSC: 81P94

check for updates

Citation: Song, X.; Chen, G.; Abd El-Latif, A.A. Quantum Color Image Encryption Scheme Based on Geometric Transformation and Intensity Channel Diffusion. *Mathematics* **2022**, *10*, 3038. https://doi.org/10.3390/math10173038

Academic Editor: Lingfeng Liu

Received: 9 June 2022
Accepted: 16 July 2022
Published: 23 August 2022

1. Introduction

Given the outstanding advantages of entanglement, superposition, and parallelism, quantum computing is widely used in all aspects of information science [1–4]. Quantum information processing is a new cross-disciplinary discipline based on mathematics, physics, and computing, and has been widely used to increase the speed of information processing and enhance communication security [5–9]. Focusing on the capture, operation, and recovery of classical images for various purposes using quantum computing techniques, Quantum IMage Processing (QIMP) [10] has evolved into a hot research topic with huge storage capacity and parallel processing capability [11–14].

The first hurdle facing QIMP is how to use qubits to represent classical images in a way that can be recognized by quantum computers. Therefore, a number of quantum image representations [15–30] have been proposed, including, Qubit Lattice [15], Real Ket [16], Flexible Representation of Quantum Images (FRQI) [17], Novel Enhanced Quantum Representation of digital images (NEQR) [18], Multi-Channel Representation for Quantum Image (MCRQI) [19], QUAntum Log-Polar Image (QUALPI) [20], Flexible Quantum Representation for Color Images (FQRCI) [21], Generalized Quantum Image Representation (GQIR) [22], Quantum States for M Colors and N Coordinates of an image (QSMC&QSNC) [23], Novel Quantum representation of Color digital Images (NCQI) [24], Flexible Representation of Quantum Color Images (FRQCI) [25], Quantum Representation of Multi-Wavelength images (QRMW) [26], Improved Flexible Representation of Quantum

Images (IFRQI) [27], Quantum Representation model of Color digital Images (QRCI) [28], and Fourier Transform Qubit Representation (FTQR) [29]. Inspired by the ideas of FRQI [17] and NEQR [18], Quantum Image Representation based on the HSI color space (QIRHSI) [30] was proposed. The model encodes hue (H) and saturation (S) through two angular vectors, respectively, and a binary sequence of q bits encodes intensity (I), not only making the number of qubits required to encode color information (10 bits) smaller but also easier to perform various operations on intensity channel.

Along with the development of quantum image representation, a number of quantum image encryption algorithms [31–44] have emerged. The proposed encryption algorithms can usually be divided into spatial and frequency domains. A novel quantum gray-scale image encryption algorithm based on one-dimensional quantum cellular automata was proposed by Yang et al. [31]. Zhou et al. [32] first designed a quantum realization of the generalized Arnold transform, based on which they proposed a quantum image encryption algorithm based on the generalized Arnold transform and double random phase encoding. A new quantum color image encryption algorithm based on hyper-chaotic systems was proposed by Tan et al. [33]. Wang et al. [34] proposed a quantum image encryption and decryption algorithm based on the frequency–spatial domain transform iteration framework. Li et al. [35] designed a quantum encryption algorithm for NCQI images based on multiple discrete chaotic systems. Li et al. [36] designed a quantum gray image encryption and compression scheme based on the quantum cosine transform and five-dimensional hyperchaotic system. Li et al. [37] proposed an encryption algorithm based on NASS quantum images using the quantum geometric transform, phase-shift transform, and quantum Haar wavelet packet transform. The NEQR image encryption and decryption algorithm based on a discrete quantum walk on a circle was proposed by Abd-El-Atty et al. [38]. Abd El-Latif et al. [39] first used the controlled alternate quantum walk (CAQW) to create PRNG, and then proposed schemes for encryption of quantum color images by controlled quantum controlled NOT gates from key sequences generated by the PRNG mechanism. Jiang et al. [40] proposed a quantum image encryption scheme based on GQIR representation and two-dimensional Henon mapping. Musanna and Kumar [41] proposed an encryption algorithm for a quantum 3D Baker mapping to scramble the 3D quantum representation of an image. Zhou et al. [42] proposed a new quantum image compression and encryption algorithm with Daubechies quantum wavelet transform (DQWT) and 3D hyperchaotic Henon maps. Zhou et al. [43] proposed a quantum image encryption algorithm for improved FRQI (FRQIM) images based on Arnold scrambling and QWT. Liu, Xiao, and Liu et al. [44] proposed a novel three-level quantum image encryption algorithm based on Arnold transform and logistic maps.

In order to improve the security of quantum encrypted images, this paper presents a color image encryption algorithm based on the QIRHSI representation of geometric transformation and intensity channel diffusion. The main contributions of the work in this paper are highlighted as follows: (1) The application of two-point swapping and a generalized logistic map to permutated pixel planes further improves security. (2) Cross-swapping and XOR, XNOR operations are applied to the intensity bit-plane to change the intensity values. (3) The quantum logistic map is used to diffuse the intensity to obtain the desired encryption effect.

The remainder of this paper is organized as follows. Section 2 is devoted to the QIRHSI representation model, geometric transform, generalized logistic map, and quantum logistic map. The proposed quantum image encryption and decryption scheme are discussed in Section 3. Section 4 provides numerical simulations and a security analysis. Finally, conclusions and future research work are presented in Section 5.

2. Background Knowledge

2.1. QIRHSI Representation Model

QIRHSI [30] was developed from the FRQI [17] and NEQR [18] models, where FRQI uses a qubit encoded by an angle parameter and NEQR uses an entangled sequence of qubits to store grayscale information. The QIRHSI model encodes hue (H) and saturation (S) information with two angles; intensity (I) and position information are represented by an entangled sequence of qubits, respectively. The QIRHSI color image is defined as

$$|I(\theta)\rangle = \frac{1}{2^n}\sum_{k=0}^{2^{2n}-1}|C_k\rangle \otimes |k\rangle = \frac{1}{2^n}\sum_{k=0}^{2^{2n}-1}|H_k\rangle|S_k\rangle|I_k\rangle \otimes |k\rangle, \tag{1}$$

wherein,

$$\begin{aligned} |H_k\rangle &= \cos\theta_{hk}|0\rangle + \sin\theta_{hk}|1\rangle \\ |S_k\rangle &= \cos\theta_{sk}|0\rangle + \sin\theta_{sk}|1\rangle \\ |I_k\rangle &= \left|C_k^0 C_k^1 \ldots C_k^{q-2} C_k^{q-1}\right\rangle \end{aligned} \tag{2}$$

$$\begin{gathered} \theta_{hk}, \theta_{sk} \in \left[0, 2^{-1}\pi\right],\ C_k^j \in \{0,1\} \\ j = 0,1,\ldots,q-1 \\ k = 0,1,\ldots,2^{2n}-1 \end{gathered} \tag{3}$$

Equation (2) implies that the intensity I_k takes values in the range $[0, 2^q - 1]$. Thus, for an image of size $2^n \times 2^n$, the total number of qubits required for QIRHSI is $2n + q + 2$. A $2^1 \times 2^1$ QIRHSI image and representation are presented in Figure 1.

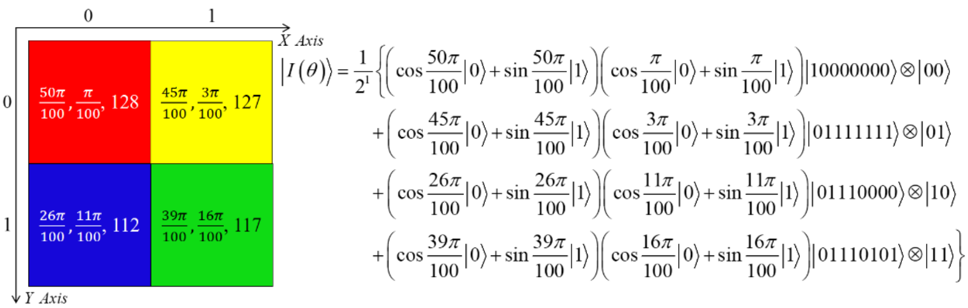


Figure 1. A $2^1 \times 2^1$ QIRHSI image and representation.

Obviously, it can be seen from Equation (2) that the 256 intensity values consist of 8 bits, so the intensity channel of the QIRHSI image can be decomposed into 8 bit planes, as indicated in Figure 2.

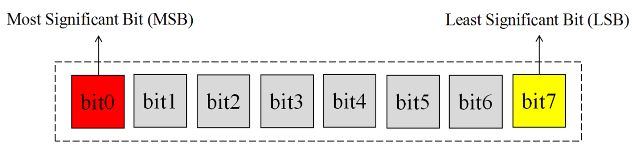


Figure 2. Bit-plane of the intensity channel of the QIRHSI image.

2.2. Quantum Geometric Transformations of QIRHSI

Reference [45] investigates quantum geometric transformations based on the QIRHSI model, including two-point swapping, circular translation, flipping transformation, and right-angle rotation.

Definition 1. *The two-point swap operation G_P acts on the two positions i, j of the QIRHSI image as follows*

$$G_P(|I(\theta)\rangle) = \frac{1}{2^n}\sum_{k=0}^{2^{2n}-1}|C_k\rangle \otimes P(|k\rangle) = \frac{1}{2^n}\left\{|C_i\rangle \otimes |j\rangle + |C_j\rangle \otimes |i\rangle + \sum_{k=0,k\neq i,j}^{2^{2n}-1}|C_k\rangle \otimes |k\rangle\right\},$$

of which $P(|k\rangle) = |k\rangle$, $k \neq i,\ j$ *and* $P(|i\rangle) = |j\rangle$, $P(|j\rangle) = |i\rangle$. *Therefore*

$$G_P = I^{\otimes 2} \otimes I^{\otimes q} \otimes P = I^{\otimes 2} \otimes I^{\otimes q} \otimes \left\{ |i\rangle\langle j| + |j\rangle\langle i| + \sum_{k=0,k\neq i,j}^{2^{2n}-1} |k\rangle\langle k| \right\}.$$

The complexity of the elementary quantum gate needed for the two-point swapping operator G_P for the quantum color image QIRHSI of size $2^n \times 2^n$ is $O(n^2)$ [45].

2.3. Generalized Logistic Map

Jafarizadeh and Behnia [46] both introduced a hierarchy of one-parameter families of chaotic mappings with invariant measures and generated generalized logistic mappings by appropriate coupling. Equation (4) defines the generalized logistic map as

$$w_{\delta+1} = \frac{4\eta^2 w_\delta (1 - w_\delta)}{1 + 4(\eta^2 - 1) w_\delta (1 - w_\delta)}, \tag{4}$$

where $w_0 \in [0, 1]$ is the initial value and η is the parameter. When $\eta \in [-4, -2] \cup [2, 4]$, the sequence computed by the generalized logistic map is pseudo-random, and Equation (4) is in a chaotic state [47].

2.4. Quantum Logistic Map

Quantum logistic mappings have many of the excellent properties of traditional chaotic systems, such as sensitivity to initial values. Quantum chaos mapping was proposed in [48], which is defined as

$$\begin{cases} x_{n+1} = \gamma\left(x_n - |x_n|^2\right) - \gamma y_n \\ y_{n+1} = -y_n e^{-2\beta} + e^{-\beta}\gamma[(2 - x_n - \overline{x}_n) y_n - x_n \overline{z}_n - \overline{x}_n z_n] \\ z_{n+1} = -z_n e^{-2\beta} + e^{-\beta}\gamma[2(1 - \overline{x}_n) z_n - 2x_n y_n - x_n] \end{cases}, \tag{5}$$

where β and γ are parameters. $\overline{x}_n$ and $\overline{z}_n$ are the conjugate complexes of x_n and z_n, respectively. When $x_n \in [0, 1]$, $y_n \in [0, 0.1]$, $z_n \in [0, 0.2]$, $\beta \in [6, +\infty)$, and $\gamma \in [0, 4]$, Equation (5) is in a chaotic state, and the quantum logistic map generates a pseudo-random sequence [49], which is used in the image encryption [50–52].

3. Quantum Color Image Encryption and Decryption

The novel quantum image encryption scheme constructed in this paper includes three steps. Firstly, the location information in the spatial domain is permuted using a generalized logistic map and two-point swap. Secondly, the intensity value is changed by the intensity bit-plane cross-swap and XOR, XNOR operations. Finally, the intensity values are diffused using a quantum logistic map to acquire the encrypted quantum image. Figure 3 presents the flow chart of the quantum color image encryption and decryption algorithm.

Assuming that the original color image to be encrypted is represented as $|I(\theta)\rangle$ (where q equals 8), its QIRHSI state is:

$$\begin{aligned} |I(\theta)\rangle &= \tfrac{1}{2^n} \sum_{k=0}^{2^{2n}-1} |H_k\rangle |S_k\rangle |I_k\rangle \otimes |k\rangle \\ &= \tfrac{1}{2^n} \sum_{k=0}^{2^{2n}-1} (\cos\theta_{hk}|0\rangle + \sin\theta_{hk}|1\rangle)(\cos\theta_{sk}|0\rangle + \sin\theta_{sk}|1\rangle) \left|C_k^0 C_k^1 \ldots C_k^7\right\rangle \otimes |k\rangle \end{aligned}$$

where $\theta_{hk}, \theta_{sk} \in \left[0, 2^{-1}\pi\right]$, $C_k^l \in \{0, 1\}$, $l = 0, 1, \ldots, 7$, $k = 0, 1, \ldots, 2^{2n} - 1$.

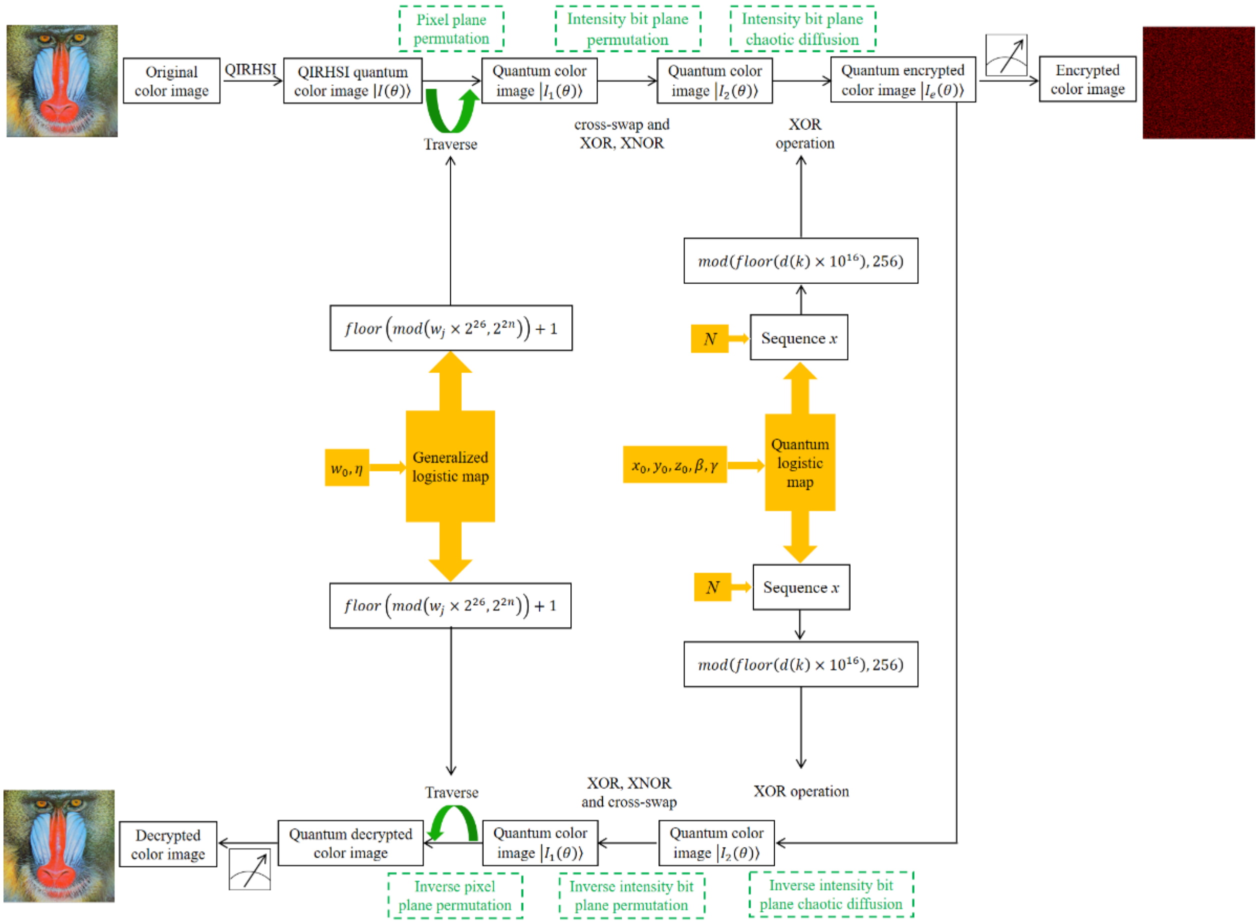


Figure 3. Diagram of the flow of the QIRHSI image encryption and decryption scheme.

3.1. Image Encryption Scheme

(1) Pixel plane permutation.

Step 1: We compute the integers with the help of $i_0 = floor(\mathrm{mod}(w_0 \times 2^{26}, 2^{2n})) + 1$, where function $floor(\cdot)$ denotes the downward rounding operation.

Step 2: Using the initial value w_0 and parameter η iterating Equation (4), w_l is obtained. $i_l = floor(\mathrm{mod}(w_l \times 2^{26}, 2^{2n})) + 1$ is then calculated.

Step 3: If $i_l \neq i_j$ for all $j = 0, 1, \ldots, l-1$, then store i_l; otherwise, there exists a j such that $i_l = i_j$, and we use Equation (4) to compute the next w_{l+1} until we obtain all different $i_j, j = 0, 1, \ldots, 2^{2n} - 1$, obtained by $i_j = floor(\mathrm{mod}(w_j \times 2^{26}, 2^{2n})) + 1$.

Step 4: The operation of swapping two adjacent pixel positions $|i_{2m}\rangle$ and $|i_{2m+1}\rangle$, $m = 0, 1, \ldots, 2^{2n-1} - 1$ on the QIRHSI image is shown in Equation (6).

$$\begin{aligned} G_{P_m} &= I^{\otimes 2} \otimes I^{\otimes 8} \otimes P_m \\ &= I^{\otimes 2} \otimes I^{\otimes 8} \otimes \left\{ |i_{2m}\rangle\langle i_{2m+1}| + |i_{2m+1}\rangle\langle i_{2m}| + \sum_{k=0, k\neq i_{2m}, i_{2m+1}}^{2^{2n}-1} |k\rangle\langle k| \right\} \end{aligned} \tag{6}$$

The operation G_{P_m} is applied to the QIRHSI image to obtain

$$\begin{aligned} G_{P_m}(|I(\theta)\rangle) &= \frac{1}{2^n} G_{P_m} \left\{ \sum_{k=0}^{2^{2n}-1} |C_k\rangle \otimes |k\rangle \right\} \\ &= \frac{1}{2^n} \left\{ |C_{i_{2m}}\rangle \otimes |i_{2m+1}\rangle + |C_{i_{2m+1}}\rangle \otimes |i_{2m}\rangle + \sum_{k=0, k\neq i_{2m}, i_{2m+1}}^{2^{2n}-1} |C_k\rangle \otimes |k\rangle \right\} \end{aligned} \tag{7}$$

We use Equation (7) twice to obtain Equation (8).

$$\begin{aligned} G_{P_l}G_{P_m}(|I(\theta)\rangle) &= \frac{1}{2^n}G_{P_l}G_{P_m}\left\{\sum_{k=0}^{2^{2n}-1}|C_k\rangle\otimes|k\rangle\right\} \\ &= \frac{1}{2^n}\Big\{|C_{i_{2m}}\rangle\otimes|i_{2m+1}\rangle+|C_{i_{2m+1}}\rangle\otimes|i_{2m}\rangle+|C_{i_{2l}}\rangle\otimes|i_{2l+1}\rangle+\left|C_{i_{2l+1}}\right\rangle\otimes|i_{2l}\rangle \\ &\quad+\sum_{k=0,k\neq i_{2m},i_{2m+1},i_{2l},i_{2l+1}}^{2^{2n}-1}|C_k\rangle\otimes|k\rangle\Big\} \end{aligned} \tag{8}$$

For a total pixel position of 2^{2n}, only 2^{2n-1} swaps are needed to traverse all pixel positions. From Equation (8), we can obtain

$$\begin{aligned} G(|I(\theta)\rangle) &= \prod_{k=0}^{2^{2n-1}-1}G_{P_k}(|I(\theta)\rangle) \\ &= \frac{1}{2^n}\Big\{|C_{i_0}\rangle\otimes|i_1\rangle+|C_{i_1}\rangle\otimes|i_0\rangle+|C_{i_2}\rangle\otimes|i_3\rangle+|C_{i_3}\rangle\otimes|i_2\rangle+\ldots+ \\ &\quad\left|C_{i_{2^{2n}-4}}\right\rangle\otimes\left|i_{2^{2n}-3}\right\rangle+\left|C_{i_{2^{2n}-3}}\right\rangle\otimes\left|i_{2^{2n}-4}\right\rangle+\left|C_{i_{2^{2n}-2}}\right\rangle\otimes\left|i_{2^{2n}-1}\right\rangle+\left|C_{i_{2^{2n}-1}}\right\rangle\otimes\left|i_{2^{2n}-2}\right\rangle\Big\} \\ &= \frac{1}{2^n}\sum_{k=0}^{2^{2n-1}-1}\left\{\left|C_{i_{2k}}\right\rangle\otimes|i_{2k+1}\rangle+\left|C_{i_{2k+1}}\right\rangle\otimes|i_{2k}\rangle\right\} \\ &= \frac{1}{2^n}\sum_{j=0}^{2^{2n}-1}\left|C_{i_j}\right\rangle\otimes\left|i_{j'}\right\rangle \\ &= \frac{1}{2^n}\sum_{j=0}^{2^{2n}-1}\left|H_{i_j}\right\rangle\left|S_{i_j}\right\rangle\left|I_{i_j}\right\rangle\otimes\left|i_{j'}\right\rangle \\ &= |I_1(\theta)\rangle \end{aligned} \tag{9}$$

Among them,

$$j' = j+(-1)^j = \begin{cases} j+1, & j=0,2,4,\ldots,2^{2n}-2 \\ j-1, & j=1,3,5,\ldots,2^{2n}-1 \end{cases}.$$

(2) Intensity bit-plane permutation.

The intensity bit-plane is intended to "tamper" with the intensity value at pixel position k. The intensity bit-plane cross-swap operation and XOR, XNOR operation are two ways in which the intensity bit-plane can be permuted. Quantum circuits for intensity bit-plane cross-swap operations are given Figures 4 and 5, presenting quantum circuits for intensity bit-plane XOR, XNOR operations. The intensity bit-plane cross-swap operation will cause the intensity bit-planes to be misaligned. Applying the U operator shown in Figure 5 to $\left|I_{i_j}\right\rangle$ yields $\left|I'_{i_j}\right\rangle$.

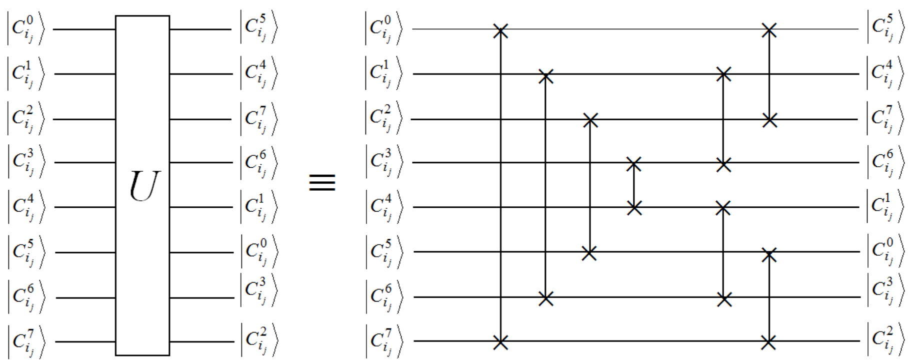


Figure 4. Quantum circuits for intensity bit-plane cross-swap operations.

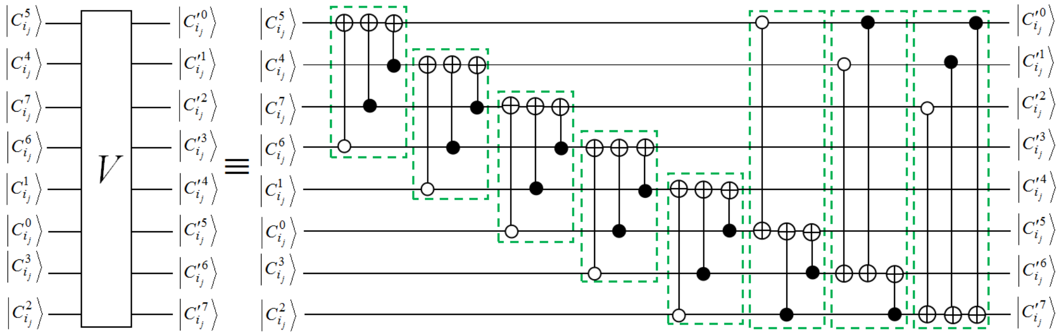


Figure 5. Quantum circuit diagram for intensity bit-plane XOR, XNOR operation.

For an arbitrary pixel location $i_{j'}$, the operator U is defined to act on $\left|I_{i_j}\right\rangle$ as follows.

$$U\left|I_{i_j}\right\rangle = U\left|C_{i_j}^0 C_{i_j}^1 \dots C_{i_j}^7\right\rangle = \left|C_{i_j}^5 C_{i_j}^4 C_{i_j}^7 C_{i_j}^6 C_{i_j}^1 C_{i_j}^0 C_{i_j}^3 C_{i_j}^2\right\rangle. \tag{10}$$

Applying the operator V shown in Figure 5 to Equation (10) in the intensity bit-plane XOR, XNOR operation gives $\left|I'_{i_j}\right\rangle$. We define the operator V as shown in Equation (11).

$$V\left(U\left|I_{i_j}\right\rangle\right) = V\left|C_{i_j}^5 C_{i_j}^4 C_{i_j}^7 C_{i_j}^6 C_{i_j}^1 C_{i_j}^0 C_{i_j}^3 C_{i_j}^2\right\rangle = \left|C_{i_j}^{\prime 0} C_{i_j}^{\prime 1} \dots C_{i_j}^{\prime 7}\right\rangle = \left|I'_{i_j}\right\rangle. \tag{11}$$

It should be specified that the 8-layer bit-plane representation of $\left|I'_{i_j}\right\rangle$ is as follows:

$$\begin{array}{ll}
\left|C_{i_j}^{\prime 0}\right\rangle = \left|\sim C_{i_j}^5 \oplus C_{i_j}^6 \oplus C_{i_j}^7 \oplus C_{i_j}^4\right\rangle, & \left|C_{i_j}^{\prime 1}\right\rangle = \left|\sim C_{i_j}^4 \oplus C_{i_j}^1 \oplus C_{i_j}^6 \oplus C_{i_j}^7\right\rangle \\
\left|C_{i_j}^{\prime 2}\right\rangle = \left|\sim C_{i_j}^7 \oplus C_{i_j}^0 \oplus C_{i_j}^1 \oplus C_{i_j}^6\right\rangle, & \left|C_{i_j}^{\prime 3}\right\rangle = \left|\sim C_{i_j}^6 \oplus C_{i_j}^3 \oplus C_{i_j}^0 \oplus C_{i_j}^1\right\rangle \\
\left|C_{i_j}^{\prime 4}\right\rangle = \left|\sim C_{i_j}^1 \oplus C_{i_j}^2 \oplus C_{i_j}^3 \oplus C_{i_j}^0\right\rangle, & \left|C_{i_j}^{\prime 5}\right\rangle = \left|\sim C_{i_j}^0 \oplus C_{i_j}^{\prime 0} \oplus C_{i_j}^2 \oplus C_{i_j}^3\right\rangle \\
\left|C_{i_j}^{\prime 6}\right\rangle = \left|\sim C_{i_j}^3 \oplus C_{i_j}^{\prime 1} \oplus C_{i_j}^{\prime 0} \oplus C_{i_j}^2\right\rangle, & \left|C_{i_j}^{\prime 7}\right\rangle = \left|\sim C_{i_j}^2 \oplus C_{i_j}^{\prime 2} \oplus C_{i_j}^{\prime 1} \oplus C_{i_j}^{\prime 0}\right\rangle
\end{array}$$

Therefore, the intensity bit-plane permutation operator F can be defined as Equation (12),

$$F = \left(I^{\otimes 2} \otimes V \otimes I^{\otimes 2n}\right) \cdot \left(I^{\otimes 2} \otimes U \otimes I^{\otimes 2n}\right), \tag{12}$$

and acting the operator F on the image $|I_1(\theta)\rangle$ gives

$$\begin{aligned}
F(|I_1(\theta)\rangle) &= \tfrac{1}{2^n} F\left\{\sum_{j=0}^{2^{2n}-1} \left|C_{i_j}\right\rangle \otimes \left|i_{j'}\right\rangle\right\} \\
&= \tfrac{1}{2^n} \sum_{j=0}^{2^{2n}-1} \left|H_{i_j}\right\rangle \left|S_{i_j}\right\rangle \otimes V\left(U\left|I_{i_j}\right\rangle\right) \otimes \left|i_{j'}\right\rangle \\
&= \tfrac{1}{2^n} \sum_{j=0}^{2^{2n}-1} \left|H_{i_j}\right\rangle \left|S_{i_j}\right\rangle \left|C_{i_j}^{\prime 0} C_{i_j}^{\prime 1} \dots C_{i_j}^{\prime 7}\right\rangle \otimes \left|i_{j'}\right\rangle \\
&= \tfrac{1}{2^n} \sum_{j=0}^{2^{2n}-1} \left|H_{i_j}\right\rangle \left|S_{i_j}\right\rangle \left|I'_{i_j}\right\rangle \otimes \left|i_{j'}\right\rangle \\
&= |I_2(\theta)\rangle
\end{aligned} \tag{13}$$

(3) Intensity bit-plane chaotic diffusion

The intensity bit-plane chaotic diffusion operation is done with the help of the chaotic sequence produced by the quantum logistic map given in Equation (5). Using the given initial values x_0, y_0, z_0 and parameters β, γ, Equation (5) will produce three chaotic sequences. Here, we only take the pseudo-random sequence $\{d(k)|k = 1, 2, \dots, N, N+1, \dots, N+2^{2n}\}$

generated by x, discarding the first N values to avoid transient effects. Since the elements in $\{d(k)\}$ take values in the range $[0,1]$, the elements in $\{d(k)\}$ are converted to integers by Equation (14).

$$d_k = \mathrm{mod}\Big(floor\Big(d(k) \times 10^{16}\Big), 256\Big). \tag{14}$$

The quantum operations in the quantum color image intensity bit-plane chaotic diffusion stage can divide into 4^n XOR sub-operations to achieve XOR operations on the intensity of each pixel. To implement the sub-operation, the sequence $D = \{d_1, d_2, \ldots, d_{2^{2n}}\}$ to control the NOT operation, where $d_k = d_k^0 d_k^1 \ldots d_k^7$, $d_k^m \in \{0,1\}$, $m = 0,1,\ldots,7$, $k = 0,1,\ldots,2^{2n}-1$. The operation W is defined in Equation (15). If d_k^m is equal to 1, then W_k is a NOT operation; otherwise, it is an identity operation I.

$$W_k = W_k^0 W_k^1 \ldots W_k^7. \tag{15}$$

Thus, the XOR operation of the intensity of the image $|I_2(\theta)\rangle$ can be realized by the operation W_k.

$$W_k\left|I'_{i_k}\right\rangle = \bigotimes_{m=0}^{7}\left(W_k^m\left|C'^m_{i_k}\right\rangle\right) = \bigotimes_{m=0}^{7}\left|C'^m_{i_k} \oplus W_k^m\right\rangle = \bigotimes_{m=0}^{7}\left|C''^m_{i_k}\right\rangle = \left|I''_{i_k}\right\rangle. \tag{16}$$

Then, the operation L_k is constructed from the XOR operation W_k, as shown in Equation (16).

$$L_k = I^{\otimes 2} \otimes I^{\otimes 8} \otimes \sum_{j=0, j\neq k}^{2^{2n}-1}\left|i_{j'}\right\rangle\left\langle i_{j'}\right| + I^{\otimes 2} \otimes W_k \otimes |i_{k'}\rangle\langle i_{k'}|. \tag{17}$$

The XOR operation on the intensity information can be implemented through the sub-operation L_k. The quantum circuit for the chaotic diffusion of the intensity bit-plane is seen in Figure 6.

$$\begin{aligned}
L_k(|I_2(\theta)\rangle) &= \frac{1}{2^n} L_k\left\{\sum_{j=0}^{2^{2n}-1}\left|H_{i_j}\right\rangle\left|S_{i_j}\right\rangle\left|I'_{i_j}\right\rangle \otimes \left|i_{j'}\right\rangle\right\} \\
&= \frac{1}{2^n}\left\{\sum_{j=0, j\neq k}^{2^{2n}-1}\left|H_{i_j}\right\rangle\left|S_{i_j}\right\rangle\left|I'_{i_j}\right\rangle \otimes \left|i_{j'}\right\rangle + |H_{i_k}\rangle|S_{i_k}\rangle \otimes W_k\left|C'^0_{i_k}C'^1_{i_k}\ldots C'^7_{i_k}\right\rangle \otimes |i_{k'}\rangle\right\} \\
&= \frac{1}{2^n}\left\{\sum_{j=0, j\neq k}^{2^{2n}-1}\left|H_{i_j}\right\rangle\left|S_{i_j}\right\rangle\left|I'_{i_j}\right\rangle \otimes \left|i_{j'}\right\rangle + |H_{i_k}\rangle|S_{i_k}\rangle \otimes \left|C''^0_{i_k}C''^1_{i_k}\ldots C''^7_{i_k}\right\rangle \otimes |i_{k'}\rangle\right\} \\
&= \frac{1}{2^n}\left\{\sum_{j=0, j\neq k}^{2^{2n}-1}\left|H_{i_j}\right\rangle\left|S_{i_j}\right\rangle\left|I'_{i_j}\right\rangle \otimes \left|i_{j'}\right\rangle + |H_{i_k}\rangle|S_{i_k}\rangle\left|I''_{i_k}\right\rangle \otimes |i_{k'}\rangle\right\}
\end{aligned} \tag{18}$$

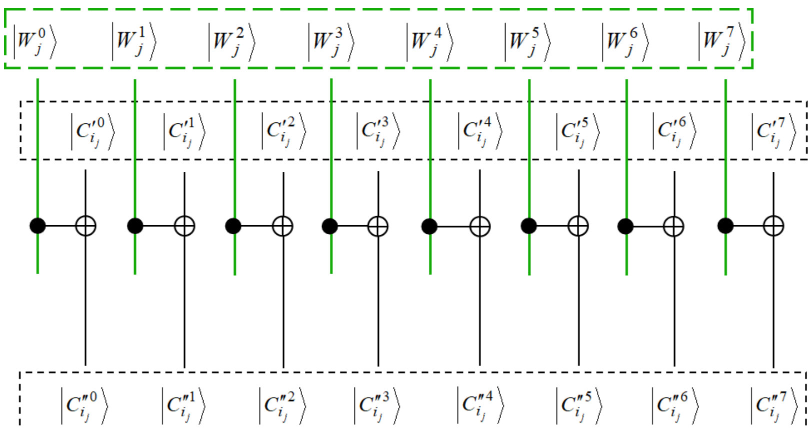


Figure 6. Intensity bit-plane chaotic diffusion in quantum circuits.

When $j = k,\ m$, we apply it to the image $|I_2(\theta)\rangle$, and obtain

$$\begin{aligned}
L_m L_k(|I_2(\theta)\rangle) &= \frac{1}{2^n} L_m L_k \left\{ \sum_{j=0}^{2^{2n}-1} \left|H_{i_j}\right\rangle \left|S_{i_j}\right\rangle \left|I'_{i_j}\right\rangle \otimes \left|i_{j'}\right\rangle \right\} \\
&= \frac{1}{2^n} \left\{ \sum_{j=0, j\neq k,m}^{2^{2n}-1} \left|H_{i_j}\right\rangle \left|S_{i_j}\right\rangle \left|C'^0_{i_j} C'^1_{i_j} \ldots C'^7_{i_j}\right\rangle \otimes \left|i_{j'}\right\rangle + \right. \\
&\left. |H_{i_m}\rangle |S_{i_m}\rangle \left|C''^0_{i_m} C''^1_{i_m} \ldots C''^7_{i_m}\right\rangle \otimes |i_{m'}\rangle + |H_{i_k}\rangle |S_{i_k}\rangle \left|C''^0_{i_k} C''^1_{i_k} \ldots C''^7_{i_k}\right\rangle \otimes |i_{k'}\rangle \right\} \\
&= \frac{1}{2^n} \left\{ \sum_{j=0, j\neq k,m}^{2^{2n}-1} \left|H_{i_j}\right\rangle \left|S_{i_j}\right\rangle \left|I'_{i_j}\right\rangle \otimes \left|i_{j'}\right\rangle + \right. \\
&\left. |H_{i_m}\rangle |S_{i_m}\rangle \left|I''_{i_m}\right\rangle \otimes |i_{m'}\rangle + |H_{i_k}\rangle |S_{i_k}\rangle \left|I''_{i_k}\right\rangle \otimes |i_{k'}\rangle \right\}
\end{aligned} \tag{19}$$

From Equation (18), it follows that

$$\begin{aligned}
L(|I_2(\theta)\rangle) &= \prod_{j=0}^{2^{2n}-1} L_j(|I_2(\theta)\rangle) \\
&= \frac{1}{2^n} \sum_{j=0}^{2^{2n}-1} \left|H_{i_j}\right\rangle \left|S_{i_j}\right\rangle \left|C''^0_{i_j} C''^1_{i_j} \ldots C''^7_{i_j}\right\rangle \otimes \left|i_{j'}\right\rangle \\
&= \frac{1}{2^n} \sum_{j=0}^{2^{2n}-1} \left|H_{i_j}\right\rangle \left|S_{i_j}\right\rangle \left|I''_{i_j}\right\rangle \otimes \left|i_{j'}\right\rangle \\
&\triangleq |I_e(\theta)\rangle
\end{aligned} \tag{20}$$

3.2. Image Decryption Scheme

The whole encryption process is reversible because the quantum operation satisfies the unitary property. It is possible to recover the original image exactly. In the decryption scheme, there are three stages: inverse intensity bit-plane chaotic diffusion, inverse intensity bit-plane permutation, and inverse pixel plane permutation. The details are developed below.

(1) Inverse intensity bit-plane chaotic diffusion.

The image $|I_2(\theta)\rangle$ is obtained using the same pseudo-random sequence generated during the chaotic diffusion of the intensity bit-plane. Applying the operator L^{-1} to the ciphertext image $|I_e(\theta)\rangle$ gives

$$\begin{aligned}
L^{-1}(|I_e(\theta)\rangle) &= \frac{1}{2^n} \prod_{j=0}^{2^{2n}-1} L_j^{-1} \left\{ \sum_{j=0}^{2^{2n}-1} \left|H_{i_j}\right\rangle \left|S_{i_j}\right\rangle \left|I''_{i_j}\right\rangle \otimes \left|i_{j'}\right\rangle \right\} \\
&= \frac{1}{2^n} \prod_{j=0}^{2^{2n}-1} L_j^{-1} \left\{ \sum_{j=0}^{2^{2n}-1} \left|H_{i_j}\right\rangle \left|S_{i_j}\right\rangle \left|C''^0_{i_j} C''^1_{i_j} \ldots C''^7_{i_j}\right\rangle \otimes \left|i_{j'}\right\rangle \right\} \\
&= \frac{1}{2^n} \sum_{j=0}^{2^{2n}-1} \left|H_{i_j}\right\rangle \left|S_{i_j}\right\rangle \left|C'^0_{i_j} C'^1_{i_j} \ldots C'^7_{i_j}\right\rangle \otimes \left|i_{j'}\right\rangle \\
&= \frac{1}{2^n} \sum_{j=0}^{2^{2n}-1} \left|H_{i_j}\right\rangle \left|S_{i_j}\right\rangle \left|I'_{i_j}\right\rangle \otimes \left|i_{j'}\right\rangle \\
&= |I_2(\theta)\rangle
\end{aligned}$$

(2) Inverse intensity bit-plane permutation.

The operator F^{-1} acts on the image $|I_2(\theta)\rangle$ as follows to give $|I_1(\theta)\rangle$.

$$\begin{aligned}
F^{-1}(|I_2(\theta)\rangle) &= \frac{1}{2^n}F^{-1}\left\{\sum_{j=0}^{2^{2n}-1}\left|H_{i_j}\right\rangle\left|S_{i_j}\right\rangle\left|I'_{i_j}\right\rangle\otimes\left|i_{j'}\right\rangle\right\} \\
&= \frac{1}{2^n}\sum_{j=0}^{2^{2n}-1}F^{-1}\left\{\left|H_{i_j}\right\rangle\left|S_{i_j}\right\rangle\left|C'^0_{i_j}C'^1_{i_j}\ldots C'^7_{i_j}\right\rangle\otimes\left|i_{j'}\right\rangle\right\} \\
&= \frac{1}{2^n}\sum_{j=0}^{2^{2n}-1}\left|H_{i_j}\right\rangle\left|S_{i_j}\right\rangle\left|C^0_{i_j}C^1_{i_j}\ldots C^7_{i_j}\right\rangle\otimes\left|i_{j'}\right\rangle \\
&= \frac{1}{2^n}\sum_{j=0}^{2^{2n}-1}\left|H_{i_j}\right\rangle\left|S_{i_j}\right\rangle\left|I_{i_j}\right\rangle\otimes\left|i_{j'}\right\rangle \\
&= |I_1(\theta)\rangle
\end{aligned}$$

(3) Inverse pixel plane permutation

The original image $|I(\theta)\rangle$ was obtained using the same pseudo-random sequence generated during the pixel plane permutation. Performing the operation G^{-1} on the image $|I_1(\theta)\rangle$ yields

$$\begin{aligned}
G^{-1}(|I_1(\theta)\rangle) &= \prod_{j=0}^{2^{2n-1}-1}\frac{1}{2^n}G^{-1}_{P_j}\left\{\sum_{k=0}^{2^{2n-1}-1}\left(\left|C_{i_{2k}}\right\rangle\otimes|i_{2k+1}\rangle+\left|C_{i_{2k+1}}\right\rangle\otimes|i_{2k}\rangle\right)\right\} \\
&= \frac{1}{2^n}\sum_{k=0}^{2^{2n}-1}|C_k\rangle\otimes|k\rangle \\
&\triangleq |I(\theta)\rangle
\end{aligned}$$

4. Numerical Simulation and Analysis

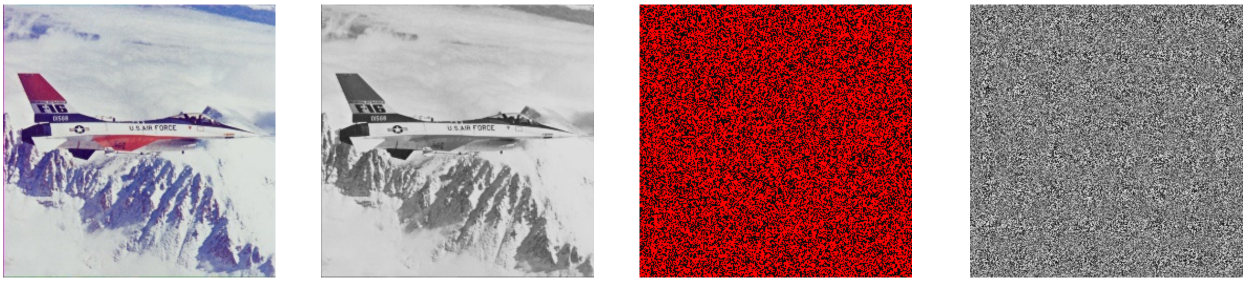
The current conditions do not allow the use of quantum computers to store and manipulate quantum states, so we simulated the experiments on a conventional computer with the help of MATLAB. In this paper, we used a laptop computer with Intel(R) Core(TM) i5-3230M CPU @2.60 GHz, 4 GB RAM, and a 64-bit operating system with MATLAB software 2018a installed for the simulation experiments. Airplane, Baboon, House, Peppers, Sailboat, and Splash are six test images [53] of size 512 × 512, as seen in the first column of Figure 7. The intensity channels of the test images are given in the second column of Figure 7. Initial values $w_0 = 0.9969$, $x_0 = 0.4634$, $y_0 = 0.0453$, $z_0 = 0.0021$ and parameters $\eta = 3.999$, $\beta = 29$, $\gamma = 3.99$, $N = 513$ are set. The third column of Figure 7 gives the encrypted image. The encrypted image intensity is seen in the last column of Figure 7.

4.1. Statistical and Differential Analysis

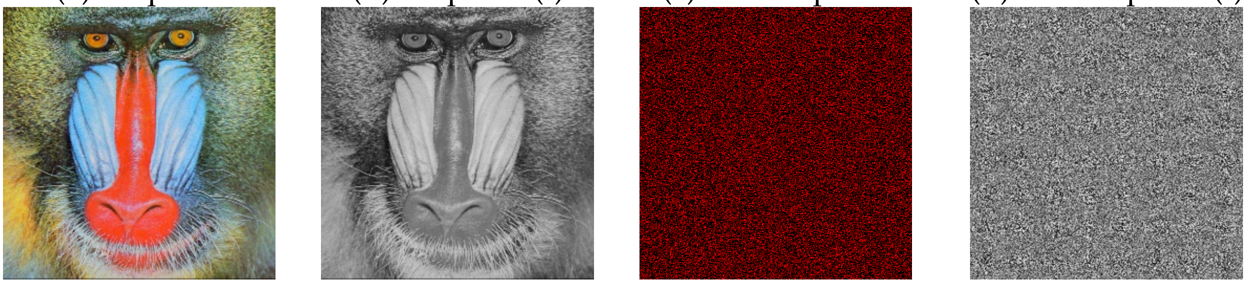
The statistical analysis of encrypted images is an extremely important metric for measuring encryption algorithms [54,55]. To clearly portray the strengths and weaknesses of encryption algorithms, statistical and differential analyses of the designed algorithm were performed, including histogram analysis, Shannon entropy analysis, correlation of adjacent pixels, NPCR and UACI analyses, spectrum analysis, and MSE and PSNR analyses.

4.1.1. Histogram Analysis

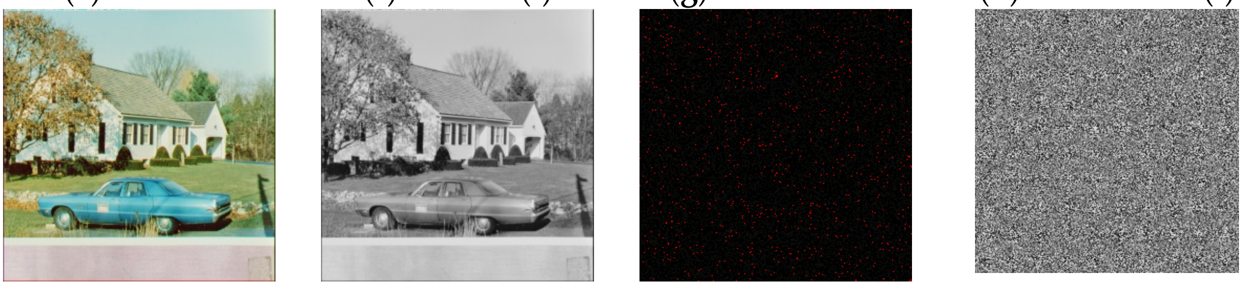
The histogram provides a visual representation of how the image pixels are situated in terms of their grayscale values. Figure 8A–F present the histograms of the intensity channels of the plaintext image in order, and (a–f) show the histograms of the intensity channels of the ciphertext image step by step. The results show that the histograms of the intensity channels of the plaintext images are high and low, while the histograms of the intensity channels of the ciphertext images are well-proportioned.



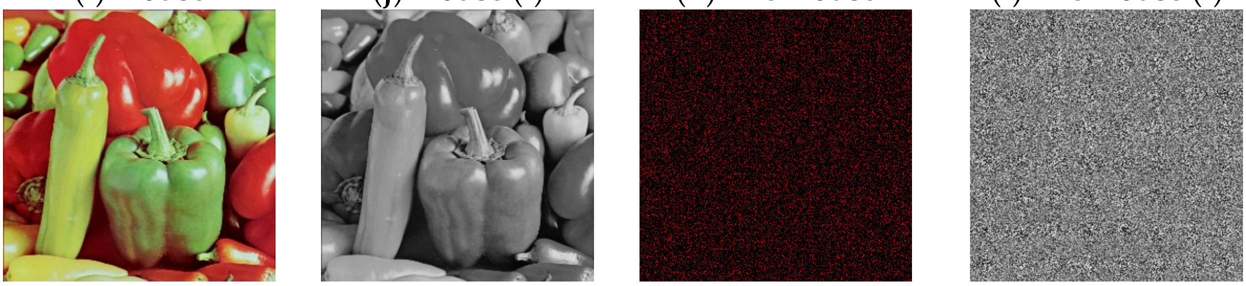
(**a**) Airplane (**b**) Airplane (I) (**c**) Enc Airplane (**d**) Enc Airplane (I)



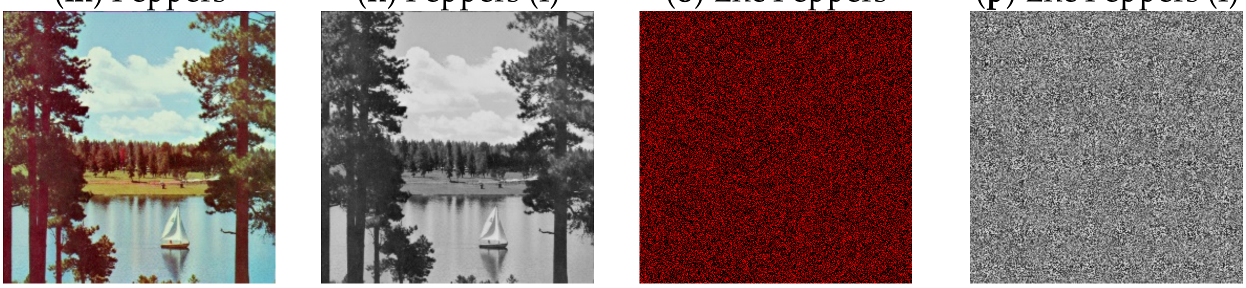
(**e**) Baboon (**f**) Baboon (I) (**g**) Enc Baboon (**h**) Enc Baboon (I)



(**i**) House (**j**) House (I) (**k**) Enc House (**l**) Enc House (I)

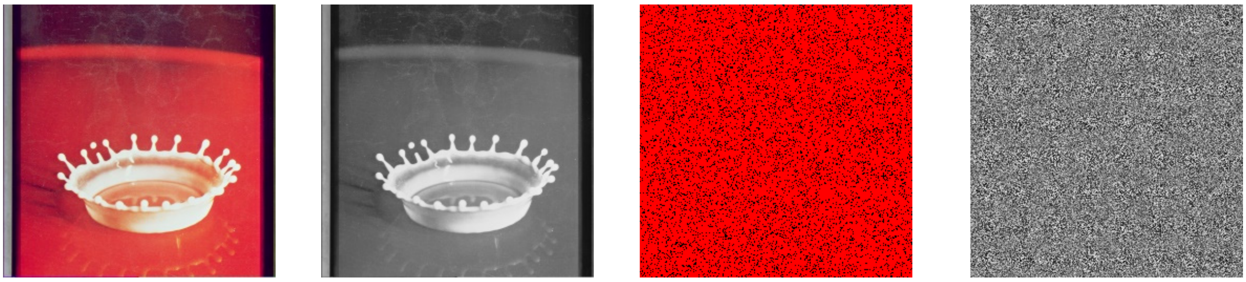


(**m**) Peppers (**n**) Peppers (I) (**o**) Enc Peppers (**p**) Enc Peppers (I)



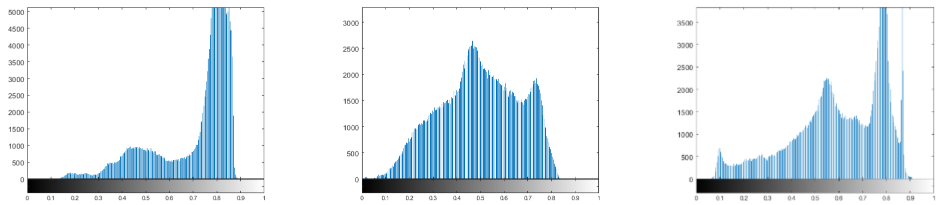
(**q**) Sailboat (**r**) Sailboat (I) (**s**) Enc Sailboat (**t**) Enc Sailboat (I)

Figure 7. *Cont.*

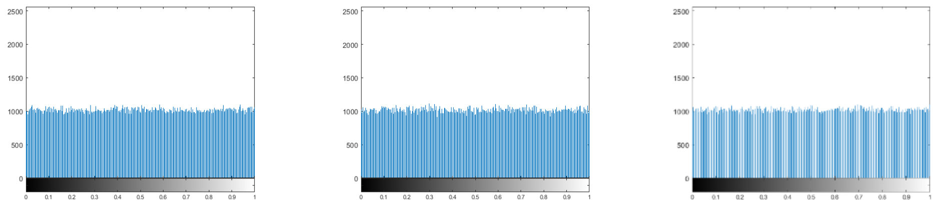


(**u**) Splash (**v**) Splash (I) (**w**) Enc Splash (**x**) Enc Splash (I)

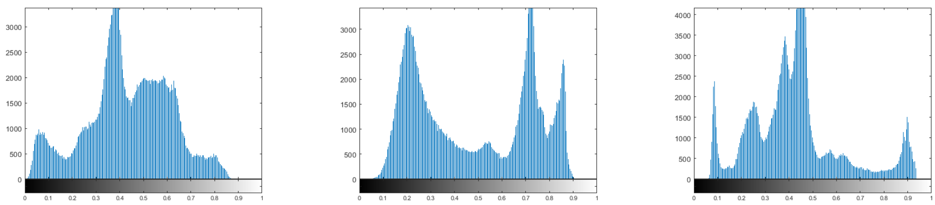
Figure 7. Results of the six test images under the encryption algorithm. The first column shows the plaintext images of airplane (**a**), baboon (**e**), house (**i**), peppers (**m**), sailboat (**q**) and splash (**u**). The second column is the intensity channel of the first column. Column three presents the image after the encryption algorithm. The intensity channels of the encrypted images are given in column four.



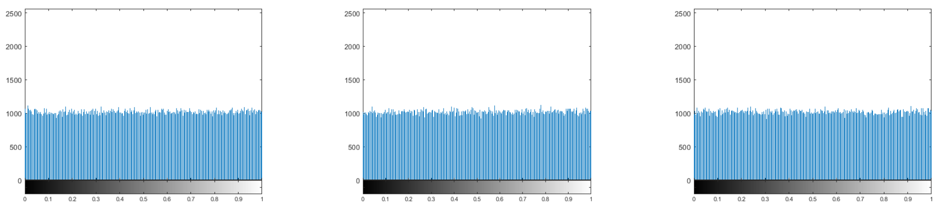
(**A**) Airplane (I) (**B**) Baboon (I) (**C**) House (I)



(**a**) Enc Airplane (I) (**b**) Enc Baboon (I) (**c**) Enc House (I)



(**D**) Peppers (I) (**E**) Sailboat (I) (**F**) Splash (I)



(**d**) Enc Peppers (I) (**e**) Enc Sailboat (I) (**f**) Enc Splash (I)

Figure 8. Histogram of the intensity channels of the plaintext and corresponding ciphertext images. (**A**–**F**) are histograms of the intensity channels of the plaintext images; (**a**–**f**) are histograms of the intensity channels of the ciphertext images.

To quantitatively analyze the histogram, Equation (21) is used to calculate the $var(H)$ and, thus, portray the uniformity of the intensity channels of the ciphertext image [56].

$$var(H) = \frac{1}{2^8 \times 2^8} \sum_{i=0}^{2^8-1} \sum_{j=0}^{2^8-1} \frac{1}{2} (h_i - h_j)^2. \tag{21}$$

where H is a vector of histogram values and the counts with pixel values i and j are recorded as h_i and h_j, respectively. The $var(H)$ of the intensity channels of the plaintext and ciphertext images are presented in Table 1. Looking at Figure 8, notice that the histogram distribution of the intensity channels of the plaintext images is non-uniform and the histogram distribution of the intensity channels of the ciphertext images is uniform. The quantitative results presented in Table 1 provide side-by-side proof that the constructed scheme is resistant to histogram attacks.

Table 1. Histogram variance of the intensity of the six images.

Images	Plaintext Images (I)	Ciphertext Images (I)
Airplane	3.1592×10^6	971.3
Baboon	6.8068×10^5	1333.1
House	1.3026×10^6	902.4
Peppers	7.7600×10^5	1065.3
Sailboat	8.3552×10^5	1167.4
Splash	1.7304×10^6	1164.3

4.1.2. Shannon Entropy Analysis

The magnitude of image uncertainty features can be measured by entropy [57]. The entropy $H(s)$ is defined as

$$H(s) = \sum_{i=0}^{M} p(s_i) \log_2 (p(s_i))^{-1},$$

whereby the probability of s_i is noted as $p(s_i)$. The smaller the difference between the $H(s)$ of the encrypted image and 8 bits, the better the cryptosystem is at resisting "wild" attacks. Table 2 lists the Shannon entropy of plaintext and ciphertext images. It is clear that the encryption algorithm performs well with values larger than 7.999, which is closer to the theoretical value of 8. Compared to [58], our test scheme is effective at resisting entropy attacks.

Table 2. Shannon entropy of plaintext and ciphertext images.

Images	Plaintext I Channel	Ciphertext I Channel	Reference [58] R Channel	Reference [58] G Channel	Reference [58] B Channel
Airplane	6.5866	7.9993	7.9474	7.9556	7.9692
Baboon	7.3899	7.9991	7.9882	7.9888	7.9912
House	7.2699	7.9994	-	-	-
Peppers	7.4320	7.9993	7.9795	7.9683	7.9640
Sailboat	7.4049	7.9992	-	-	-
Splash	7.1201	7.9992	-	-	-

4.1.3. Correlation between Adjacent Pixels

The role of encryption algorithms is to disrupt the correlation between pixels and, thus, achieve the purpose of effectively protecting the image information. The closer the absolute value of the correlation coefficient between adjacent pixels in a ciphertext image is to zero, the more resistant it is to statistical attacks.

To measure the correlation of the adjacent pixels in the horizontal direction (HD), vertical direction (VD), and diagonal direction (DD) in plaintext and ciphertext images, respectively, we perform the following operation to randomly select $N = 10000$ pairs of adjacent two pixels (HD, VD, DD) from plaintext and ciphertext images, and calculate the correlation coefficients with the help of Equation (22):

$$\gamma_{xy} = \frac{\sum_{i=1}^{N}\left(x_i - N^{-1}\sum_{i=1}^{N} x_i\right)\left(y_i - N^{-1}\sum_{i=1}^{N} y_i\right)}{\sqrt{\sum_{i=1}^{N}\left(x_i - N^{-1}\sum_{i=1}^{N} x_i\right)^2} \cdot \sqrt{\sum_{i=1}^{N}\left(y_i - N^{-1}\sum_{i=1}^{N} y_i\right)^2}}, \tag{22}$$

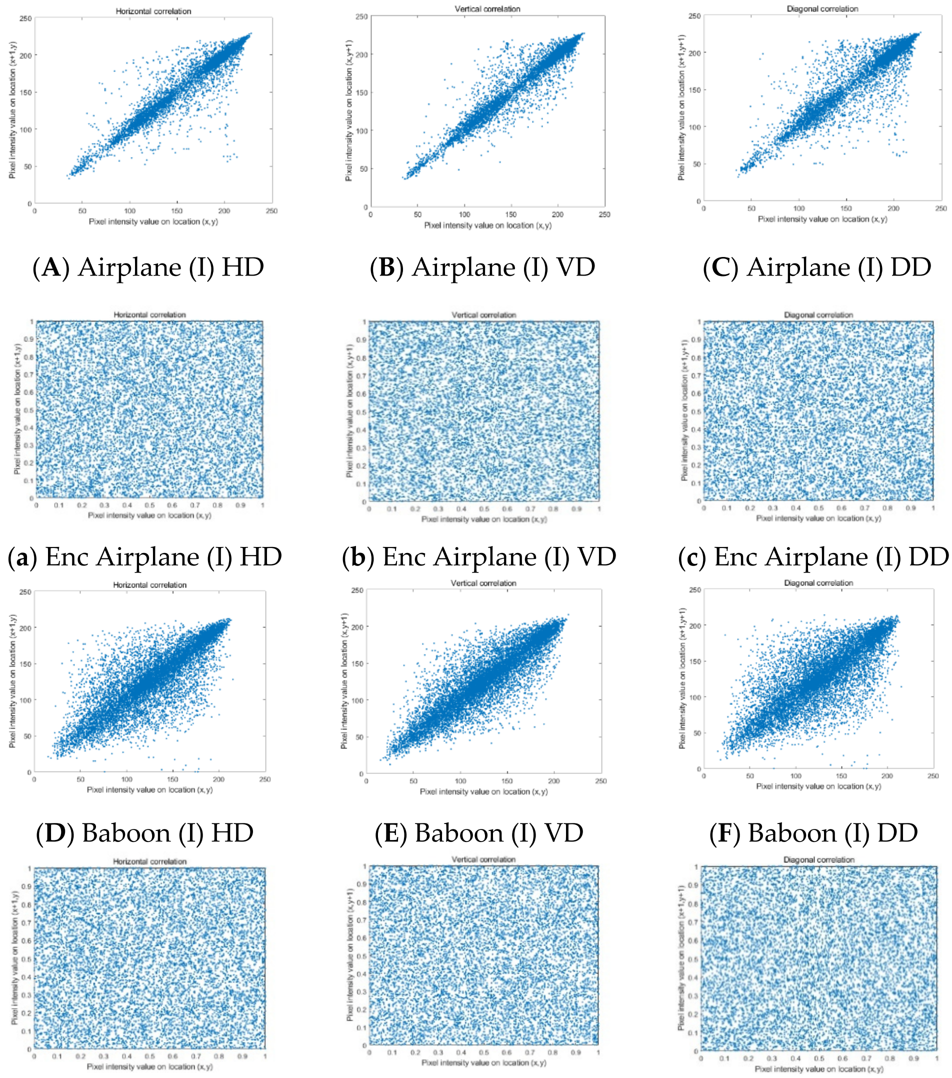
in which the correlation coefficient is denoted γ_{xy}, the two adjacent pixel values are denoted x_i and y_i, and the chosen total number of pixel pairs is N. Observing Figure 9, the γ_{xy} of the ciphertext image intensity channels is much weaker than that of the plaintext image intensity channels. Table 3 presents the correlation values for the plaintext and ciphertext image intensity channels HD, VD, and DD, which have values close to 1 and 0, respectively. This confirms from the side that the proposed encryption algorithm can resist the correlation attack. In addition, Table 4 presents a comparison between the correlation coefficients of the proposed encryption algorithm and the algorithm in [58]. The results show that the proposed algorithm is comparable to the algorithm in [58].

Table 3. Correlation coefficients of the intensity channels of plaintext and ciphertext images.

Images	HD	VD	DD
Airplane (I)	0.9843	0.9856	0.9756
Enc Airplane (I)	0.0129	−0.0195	−0.0264
Baboon (I)	0.8638	0.9083	0.8439
Enc Baboon (I)	-6.5926×10^{-4}	−0.0016	−0.0060
House (I)	0.9685	0.9770	0.9547
Enc House (I)	0.0248	−0.0201	6.5579×10^{-4}
Peppers (I)	0.9838	0.9820	0.9750
Enc Peppers (I)	−0.0067	−0.0038	0.0063
Sailboat (I)	0.9727	0.9758	0.9613
Enc Sailboat (I)	−0.0116	−0.0090	0.0078
Splash (I)	0.9889	0.9821	0.9779
Enc Splash (I)	0.0113	−0.0130	0.0021

Table 4. Correlation coefficients of ciphertext images obtained by different algorithms.

Images	HD	VD	DD
Enc Airplane I channel	0.0129	−0.0195	−0.0264
Reference [58] R channel	0.0039	0.0032	−0.0076
Reference [58] G channel	0.0074	0.0010	0.0005
Reference [58] B channel	−0.0057	−0.0021	0.0009
Enc Baboon I channel	-6.5926×10^{-4}	−0.0016	−0.0060
Reference [58] R channel	0.0063	0.0058	−0.0063
Reference [58] G channel	0.0004	0.0075	−0.0091
Reference [58] B channel	−0.0046	0.0029	−0.0032
Enc Peppers I channel	−0.0067	−0.0038	0.0063
Reference [58] R channel	0.0079	−0.0025	0.0087
Reference [58] G channel	−0.0023	0.0180	−0.0014
Reference [58] B channel	−0.0037	0.0205	−0.0011



(**A**) Airplane (I) HD (**B**) Airplane (I) VD (**C**) Airplane (I) DD

(**a**) Enc Airplane (I) HD (**b**) Enc Airplane (I) VD (**c**) Enc Airplane (I) DD

(**D**) Baboon (I) HD (**E**) Baboon (I) VD (**F**) Baboon (I) DD

(**d**) Enc Baboon (I) HD (**e**) Enc Baboon (I) VD (**f**) Enc Baboon (I) DD

Figure 9. Correlation coefficients of plaintext and ciphertext image intensity channels: the first row (**A**–**C**) and the third row (**D**–**F**) are the correlation values of the HD, VD, and DD of the intensity channels of the plaintext image airplane and baboon; the second row (**a**–**c**) and the fourth row (**d**–**f**) are the correlation values of the corresponding ciphertext image intensity channels in HD, VD, and DD.

4.1.4. NPCR and UACI Analysis

The Number of Pixel Change Rate (NPCR) and Uniform Average Change Intensity (UACI) can be used to measure the sensitivity of the encryption algorithm to plaintext images. The NPCR and UACI are defined as follows.

$$NPCR = \frac{1}{2^n \times 2^n} \sum_{i=0}^{2^n-1} \sum_{j=0}^{2^n-1} D(i,j) \times 100\%,$$

$$D(i,j) = \begin{cases} 1, & if\ X(i,j) \neq Y(i,j) \\ 0, & if\ X(i,j) = Y(i,j) \end{cases},$$

$$UACI = \frac{1}{2^n \times 2^n} \sum_{i=0}^{2^n-1} \sum_{j=0}^{2^n-1} \frac{|X(i,j) - Y(i,j)|}{2^8 - 1} \times 100\%,$$

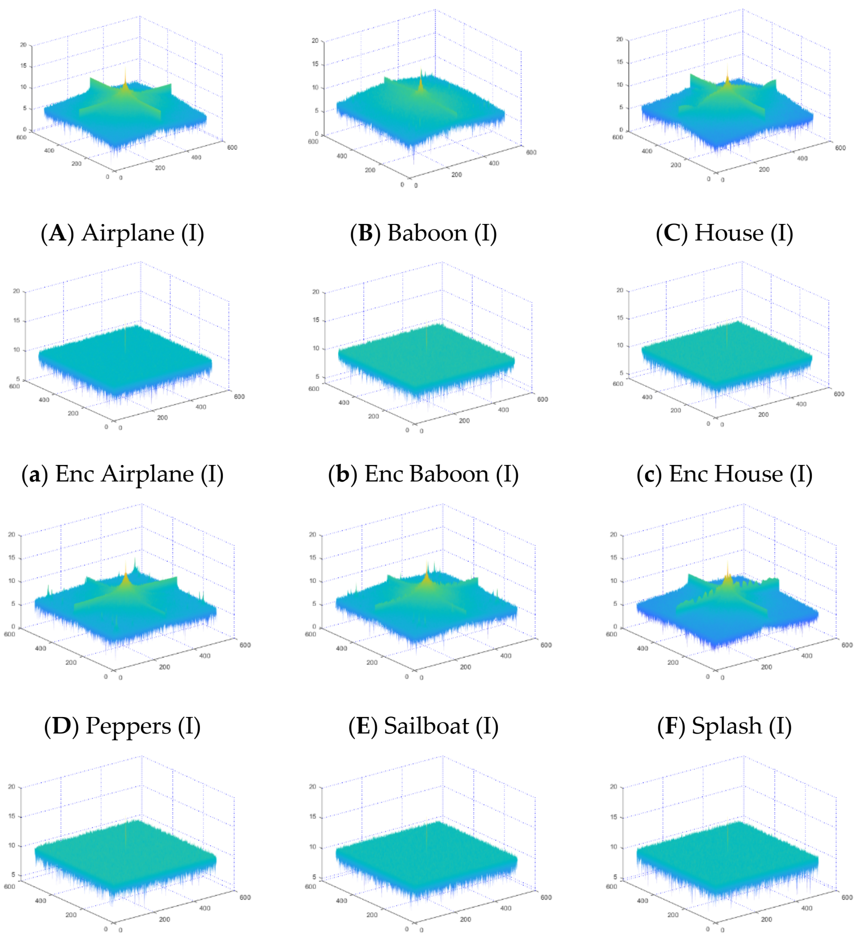
where X and Y denote the intensity channel of the ciphertext image and the intensity channel of the plaintext image changed by one pixel, respectively. The value of the first pixel in the intensity channel of the plaintext image is added by 1 and the corresponding NPCR and UACI are calculated. The results are shown in Table 5. The NPCR of the intensity channels of all six images hovered around 99.60%, so the designed encryption algorithm is sensitive to slight variations of pixels in the intensity channels of the plaintext images.

Table 5. Results of NPCR and UACI tests.

Images	NPCR(%)	UACI(%)
Airplane (I)	99.6086	32.2671
Baboon (I)	99.5918	27.8789
House (I)	99.6128	30.1007
Peppers (I)	99.6101	28.7183
Sailboat (I)	99.6143	31.3058
Splash (I)	99.6078	29.1101

4.1.5. Spectrum Analysis

A spectrum analysis is also used as an important analytical tool to measure the statistical properties of ciphertext images [38,59]. Figure 10 displays the spectrum of six image intensities.



(**A**) Airplane (I) (**B**) Baboon (I) (**C**) House (I)

(**a**) Enc Airplane (I) (**b**) Enc Baboon (I) (**c**) Enc House (I)

(**D**) Peppers (I) (**E**) Sailboat (I) (**F**) Splash (I)

(**d**) Enc Peppers (I) (**e**) Enc Sailboat (I) (**f**) Enc Splash (I)

Figure 10. Spectral analysis of the intensity channels of plaintext and ciphertext images.

The standard deviations [60] of six image intensity channels were calculated using the function $std(\cdot)$, and the results are shown in Table 6. The standard deviation of all ciphertext image intensity channels is close to 73.9, which in turn confirms the well-distributed pixels in the ciphertext image intensity channels. Therefore, the encryption algorithm is highly effective against spectrum attacks.

Table 6. Standard deviation of six image intensities.

Images	Plaintext Images (I)	Ciphertext Images (I)
Airplane	41.5005	73.9329
Baboon	43.0336	73.8667
House	49.8598	73.9198
Peppers	45.5237	73.9726
Sailboat	63.6911	73.8974
Splash	47.5419	73.9627

4.1.6. MSE and PSNR Analysis

The ideal ciphertext and plaintext images should have significant differences. We use the mean square error (MSE) to measure the difference between ciphertext and plaintext images, which is defined below:

$$MSE = \frac{1}{2^n \times 2^n} \sum_{i=0}^{2^n-1} \sum_{j=0}^{2^n-1} (f_{ij} - g_{ij})^2, \tag{23}$$

where f_{ij} and g_{ij} denote the intensity values of plaintext and ciphertext image pixels ij, respectively. The quality of the intensity channel of the ciphertext image can be measured by the peak signal-to-noise ratio (PSNR), as expressed in Equation (24):

$$PSNR = 10 \log_{10} \left(\frac{2^8 - 1}{\sqrt{MSE}} \right)^2. \tag{24}$$

Table 7 lists the MSE and PSNR values of the ciphertext images, which in turn corroborate the better cryptographic quality of our proposed scheme.

Table 7. MSE and PSNR for plaintext and ciphertext images.

Images	MSE I Channel	PSNR I Channel	PSNR [58]
Airplane	1.0140×10^4	8.0706	7.9741
Baboon	7.2915×10^3	9.5026	8.7691
House	8.7339×10^3	8.7187	-
Peppers	7.8308×10^3	9.1927	8.0732
Sailboat	9.5619×10^3	8.3458	-
Splash	8.6710×10^3	9.0615	-

4.2. Key Sensitivity Analysis

The higher the key sensitivity of the encryption algorithm, the more subtle key changes can cause decryption to fail. In this paper, we took the intensity channel of a splash image of size $2^9 \times 2^9$ as an example, and decrypted the intensity channel of the ciphertext image by a slight change of the key; the decryption results are displayed in Figure 11. Observing Figure 11, the ciphertext image cannot be restored to the plaintext image when the decryption key undergoes a slight transformation. Therefore, any slight change in the key will result in unsuccessful decryption.

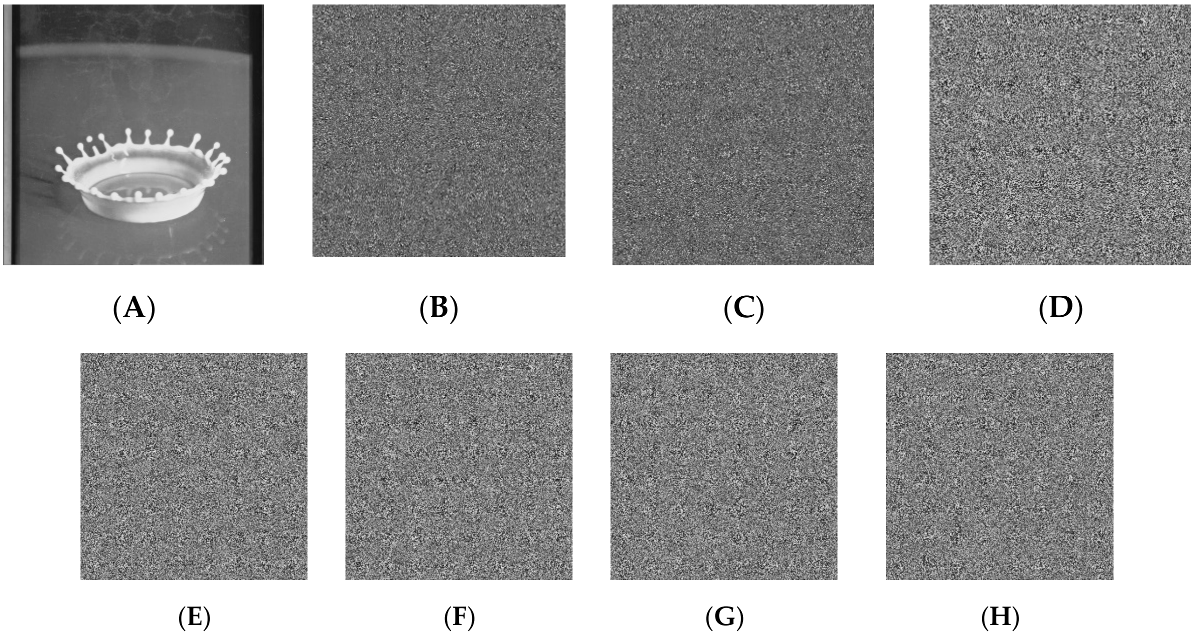


Figure 11. The decrypted image intensity channels using the correct and incorrect keys. (**A**) Correct key. (**B**) Incorrect key $w_0 + 10^{-15}$. (**C**) Incorrect key $\eta + 10^{-15}$. (**D**) Incorrect key $x_0 + 10^{-15}$. (**E**) Incorrect key $y_0 + 10^{-16}$. (**F**) Incorrect key $z_0 + 10^{-4}$. (**G**) Incorrect key $\beta + 10^{-3}$. (**H**) Incorrect key $\gamma + 10^{-15}$.

4.3. Key Space Analysis

All keys in a cryptosystem constitute the key space. In the designed algorithm, the total key consists of the initial value w_0 of the generalized logistic map and parameters η, initial values x_0, y_0, z_0 of the quantum logistic map, and parameters β, γ. Since the keys are independent of each other, the key space of the algorithm is

$$\text{Key Space} = 10^{15} \times 10^{15} \times 10^{15} \times 10^{16} \times 10^{4} \times 10^{3} \times 10^{15} = 10^{83} \approx 2^{276} >> 2^{100}.$$

Table 8 compares the key space of the constructed quantum color image encryption algorithm with other quantum color image encryption algorithms and can prove that our algorithm has a larger key space. In other words, the total key space can effectively resist violent attacks.

Table 8. The key space of the algorithm in this paper and other related algorithms.

Algorithms	**Key Space**
Proposed	10^{83}
Khan et al. [58]	$(9!)^2 \cdot 10^{42}$
Tan et al. [33]	10^{60}
Li et al. [35]	10^{42}
Abd El-Latif et al. [39]	2^{359}

4.4. Robustness Analysis

A common method for assessing the robustness of encryption algorithms against occlusion attacks is to lose part of the data of the ciphertext image and then restore only the original image from the remaining data. Figure 12 displays the encrypted images and the decrypted images obtained under different occlusion scenarios. It is found that most of the information can be recovered after decryption, which in turn indicates that the designed scheme is resistant to occlusion attacks to a limited extent.

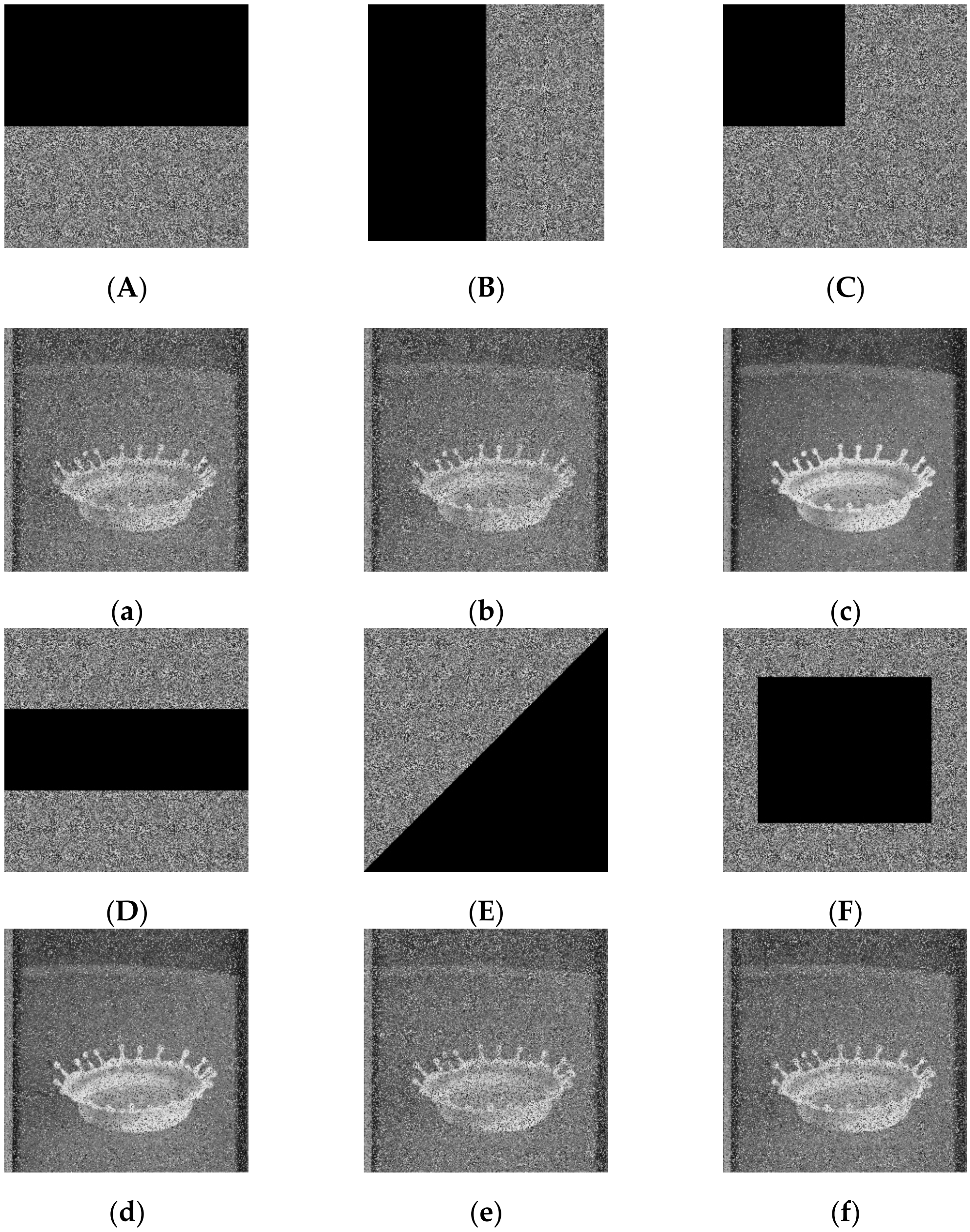


Figure 12. Intensity channels of decrypted images for different occlusion cases. The (**A**–**F**) encrypted Splash image is occluded, and the (**a**–**f**) corresponding to the decrypted image.

4.5. NIST SP 800-22 Analysis

To verify the randomization properties of the ciphertext image airplane intensity channel (see Figure 7d), the randomness of the sequence is tested using the NIST SP 800-22 tool [39]. Each test generates a p-value in $[0, 1]$, and only when the p-value is greater than the threshold $\mu = 0$ means that the test is passed. The test results in Table 9 show that our scheme has successfully passed the NIST SP 800-22 test.

Table 9. NIST SP 800-22 test results for the encrypted airplane image intensity channel.

Test Name	P Enc Airplane I Channel	Passed
Frequency	0.583692	√
Approximate Entropy	0.363808	√
Block Frequency	0.773887	√
Cumulative Sums Forward	0.658723	√
Cumulative Sums Reverse	0.657795	√
FFT	0.861586	√
Linear Complexity (block = 500)	0.328508	√
Longest Run	0.445217	√
Non Overlapping Template	0.468400	√
Overlapping Template	0.309034	√
Random Excursions (x = −1)	0.572277	√
Random Excursions Variant (x = 1)	0.679398	√
Rank	0.730751	√
Runs	0.472942	√
Serial 1	0.346267	√
Serial 2	0.481713	√
Universal	0.542511	√

4.6. Computational Complexity Analysis

To calculate the complexity of the quantum circuits in the encryption algorithm, CNOT gates and NOT gates are used as the basic quantum gates. The designed image encryption scheme consists of three steps, so the complexity of computing quantum gates depends on the pixel plane permutation, intensity bit-plane permutation, and intensity bit-plane chaos diffusion. In the pixel plane permutation stage, the complexity of the quantum gates required for operation G is $O\left(n^2\right)$. In the intensity bit-plane permutation stage, operation F uses eight swap gates, 24 CNOT gates, and 16 NOT gates, and one swap gate is used with three controlled NOT gates; therefore, operation F needs 48 CNOT gates and 16 NOT gates. In the intensity bit-plane chaos diffusion stage, in order to calculate the quantum gates required for operation L_k, it is sufficient to consider only the quantum gates required for sub-operation W_k. The intensity of each pixel in the image QIRHSI is encoded by eight qubits and the operation W_k^m acts on each qubit. When $d_k^m = 1$, W_k^m will be implemented by $2n - CNOT$. A $n - CNOT$ gate has the same effect as $4n - 8$ Toffoli gates. A Toffoli gate can achieve the results of 6 CNOT gates [61,62]. Therefore, $384n - 384$ CNOT gates are required for quantum operation L_k, i.e., $384n - 384$ CNOT gates are required to operate L_k.

In summary, the complexity of the quantum gates required for the encryption algorithm is shown below.

$$\begin{aligned} &O\left(n^2\right) + O(48\ \mathrm{CNOT} + 16\ \mathrm{NOT} + 384n - 384\ \mathrm{CNOT}) \\ &= O\left(n^2 + 384n - 320\right) \\ &\approx O\left(n^2\right) \end{aligned} \tag{25}$$

Equation (25) implies that the designed quantum color image encryption method can encrypt $2^n \times 2^n$ QIRHSI images by using $O\left(n^2\right)$ elementary quantum gates when the value of q is 8. Thus, all things being equal, quantum algorithms are more cost effective than classical algorithms $O\left(2^{2n}\right)$.

5. Discussions

The quantum color image encryption scheme based on geometric transformation and intensity channel diffusion constructed in this paper has flexibility and high security, but it also has some limitations. The encryption scheme includes pixel-plane permutation, intensity bit-plane permutation, and intensity bit-plane chaos diffusion operations, but fails to perform color diffusion operations on the hue and saturation channels. In the future, more research should be conducted to make fuller use of the relevant properties of the hue and saturation channels to design a more perfect encryption scheme and achieve a better encryption effect.

6. Conclusions

We propose a quantum color image encryption scheme based on geometric transformation and intensity channel diffusion. The scheme includes pixel plane permutation, intensity bit-plane permutation, and intensity bit-plane chaotic diffusion, and the corresponding quantum circuit is given. In order to make the pixel plane permutated "more random", the pixel plane permutation stage is combined with a generalized logistic map for permuting, and the key space is increased by setting different initial values and parameters. During the intensity bit-plane permutation stage, cross-swapping and XOR, XNOR operations are used to tamper with the intensity values. In addition, the intensity bit-plane chaotic diffusion stage is accomplished by interacting the chaotic sequence generated by the quantum logistic mapping with the intensity bit-plane via the XOR operation.

After a series of tests and experimental analyses, the algorithm has high key sensitivity and a large key space. In addition, various statistical and differential analyses covering histogram, Shannon entropy, correlation coefficient, NPCR and UACI, spectrum analysis, MSE, and PSNR are performed in this paper. The Shannon entropy is very close to the ideal value of 8, the correlation coefficient is nearly 0, the value of NPCR is close to 99.60%, the standard deviation is almost 73.9, the MSE is approximately 8704.85, and the PSNR is close to 8.8153. Subsequently, it is verified that the algorithm has good robustness against occlusion attacks. The bit sequence of the ciphertext image passed the NIST random number detection.

The significance of this paper involves the combination of geometric transformation and the intensity channel with two chaos mappings, which, on the one hand, can combine geometric transformation (i.e., two-point swapping) with chaos mapping, and on the other hand can sufficiently apply chaos mapping to intensity channel diffusion. The quantum image encryption algorithm designed in this paper is not only resistant to various attacks, but it also has portability and is a secure and reliable quantum image encryption scheme.

Future focus should be on a further combination of the quantum image representation model QIRHSI with chaotic systems and its application in quantum cryptography or medical images.

Author Contributions: Conceptualization, G.C. and X.S.; methodology, G.C.; software, G.C.; validation, G.C., X.S. and A.A.A.E.-L.; formal analysis, G.C.; investigation, G.C. and A.A.A.E.-L.; resources, G.C.; data curation, X.S.; writing—original draft preparation, G.C. and X.S.; writing—review and editing, A.A.A.E.-L.; visualization, X.S. and A.A.A.E.-L.; supervision, X.S.; project administration, X.S.; funding acquisition, X.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the EIAS Data Science Lab, College of Computer and Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing not applicable.

Conflicts of Interest: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

1. Nielsen, M.A.; Chuang, I.L. *Quantum Computation and Quantum Information*, 10th Anniversary ed.; Cambridge University Press: Cambridge, UK, 2010; pp. 171–242.
2. Feynman, R.P. Simulating physics with computers. *Int. J. Theor. Phys.* **1982**, *21*, 1–22. [CrossRef]
3. Grover, L.K. A fast quantum mechanical algorithm for database search. In Proceedings of the 28th Annual ACM Symposium on Theory of Computing, Philadelphia, PA, USA, 22–24 May 1996.

4. Shor, P.W. Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 20–22 November 1994.
5. Nestor, T.; Jacques, K. *A Particular Class of Simple Chaotic Circuits: Multistability Analysis*; Lap LAMBERT Academic Publishing: Chisinau, Moldova, 2019; pp. 30–59.
6. Tsafack, N.; Kengne, J. Multiple coexisting attractors in a generalized Chua's circuit with a smoothly adjustable symmetry and nonlinearity. *J. Phys. Math.* **2019**, *10*, 0902–2090.
7. Nestor, T.; De Dieu, N.J.; Jacques, K.; Yves, E.J.; Iliyasu, A.M.; Abd El-Latif, A.A. A multidimensional hyperjerk oscillator: Dynamics analysis, analogue and embedded systems implementation, and its application as a cryptosystem. *Sensors* **2019**, *20*, 83. [CrossRef] [PubMed]
8. Signing, V.R.F.; Tegue, G.A.G.; Kountchou, M.; Njitacke, Z.T.; Tsafack, N.; Nkapkop, J.D.D.; Lessouga Etoundi, C.M.; Kengne, J. A cryptosystem based on a chameleon chaotic system and dynamic DNA coding. *Chaos Solitons Fractals* **2022**, *155*, 111777. [CrossRef]
9. Alhudhaif, A.; Ahmad, M.; Alkhayyat, A.; Tsafack, N.; Farhan, A.K.; Ahmed, R. Block cipher nonlinear confusion components based on new 5-D hyperchaotic system. *IEEE Access* **2021**, *9*, 87686–87696. [CrossRef]
10. Yan, F.; Venegas-Andraca, S.E. *Quantum Image Processing*, 1st ed.; Springer: Singapore, 2020; pp. 19–102.
11. Yan, F.; Iliyasu, A.M.; Jiang, Z.G. Quantum computation-based image representation, Process. operations and their applications. *Entropy* **2014**, *16*, 5290–5338. [CrossRef]
12. Abd El-Latif, A.A.; Abd-El-Atty, B.; Abou-Nassar, E.M.; Venegas-Andraca, S.E. Controlled alternate quantum walks based privacy preserving healthcare images in internet of things. *Opt. Laser Technol.* **2020**, *124*, 105942. [CrossRef]
13. Abd El-Latif, A.A.; Abd-El-Atty, B.; Venegas-Andraca, S.E.; Mazurczyk, W. Efficient quantum-based security protocols for information sharing and data protection in 5G networks. *Future Gener. Comput. Syst.* **2019**, *100*, 893–906. [CrossRef]
14. Abd El-Latif, A.A.; Abd-El-Atty, B.; Amin, M.; Iliyasu, A.M. Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications. *Sci. Rep.* **2020**, *10*, 1–16.
15. Venegas-Andraca, S.E.; Bose, S. Storing, processing, and retrieving an image using quantum mechanics. *Quantum Inf. Comput.* **2003**, *5105*, 137–147.
16. Latorre, J.I. Image compression and entanglement. *Quantum Phys.* **2005**, 1–4. [CrossRef]
17. Le, P.Q.; Dong, F.; Hirota, K. A flexible representation of quantum images for polynomial preparation, image compression, and Process. operations. *Quantum Inf. Process.* **2011**, *10*, 63–84. [CrossRef]
18. Zhang, Y.; Lu, K.; Gao, Y.H.; Wang, M. NEQR: A novel enhanced quantum representation of digital images. *Quantum Inf. Process.* **2013**, *12*, 2833–2860. [CrossRef]
19. Sun, B.; Le, P.Q.; Iliyasu, A.M.; Yan, F.; Garcia, J.A.; Dong, F.Y.; Hirota, K. A multi-channel representation for images on quantum computers using the RGBα color space. In Proceedings of the IEEE 7th International Symposium on Intelligent Signal Processing, Floriana, Malta, 19–21 September 2011.
20. Zhang, Y.; Lu, K.; Gao, Y.H.; Xu, K. A novel quantum representation for log-polar images. *Quantum Inf. Process.* **2013**, *12*, 3103–3126. [CrossRef]
21. Yang, Y.G.; Jia, X.; Sun, S.J.; Pan, Q.X. Quantum cryptographic algorithm for color images using quantum Fourier transform and double random-phase encoding. *Inform. Sci.* **2014**, *277*, 445–457. [CrossRef]
22. Jiang, N.; Wang, J.; Mu, Y. Quantum image scaling up based on nearest-neighbor interpolation with integer scaling ratio. *Quantum Inf. Process.* **2015**, *14*, 4001–4026. [CrossRef]
23. Li, H.S.; Zhu, Q.X.; Lan, S.; Shen, C.Y.; Zhou, R.G.; Mo, J. Image storage, retrieval, compression and segmentation in a quantum system. *Quantum Inf. Process.* **2013**, *12*, 2269–2290. [CrossRef]
24. Sang, J.Z.; Wang, S.; Li, Q. A novel quantum representation of color digital images. *Quantum Inf. Process.* **2017**, *16*, 1–14. [CrossRef]
25. Li, P.C.; Liu, X.D. Color image representation model and its application based on an improved FRQI. *Int. J. Quantum Inf.* **2018**, *16*, 1850005. [CrossRef]
26. Şahin, E.; Yilmaz, I. QRMW: Quantum representation of multi wavelength images. *Turk. J. Electr. Eng. Comput.* **2018**, *26*, 768–779. [CrossRef]
27. Khan, R.A. An improved flexible representation of quantum images. *Quantum Inf. Process.* **2019**, *18*, 1–19. [CrossRef]
28. Wang, L.; Ran, Q.W.; Ma, J.; Yu, S.Y.; Tan, L.Y. QRCI: A new quantum representation model of color digital images. *Opt. Commun.* **2019**, *438*, 147–158. [CrossRef]
29. Grigoryan, A.M.; Agaian, S.S. New look on quantum representation of images: Fourier transform representation. *Quantum Inf. Process.* **2020**, *19*, 1–26. [CrossRef]
30. Chen, G.L.; Song, X.H.; Venegas-Andraca, S.E.; Abd El-Latif, A.A. QIRHSI: Novel quantum image representation based on HSI color space model. *Quantum Inf. Process.* **2022**, *21*, 1–31. [CrossRef]
31. Yang, Y.G.; Tian, J.; Lei, H.; Zhou, Y.H.; Shi, W.M. Novel quantum image encryption using one-dimensional quantum cellular automata. *Inform. Sci.* **2016**, *345*, 257–270. [CrossRef]
32. Zhou, N.R.; Hua, T.X.; Gong, L.H.; Pei, D.J.; Liao, Q.H. Quantum image encryption based on generalized Arnold transform and double random-phase encoding. *Quantum Inf. Process.* **2015**, *14*, 1193–1213. [CrossRef]
33. Tan, R.C.; Lei, T.; Zhao, Q.M.; Gong, L.H.; Zhou, Z.H. Quantum color image encryption algorithm based on a hyper-chaotic system and quantum Fourier transform. *Int. J. Theor. Phys.* **2016**, *55*, 5368–5384. [CrossRef]

34. Wang, H.; Wang, J.; Geng, Y.C.; Song, Y.; Liu, J.Q. Quantum image encryption based on iterative framework of frequency-spatial domain transforms. *Int. J. Theor. Phys.* **2017**, *56*, 3029–3049. [CrossRef]
35. Li, L.; Abd-El-Atty, B.; Abd El-Latif, A.A.; Ahmed, G. Quantum color image encryption based on multiple discrete chaotic systems. In Proceedings of the Federated Conference on Computer Science and Information Systems (FedCSIS), Prague, Czech Republic, 3–6 September 2017.
36. Li, X.Z.; Chen, W.W.; Wang, Y.Q. Quantum image compression-encryption scheme based on quantum discrete cosine transform. *Int. J. Theor. Phys.* **2018**, *57*, 2904–2919. [CrossRef]
37. Li, H.S.; Li, C.Y.; Chen, X.; Xia, H.Y. Quantum image encryption based on phase-shift transform and quantum Haar wavelet packet transform. *Mod. Phys. Lett. A* **2019**, *34*, 1950214. [CrossRef]
38. Abd-El-Atty, B.; Abd El-Latif, A.A.; Venegas-Andraca, S.E. An encryption protocol for NEQR images based on one-particle quantum walks on a circle. *Quantum Inf. Process.* **2019**, *18*, 1–26. [CrossRef]
39. Abd El-Latif, A.A.; Abd-El-Atty, B.; Venegas-Andraca, S.E. Controlled alternate quantum walk-based pseudo-random number generator and its application to quantum color image encryption. *Phys. A* **2020**, *547*, 123869. [CrossRef]
40. Jiang, N.; Dong, X.; Hu, H.; Ji, Z.X.; Zhang, W.Y. Quantum image encryption based on Henon mapping. *Int. J. Theor. Phys.* **2019**, *58*, 979–991. [CrossRef]
41. Musanna, F.; Kumar, S. Image encryption using quantum 3-D Baker map and generalized gray code coupled with fractional Chen's chaotic system. *Quantum Inf. Process.* **2020**, *19*, 1–31. [CrossRef]
42. Zhou, N.R.; Huang, L.X.; Gong, L.H.; Zeng, Q.W. Novel quantum image compression and encryption algorithm based on DQWT and 3D hyper-chaotic Henon map. *Quantum Inf. Process.* **2020**, *19*, 1–21. [CrossRef]
43. Hu, W.W.; Zhou, R.G.; Luo, J.; Jiang, S.X.; Luo, G.F. Quantum image encryption algorithm based on Arnold scrambling and wavelet transforms. *Quantum Inf. Process.* **2020**, *19*, 1–29. [CrossRef]
44. Liu, X.; Xiao, D.; Liu, C. Three-level quantum image encryption based on Arnold transform and logistic map. *Quantum Inf. Process.* **2021**, *20*, 1–22. [CrossRef]
45. Song, X.H.; Wang, S.; Niu, X.M. Multi-channel quantum image representation based on phase transform and elementary transformations. *J. Inf. Hiding Multimed. Signal Process.* **2014**, *5*, 574–585.
46. Jafarizadeh, M.A.; Behnia, S. Hierarchy of chaotic maps with an invariant measure and their coupling. *Phys. D* **2001**, *159*, 1–21. [CrossRef]
47. Abd El-Latif, A.A.; Niu, X.M.; Amin, M. A new image cipher in time and frequency domains. *Opt. Commun.* **2012**, *285*, 4241–4251. [CrossRef]
48. Goggin, M.E.; Sundaram, B.; Milonni, P.W. Quantum logistic map. *Phys. Rev. A* **1990**, *41*, 5705. [CrossRef] [PubMed]
49. Akhshani, A.; Akhavan, A.; Mobaraki, A.; Lim, S.C.; Hassan, Z. Pseudo random number generator based on quantum chaotic map. *Commun. Nonlinear Sci. Numer. Simul.* **2014**, *19*, 101–111. [CrossRef]
50. Seyedzadeh, S.M.; Norouzi, B.; Mosavi, M.R.; Mirzakuchaki, S. A novel color image encryption algorithm based on spatial permutation and quantum chaotic map. *Nonlinear Dyn.* **2015**, *81*, 511–529. [CrossRef]
51. Ye, G.D.; Jiao, K.; Huang, X. Quantum logistic image encryption algorithm based on SHA-3 and RSA. *Nonlinear Dyn.* **2021**, *104*, 2807–2827. [CrossRef]
52. Ye, G.D.; Wu, H.; Jiao, K.; Mei, D. Asymmetric image encryption scheme based on the Quantum logistic map and cyclic modulo diffusion. *Math. Biosci. Eng.* **2021**, *18*, 5427–5448. [CrossRef]
53. The USC-SIPI Image Database. Available online: http://sipi.usc.edu/database/database.php (accessed on 17 September 2021).
54. Njitacke, Z.T.; Koumetio, B.N.; Ramakrishnan, B.; Leutcho, G.D.; Fozin, T.F.; Tsafack, N.; Rajagopal, K.; Kengne, J. Hamiltonian energy and coexistence of hidden firing patterns from bidirectional coupling between two different neurons. *Cogn. Neurodyn.* **2021**, *16*, 899–916. [CrossRef]
55. Njitacke, Z.T.; Tsafack, N.; Ramakrishnan, B.; Rajagopal, K.; Kengne, J.; Awrejcewicz, J. Complex dynamics from heterogeneous coupling and electromagnetic effect on two neurons: Application in images encryption. *Chaos Solitons Fractals* **2021**, *153*, 111577. [CrossRef]
56. Zhang, Y.Q.; Wang, X.Y. A symmetric image encryption algorithm based on mixed linear-nonlinear coupled map lattice. *Inform. Sci.* **2014**, *273*, 329–351. [CrossRef]
57. Amin, M.; Abd El-Latif, A.A. Efficient modified RC5 based on chaos adapted to image encryption. *J. Electron. Imaging* **2010**, *19*, 013012. [CrossRef]
58. Khan, M.; Rasheed, A. Permutation-based special linear transforms with application in quantum image encryption algorithm. *Quantum Inf. Process.* **2019**, *18*, 1–21. [CrossRef]
59. Available online: https://ww2.mathworks.cn/help/matlab/ref/fft2.html?searchHighlight=fft2&s_tid=srchtitle (accessed on 20 September 2021).
60. Available online: https://ww2.mathworks.cn/help/matlab/ref/std.html?searchHighlight=std&s_tid=srchtitle (accessed on 20 September 2021).
61. Lloyd, S. Almost any quantum logic gate is universal. *Phys. Rev. Lett.* **1995**, *75*, 346. [CrossRef] [PubMed]
62. Vedral, V.; Barenco, A.; Ekert, A. Quantum networks for elementary arithmetic operations. *Phys. Rev. A* **1996**, *54*, 147. [CrossRef] [PubMed]