entropy

Article

Image Encryption Using Quantum 3D Mobius Scrambling and 3D Hyper-Chaotic Henon Map

Ling Wang, Qiwen Ran and Junrong Ding

Special Issue

Advanced Technology in Quantum Cryptography

Edited by
Prof. Dr. Qin Wang, Dr. Hong-Wei Li, Dr. Jin Dong Wang and Dr. Xing-Yu Zhou

MDPI

https://doi.org/10.3390/e25121629

entropy

MDPI

Article

Image Encryption Using Quantum 3D Mobius Scrambling and 3D Hyper-Chaotic Henon Map

Ling Wang [1,*], Qiwen Ran [2] and Junrong Ding [2]

[1] School of Internet, Anhui University, Hefei 230039, China
[2] National Key Laboratory of Tunable Laser Technology, Harbin Institute of Technology, Harbin 150001, China
* Correspondence: wangling@ahu.edu.cn

Abstract: In encryption technology, image scrambling is a common processing operation. This paper proposes a quantum version of the 3D Mobius scrambling transform based on the QRCI model, which changes not only the position of pixels but also the gray values. The corresponding quantum circuits are devised. Furthermore, an encryption scheme combining the quantum 3D Mobius transform with the 3D hyper-chaotic Henon map is suggested to protect the security of image information. To facilitate subsequent processing, the RGB color image is first represented with QRCI. Then, to achieve the pixel-level permutation effect, the quantum 3D Mobius transform is applied to scramble bit-planes and pixel positions. Ultimately, to increase the diffusion effect, the scrambled image is XORed with a key image created by the 3D hyper-chaotic Henon map to produce the encrypted image. Numerical simulations and result analyses indicate that our designed encryption scheme is secure and reliable. It offers better performance in the aspect of key space, histogram variance, and correlation coefficient than some of the latest algorithms.

Keywords: quantum 3D Mobius scrambling; 3D hyper-chaotic Henon map; quantum circuits; quantum image encryption

check for updates

Citation: Wang, L.; Ran, Q.; Ding, J. Image Encryption Using Quantum 3D Mobius Scrambling and 3D Hyper-Chaotic Henon Map. *Entropy* **2023**, *25*, 1629. https://doi.org/10.3390/e25121629

Academic Editors: Qin Wang, Hong-Wei Li, Jin Dong Wang and Xing-Yu Zhou

Received: 25 October 2023
Revised: 27 November 2023
Accepted: 4 December 2023
Published: 6 December 2023

1. Introduction

Based on the principles of quantum mechanics, quantum computing, which provides massive parallel computation [1], and unconditional security [2] for the data have been widely used in many information science fields. Quantum computing lays a solid foundation for the emergence and development of quantum information processing technology [3,4]. Since images are an important information transmission medium [5,6], how to process image information in quantum computers is a hotspot in research [7]. Quantum image processing has great significance to the security of images.

To store images by using qubits in quantum computers, researchers developed a great deal of representation models [8]. Qubit Lattice, as the first representation model, was put forward in 2003 [9]. Afterward, Real Ket, which allows using n qubits to represent an image of size $2^n \times 2^n$ was proposed [10]. In 2011, FRQI representation was designed [11], in which the image information was encoded as a superposition of quantum entangled states. Extending from FRQI, Zhang et al. presented NEQR representation [12]. It uses an entangled qubit sequence to encode grayscale information. After that, some other representation models were successively raised, including QUALPI [13], NAQSS [14], NCQI [15], GNEQR [16], FTQR [17], QIRHSI [18] and many more. Recently, Wang et al. devised the QRCI representation for storing RGB color images, which has a lower quantum cost [19].

Since quantum computing has enormous information-carrying capacity and strong computing power, many image encryption techniques making use of quantum computing have been suggested. Zhou et al. achieved an encryption algorithm with geometric transformations in 2013 [20]. In 2014, by means of restricted geometric and color transformations, Song et al. presented an encryption method for FRQI images [21]. Subsequently, the quantum realization circuit of the generalized Arnold transform was constructed and put to use in [22,23]. Gong et al. designed a novel encryption scheme by exploiting quantum XOR operations [24]. To solve the problem that some spatial domain transforms are periodic, an encryption algorithm by utilizing Fibonacci scrambling and geometric transform iteratively was presented [25]. In addition, Li et al. achieved an encryption method by exploiting phase-shift transform and Haar wavelet transform [26]. With the bit-level permutation operation, a cryptosystem for the NEQR model was proposed [27]. By utilizing image correlation decomposition, Zhang et al. proposed a quantum image encryption algorithm, which has a large key space [28]. Song et al. encrypted the QIRHSI image by using geometric transformation and intensity channel diffusion [29]. Lately, Liu et al. presented an independent bit-plane permutation, which was used to create a novel algorithm to encrypt quantum images [30]. Gao et al. developed an encryption technique based on quantum DNA coding and Hilbert scrambling operation [31].

Quantum image encryption using scrambling transforms is a widely used technique. Traditional algorithms like Arnold, Fibonacci, and Hilbert have been implemented using quantum circuits for image scrambling, as described in [32,33]. However, these algorithms have a limited range of scrambling and only disrupt the positions of pixels, leaving the distribution of pixel grayscales unchanged [34]. Therefore, it is crucial to explore newer and more efficient quantum scrambling algorithms that can be applied to quantum image encryption to enhance the security of cryptosystems. In this paper, a quantum image scrambling algorithm is designed based on the 3D Mobius transform to simultaneously change pixel locations and gray values, effectively eliminating correlation between adjacent pixels. To protect the security of quantum images, an encryption scheme is proposed that combines quantum 3D Mobius scrambling with a 3D hyper-chaotic Henon map. Firstly, the RGB color image is represented with QRCI. Then, to achieve the pixel-level permutation effect, the quantum 3D Mobius transform is applied to scramble bit-planes and pixel positions. Finally, to improve the security performance, quantum XOR operations controlled by the 3D hyper-chaotic Henon map are adopted to modify the color information of the scrambled image to obtain the ciphertext image. All of the quantum circuits utilized in the encryption procedure are developed. The main work of this study is summarized as below.

1. A quantum image-scrambling algorithm is created based on the 3D Mobius transform, which has a pixel-level scrambling effect and performs better than the quantum Arnold/Fibonacci transform.
2. A quantum image encryption scheme is suggested by combining quantum 3D Mobius scrambling with XOR diffusion. The quantum circuits for encryption operation are designed.
3. To obtain the desired encryption effect, the scrambling and diffusion operations are controlled by sequences generated by the 3D hyper-chaotic Henon map. The security of our encryption scheme is enhanced by the randomness and unpredictability of chaotic sequences.
4. Simulation results and comparative analysis demonstrate that our designed encryption scheme exhibits significant reliability and security.

The remainder of this paper is structured as follows. In Section 2, we briefly review the preliminary knowledge. Section 3 describes how to procure a quantum 3D Mobius scrambling algorithm in detail. The process of encryption and decryption is given in Section 4. Section 5 presents simulation results and comparative analysis. Finally, Section 6 concludes this paper.

2. Preliminaries

2.1. QRCI Image Representation Model

QRCI can represent a RGB color image of size $2^n \times 2^n$ by using only $2n+6$ qubits [19], whose storage capacity is 2^{18} times higher than that of NCQI.

Supposing a $2^n \times 2^n$ RGB color image and each channel takes values within $[0, 255]$, the corresponding QRCI is expressed as:

$$
\begin{aligned}
|I\rangle &= \frac{1}{\sqrt{2^{2n+3}}} \sum_{L=0}^{2^3-1} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} |C_L(Y,X)\rangle \otimes |LYX\rangle \\
&= \frac{1}{\sqrt{2^{2n+3}}} \sum_{L=0}^{2^3-1} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} |R_{LYX} G_{LYX} B_{LYX}\rangle \otimes |LYX\rangle
\end{aligned} \tag{1}
$$

where $R_{LYX}, G_{LYX}, B_{LYX} \in \{0,1\}$ represent the values of three channels on the L-th bit-plane in position (Y,X), respectively. $|L\rangle = |L_2 L_1 L_0\rangle$ denotes the bit-plane order and $|YX\rangle = |Y_{n-1} Y_{n-2} \dots Y_0\rangle |X_{n-1} X_{n-2} \dots X_0\rangle$ denotes the pixel position. The comparative analysis in reference [19] shows that QRCI requires fewer qubits compared with the other representation models.

2.2. Quantum Modules

Some basic quantum modules required in our algorithm are introduced in this subsection.

Quantum adder (ADDER) can calculate the sum of two numbers [35]. Its circuit is exhibited in Figure 1a.

If the black bar is adjusted to the left, Figure 1a will become a quantum subtractor. Figure 1b shows the corresponding circuit.

In addition, quantum double-output adder (D-ADDER) [36] and quantum multiplier (MULER) [37] are also exploited in this paper, whose circuits are displayed in Figure 1c and Figure 1d, respectively.

Quantum comparator (COMOR) is implemented to show the comparison result of two numbers, i.e., $c = 0$, when $b \geq a$; otherwise, $c = 1$ [38]. The corresponding circuit is shown in Figure 1e.

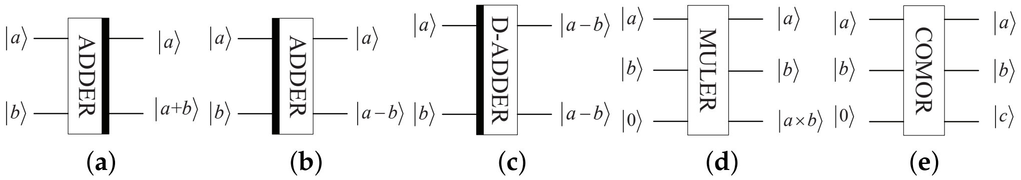


Figure 1. Basic quantum modules: (**a**) adder, (**b**) subtractor, (**c**) double-output adder, (**d**) multiplier, (**e**) comparator.

2.3. 3D Hyper-Chaotic Henon Map

The mathematical expression of 3D hyper-chaotic Henon map is:

$$
\begin{cases}
u_{i+1} = \sigma - v_i^2 - \rho w_i \\
v_{i+1} = u_i \\
w_{i+1} = v_i
\end{cases} \tag{2}
$$

where u, v and w denote three variables, while σ and ρ are two control parameters. When σ and ρ are 1.99, 0.001, respectively, map (2) exhibits a hyper-chaotic behavior [39]. The initial values are set to $u_0 = 0$, $v_0 = 0$, and $w_0 = 0.1$. Figures 2 and 3 display the bifurcation diagram and phase diagram of the 3D hyper-chaotic Henon map, respectively.

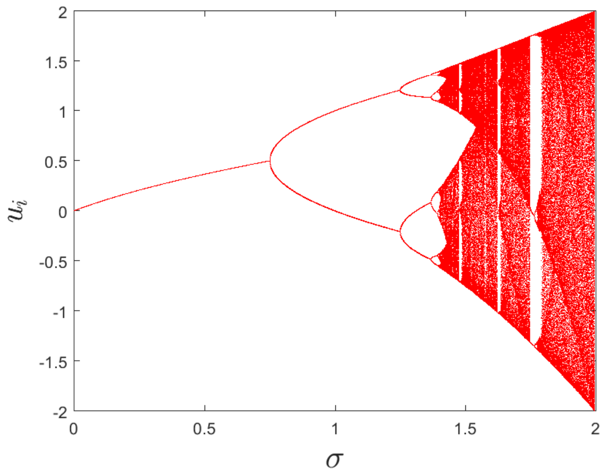


Figure 2. The bifurcation diagram of u-sequence.

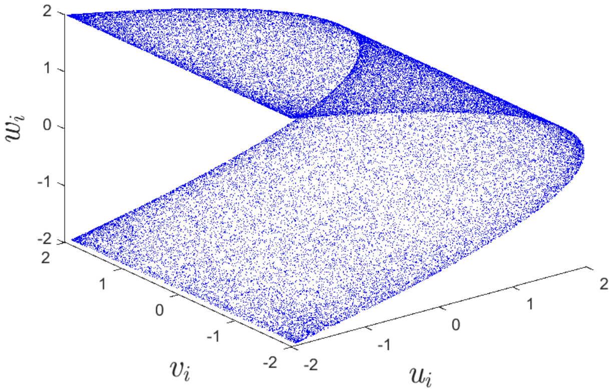


Figure 3. The phase diagram of 3D hyper-chaotic Henon map.

As the hyper-chaotic maps have more complicated dynamic behaviors than 1D chaotic maps, this paper adopts map (2) to create the sequences controlling the encryption operations. The randomness and unpredictability of chaotic sequences will improve the encryption effect.

3. Three-Dimensional (3D) Mobius Quantum Image-Scrambling Algorithm

3.1. Two-Dimensional (2D) Mobius Transform

The Mobius band is a topological transform in continuous space; that is, the rectangular band is folded reversely and then the vertices are overlapped in pairs. To apply this topological transform to image scrambling, the image can be regarded as a rectangular Mobius band consisting of discrete dot arrays. Suppose the matrix of an image with size $M \times N$ is represented as $A = \left[a_{ij}\right]_{M \times N}$. When the image is folded reversely along the horizontal direction, the i-th row and the $(M+1-i)$-th row $(i = 1, 2, \cdots, M)$ correspond to each other. Likewise, when the image is folded reversely along the vertical direction, the j-th column and the $(N+1-j)$-th column $(j = 1, 2, \cdots, N)$ correspond to each other. Pairwise corresponding rows or columns form a circle. By performing shift operation on it, the image-scrambling model based on the Mobius band can be deduced, where the count of the cycle shift operation can be regarded as the image-scrambling parameters.

Assuming there are two sequences $\{r(1), r(2), \ldots, r(M)\}$, $\{c(1), c(2), \ldots, c(N)\}$, for $\forall\, i, j$, they satisfy $r(i) = r(M-i+1) \in \{1, 2, \ldots, N\}$, $c(j) = c(N-j+1) \in \{1, 2, \ldots, M\}$; then, the discrete expression of spatial domain image scrambling based on the 2D Mobius transform is as shown below.

For the horizontal direction folding, $S_x(i,j)$ is as:

$$S_x(i,j) = \begin{cases} (M-i+1, N-r(i)+j), & 1 \le j \le r(i) \\ (i, j-r(i)), & r(i) < j \le N \end{cases} \tag{3}$$

where $r(i)$ is the shift count of the i-th row.

For the vertical direction folding, $S_y(i,j)$ is as:

$$S_y(i,j) = \begin{cases} (M-c(j)+i, N-j+1), & 1 \le i \le c(j) \\ (i-c(j), j), & c(j) < i \le M \end{cases} \tag{4}$$

where $c(j)$ is the shift count of the j-th column.

The scrambled image $S(A)$ can be obatined after the original image A is successively transformed once by (3) and (4). In order to obtain a better scrambling effect, the scrambling operation can be performed many times.

The inverse 2D Mobius transform can be realized by executing the following equations:

$$S_y^{-1}(i,j) = \begin{cases} (i+c(j)-M, N-j+1), & M-c(j) < i \le M \\ (i+c(j), j), & 1 \le i \le M-c(j) \end{cases} \tag{5}$$

$$S_x^{-1}(i,j) = \begin{cases} (M-i+1, j+r(i)-N), & N-r(i) < j \le N \\ (i, j+r(i)), & 1 \le j \le N-r(i) \end{cases} \tag{6}$$

3.2. Three-Dimensional (3D) Mobius Scrambling Algorithm

Two-dimensional (2D) Mobius transform can be expanded to the 3D Mobius transform. Suppose there is a three-dimensional cube $A = \left[a_{ijl}\right]_{W\times H\times L}$. Three matrices $[r_1(j,l)]_{H\times L}$, $[r_2(i,l)]_{W\times L}$ and $[r_3(i,j)]_{W\times H}$ are used to control the shift counts, and for $\forall\, i,j,l$, they satisfy $r_1(j,l) = r_1(H-j+1, L-l+1) \in \{1,2,\ldots,W\}$, $r_2(i,l) = r_2(W-i+1, L-l+1) \in \{1,2,\ldots,H\}$, $r_3(i,j) = r_3(W-i+1, H-j+1) \in \{1,2,\ldots,L\}$. The corresponding three scrambling operations based on the 2D Mobius transform are as follows.

For the x-axis direction folding, the expression of discrete transform $S_x(i,j,l)$ is as follows:

$$S_x(i,j,l) = \begin{cases} (W-r_1(j,l)+i, H-j+1, L-l+1), & 1 \le i \le r_1(j,l) \\ (i-r_1(j,l), j, l), & r_1(j,l) < i \le W \end{cases} \tag{7}$$

where $r_1(j,l)$ is the shift count.

For the y-axis direction folding, the expression of discrete transform $S_y(i,j,l)$ is as follows:

$$S_y(i,j,l) = \begin{cases} (W-i+1, H-r_2(i,l)+j, L-l+1), & 1 \le j \le r_2(i,l) \\ (i, j-r_2(i,l), l), & r_2(i,l) < j \le H \end{cases} \tag{8}$$

where $r_2(i,l)$ is the shift count.

Likewise, for the z-axis direction folding, the expression of discrete transform $S_z(i,j,l)$ is as follows:

$$S_z(i,j,l) = \begin{cases} (W-i+1, H-j+1, L-r_3(i,j)+l), & 1 \le l \le r_3(i,j) \\ (i, j, l-r_3(i,j)), & r_3(i,j) < l \le L \end{cases} \tag{9}$$

where $r_3(i,j)$ is the shift count.

Calculating Equations (7)–(9) in order; then, the result of 3D Mobius scrambling can be obtained. The scrambling algorithm can be performed as many times as needed.

The inverse 3D Mobius transform can be realized by executing the following equations in order:

$$S_z^{-1}(i,j,l) = \begin{cases} (W-i+1, H-j+1, l+r_3(i,j)-L), & L-r_3(i,j) < l \le L \\ (i,j,l+r_3(i,j)), & 1 \le l \le L-r_3(i,j) \end{cases} \tag{10}$$

$$S_y^{-1}(i,j,l) = \begin{cases} (W-i+1, j+r_2(i,l)-H, L-l+1), & H-r_2(i,l) < j \le H \\ (i,j+r_2(i,l),l), & 1 \le j \le H-r_2(i,l) \end{cases} \tag{11}$$

$$S_x^{-1}(i,j,l) = \begin{cases} (i+r_1(j,l)-W, H-j+1, L-l+1), & W-r_1(j,l) < i \le W \\ (i+r_1(j,l),j,l), & 1 \le i \le W-r_1(j,l) \end{cases} \tag{12}$$

3.3. The Quantum Circuit of 3D Mobius Scrambling

In this paper, the QRCI model is adopted, which can be viewed as a 3D image model, where the three dimensions are the X-axis, Y-axis, and L-axis, respectively. Therefore, we consider scrambling a QRCI image shown in Equation (1) by using the 3D Mobius transform. It should be noted that $X, Y \in [0, 2^n - 1]$ and $L \in \left[0, 2^3 - 1\right]$. Assuming $S = S_L S_Y S_X$, quantum 3D Mobius scrambling transform M_b can be constructed as follows:

$$M_b = I^{\otimes 3} \otimes S = I^{\otimes 3} \otimes (S_L S_Y S_X) \tag{13}$$

By performing M_b on the QRCI image $|I\rangle$, the scrambled image $\left|I_{M_b}\right\rangle$ can be obtained:

$$\begin{aligned} \left|I_{M_b}\right\rangle &= M_b|I\rangle \\ &= \left(I^{\otimes 3} \otimes S\right) \frac{1}{\sqrt{2^{2n+3}}} \sum_{L=0}^{2^3-1} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} |C_L(Y,X)\rangle \otimes |LYX\rangle \\ &= \frac{1}{\sqrt{2^{2n+3}}} \sum_{L=0}^{2^3-1} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} |C_L(Y,X)\rangle \otimes S_L S_Y S_X(|LYX\rangle) \\ &= \frac{1}{\sqrt{2^{2n+3}}} \sum_{L=0}^{2^3-1} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} |C_L(Y,X)\rangle \otimes |L^* Y^* X^*\rangle \end{aligned} \tag{14}$$

where S_X, S_Y and S_L perform the following functions:

$$\begin{aligned} &\left|L'Y'X'\right\rangle = S_X|LYX\rangle \\ &= \begin{cases} \left|2^3-1-L\right\rangle|2^n-1-Y\rangle|2^n-U(L,Y)+X\rangle, & 0 \le X < U(L,Y) \\ |L\rangle|Y\rangle|X-U(L,Y)\rangle, & U(L,Y) \le X \le 2^n-1 \end{cases} \end{aligned} \tag{15}$$

$$\begin{aligned} &\left|L'Y'X'\right\rangle = S_Y|LYX\rangle \\ &= \begin{cases} \left|2^3-1-L\right\rangle|2^n-V(L,X)+Y\rangle|2^n-1-X\rangle, & 0 \le Y < V(L,X) \\ |L\rangle|Y-V(L,X)\rangle|X\rangle, & V(L,X) \le Y \le 2^n-1 \end{cases} \end{aligned} \tag{16}$$

$$\begin{aligned} &\left|L'Y'X'\right\rangle = S_L|LYX\rangle \\ &= \begin{cases} \left|2^3-W(Y,X)+L\right\rangle|2^n-1-Y\rangle|2^n-1-X\rangle, & 0 \le L < W(Y,X) \\ |L-W(Y,X)\rangle|Y\rangle|X\rangle, & W(Y,X) \le L \le 2^3-1 \end{cases} \end{aligned} \tag{17}$$

where $U(L,Y)$, $V(L,X)$ and $W(Y,X)$ denote the shift counts of folding along the X-axis, Y-axis and L-axis, respectively. For $\forall\, X, Y, L$, they satisfy $U(L,Y) = U\left(2^3-1-L, 2^n-1-Y\right) \in \{0,1,\ldots,2^n-1\}$, $V(L,X) = V\left(2^3-1-L, 2^n-1-X\right) \in \{0,1,\ldots,2^n-1\}$, $W(Y,X) = W(2^n-1-Y, 2^n-1-X) \in \left\{0,1,\ldots,2^3-1\right\}$.

According to Equation (13), the quantum 3D Mobius scrambling algorithm can be implemented by three sub-operations, i.e., S_X, S_Y and S_L. For the sub-operation S_X, it can be implemented as follows. First, the subfunction, when $0 \leq X < U(L,Y)$, is implemented:

$$P|LYX\rangle = \left|2^3 - 1 - L\right\rangle|2^n - 1 - Y\rangle|2^n - U(L,Y) + X\rangle \tag{18}$$

After that, the result obtained from Equation (18) is transformed by the following formula:

$$Q|LYX\rangle = \left|2^3 - 1 - L\right\rangle|2^n - 1 - Y\rangle|X - 2^n\rangle \tag{19}$$

As a result, the composite of P and Q is equivalent to the subfunction when $U(L,Y) \leq X \leq 2^n - 1$:

$$QP|LYX\rangle = |L\rangle|Y\rangle|X - U(L,Y)\rangle \tag{20}$$

By using some basic quantum modules, Figure 4a shows the circuit of S_X. Similarly, Figure 4b,c shows the circuits of S_Y and S_L, respectively.

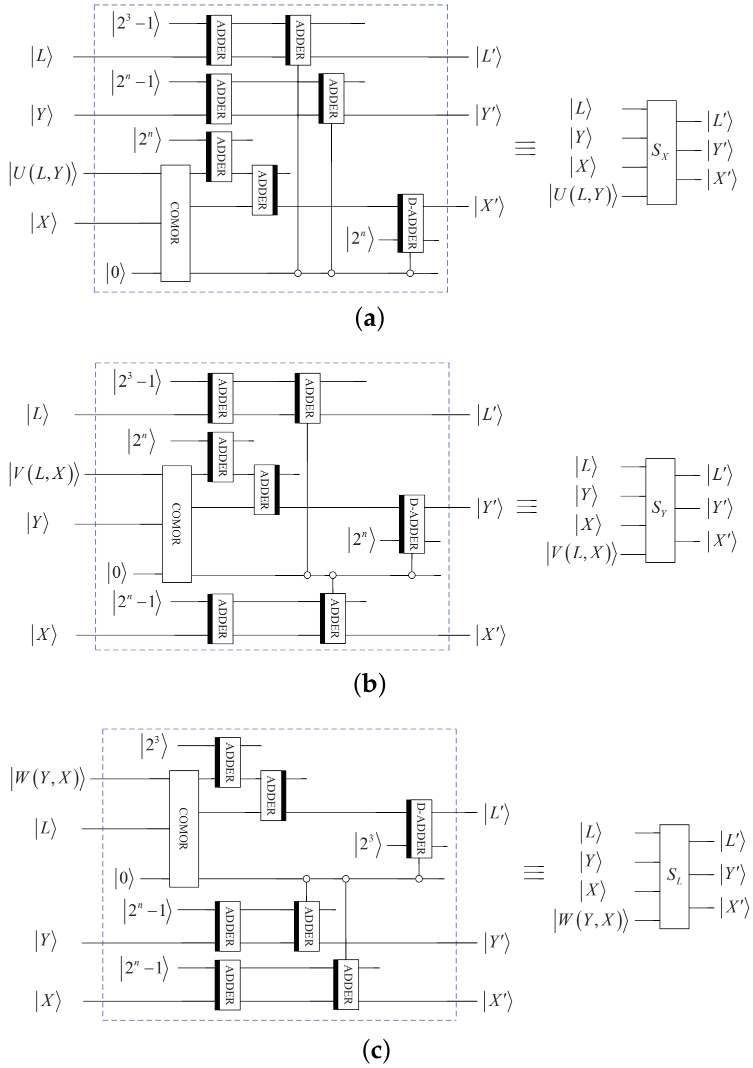


Figure 4. Elementary quantum circuits: (**a**) S_X. (**b**) S_Y. (**c**) S_L.

Above all, the whole quantum circuit of 3D Mobius scrambling is shown in Figure 5.

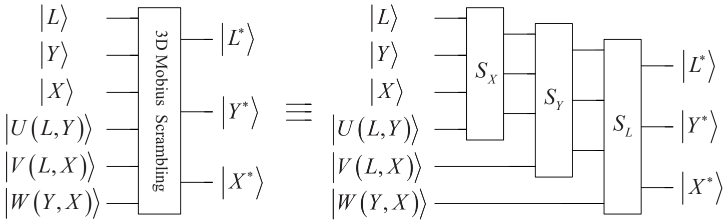


Figure 5. Quantum circuit for 3D Mobius scrambling transform.

Inverse 3D Mobius scrambling is needed to recover the original image. Supposing $S^{-1} = S_X^{-1}S_Y^{-1}S_L^{-1}$, quantum inverse 3D Mobius scrambling transform M_b^{-1} can be constructed as:

$$M_b^{-1} = I^{\otimes 3} \otimes S^{-1} = I^{\otimes 3} \otimes \left(S_X^{-1}S_Y^{-1}S_L^{-1}\right) \tag{21}$$

Through applying the transform M_b^{-1} to $|I_{M_b}\rangle$, the original QRCI image can be gained:

$$\begin{aligned} |I\rangle &= M_b^{-1}|I_{M_b}\rangle \\ &= \left(I^{\otimes 3} \otimes S^{-1}\right)\frac{1}{\sqrt{2^{2n+3}}}\sum_{L=0}^{2^3-1}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|C_L(Y,X)\rangle \otimes |L^*Y^*X^*\rangle \\ &= \frac{1}{\sqrt{2^{2n+3}}}\sum_{L=0}^{2^3-1}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|C_L(Y,X)\rangle \otimes S_X^{-1}S_Y^{-1}S_L^{-1}(|L^*Y^*X^*\rangle) \\ &= \frac{1}{\sqrt{2^{2n+3}}}\sum_{L=0}^{2^3-1}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|C_L(Y,X)\rangle \otimes |LYX\rangle \end{aligned} \tag{22}$$

where S_L^{-1}, S_Y^{-1} and S_X^{-1} perform the following functions:

$$\begin{aligned} &|L'Y'X'\rangle = S_L^{-1}|LYX\rangle \\ =&\begin{cases} \left|L + W(Y,X) - 2^3\right\rangle|2^n - 1 - Y\rangle|2^n - 1 - X\rangle, & 2^3 - W(Y,X) \le L \le 2^3 - 1 \\ |L + W(Y,X)\rangle|Y\rangle|X\rangle, & 0 \le L < 2^3 - W(Y,X) \end{cases} \end{aligned} \tag{23}$$

$$\begin{aligned} &|L'Y'X'\rangle = S_Y^{-1}|LYX\rangle \\ =&\begin{cases} \left|2^3 - 1 - L\right\rangle|Y + V(L,X) - 2^n\rangle|2^n - 1 - X\rangle, & 2^n - V(L,X) \le Y \le 2^n - 1 \\ |L\rangle|Y + V(L,X)\rangle|X\rangle, & 0 \le Y < 2^n - V(L,X) \end{cases} \end{aligned} \tag{24}$$

$$\begin{aligned} &|L'Y'X'\rangle = S_X^{-1}|LYX\rangle \\ =&\begin{cases} \left|2^3 - 1 - L\right\rangle|2^n - 1 - Y\rangle|X + U(L,Y) - 2^n\rangle, & 2^n - U(L,Y) \le X \le 2^n - 1 \\ |L\rangle|Y\rangle|X + U(L,Y)\rangle, & 0 \le X < 2^n - U(L,Y) \end{cases} \end{aligned} \tag{25}$$

For the sub-operation S_L^{-1}, it can be implemented in two steps. The first step is to implement the subfunction when $0 \le L < 2^3 - W(Y,X)$:

$$P'|LYX\rangle = |L + W(Y,X)\rangle|Y\rangle|X\rangle \tag{26}$$

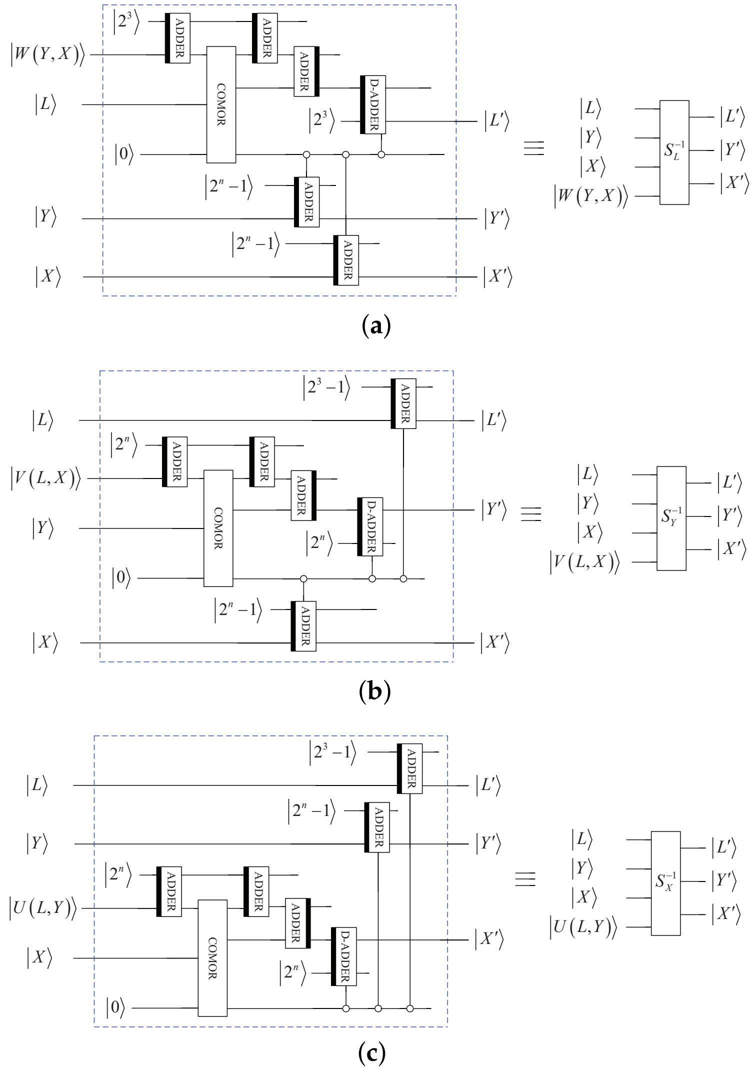
The second step is to modify the produced result by utilizing the following formula:

$$Q'|LYX\rangle = \left|L - 2^3\right\rangle|2^n - 1 - Y\rangle|2^n - 1 - X\rangle \tag{27}$$

Therefore, when $2^3 - W(Y,X) \leq L \leq 2^3 - 1$, the corresponding subfunction is equivalent to the composite of P' and Q' as below:

$$Q'P'|LYX\rangle = \left|L + W(Y,X) - 2^3\right\rangle|2^n - 1 - Y\rangle|2^n - 1 - X\rangle \tag{28}$$

The quantum circuit of sub-operation S_L^{-1} is depicted in Figure 6a. In the same way, the quantum circuits of S_Y^{-1} and S_X^{-1} are depicted in Figure 6b,c.



(**a**)

(**b**)

(**c**)

Figure 6. Elementary quantum circuits: (**a**) S_L^{-1}. (**b**) S_Y^{-1}. (**c**) S_X^{-1}.

The whole circuit for quantum inverse 3D Mobius scrambling transform is shown in Figure 7.

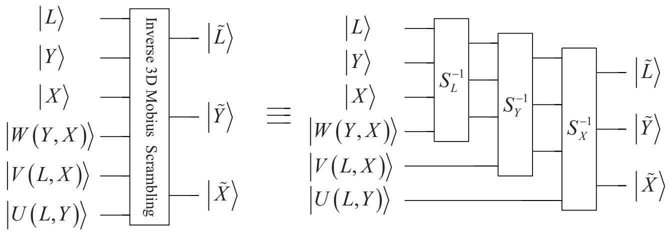


Figure 7. Quantum circuit for inverse 3D Mobius transform.

3.4. Scrambling Result and Anti-Attack Ability Analysis

To verify the scrambling result of the 3D Mobius transform, a 256 × 256 color image of peppers shown in Figure 8a is used for testing. Three matrices that control the shift counts are randomly selected. The scrambled image after applying the 3D Mobius transform one time is shown in Figure 8b. It demonstrates that the 3D Mobius scrambling transform is effective and can visually hide the information about the image.

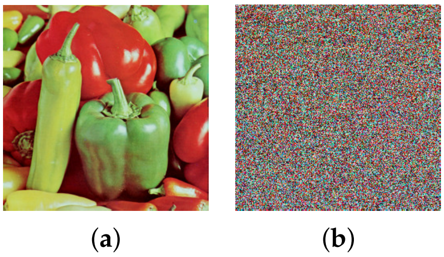
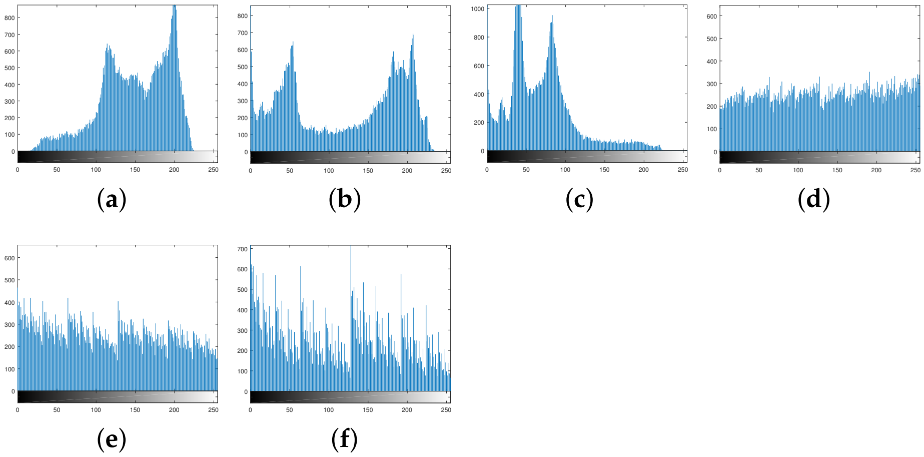

(**a**) (**b**)

Figure 8. Scrambling results: (**a**) Peppers, (**b**) scrambled Peppers.

The histogram distributions are displayed in Figure 9. Figure 10a,b show the scrambled images after 100 iterations of the Arnold and Fibonacci transforms, respectively. The corresponding RGB histograms are displayed in Figure 11. The 3D Mobius scrambling transform differs from the Arnold/Fibonacci transform in that it changes both the position of pixels and the distribution of gray values in the histogram. This is because it simultaneously scrambles bit-planes and pixel positions. As a result, the 3D Mobius scrambling transform alters the statistical properties of the original image to a significant extent.



(**a**) (**b**) (**c**) (**d**)
(**e**) (**f**)

Figure 9. Histograms: (**a**) R channel of Peppers. (**b**) G channel of Peppers. (**c**) B channel of Peppers. (**d**) R channel of scrambled Peppers. (**e**) G channel of scrambled Peppers. (**f**) B channel of scrambled Peppers.

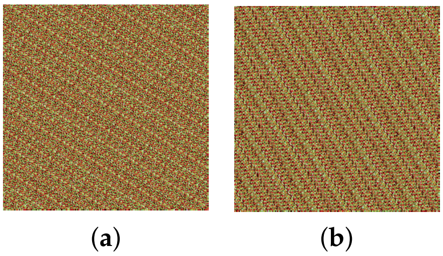
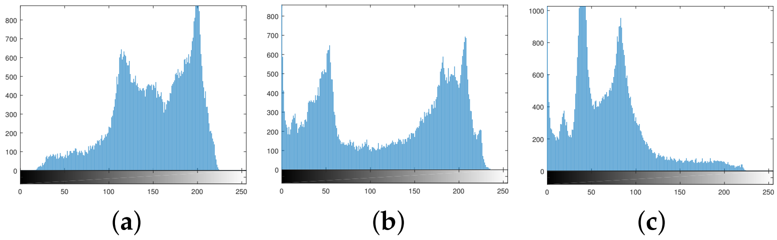

(**a**) (**b**)

Figure 10. Scrambling results of Arnold/Fibonacci transform: (**a**) Arnold. (**b**) Fibonacci.



(**a**) (**b**) (**c**)

Figure 11. Histograms of using Arnold/Fibonacci transform: (**a**) R channel. (**b**) G channel. (**c**) B channel.

To further estimate the scrambling performance of the 3D Mobius transform, the correlation of adjacent pixels is considered. The formula for calculating the coefficient used to evaluate this correlation is:

$$CC = \frac{\sum\limits_{i=1}^{H}(x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\sum\limits_{i=1}^{H}(x_i - \overline{x})^2 \sum\limits_{i=1}^{H}(y_i - \overline{y})^2}} \tag{29}$$

where x_i and y_i denote two neighboring pixel values. $\overline{x} = \frac{1}{H}\sum_{i=1}^{H} x_i$ and $\overline{y} = \frac{1}{H}\sum_{i=1}^{H} y_i$ are the expectation values. The CC values of Peppers in horizontal, vertical, and diagonal directions are listed in Table 1. It is shown that the correlation of adjacent pixels has been significantly reduced.

Table 1. Adjacent pixel correlation coefficient.

Peppers	Original			Scrambled		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
R	0.9704	0.9646	0.9400	0.0114	0.0103	0.0119
G	0.9740	0.9698	0.9470	−0.0091	0.0062	−0.0077
B	0.9645	0.9534	0.9261	0.0046	0.0065	0.0068

Hou et al. proposed a quantum image-scrambling algorithm based on a discrete Baker map, which could be implemented by swapping qubits [34]. The CC values of scrambled Peppers derived from the Baker map are compiled in Table 2. The results show that the correlation between adjacent pixels decreases with the increase in scrambling times. After 16 times of scrambling, the adjacent pixels are almost no longer correlated. It can be seen from Tables 1 and 2 that the 3D Mobius scrambling could weaken the correlation better since it has more scrambling parameters.

Table 2. Adjacent pixel correlation coefficient of scrambled Peppers in [34].

Scrambled Peppers	Horizontal	Vertical	Diagonal
1 time	0.9704	0.8369	0.7654
3 times	0.6275	0.2013	0.0708
16 times	0.0724	0.0724	0.0176
96 times	0.0285	0.0170	0.0129

If the scrambling algorithm is open, assume that the attackers do not know the key matrices and make a brute-force attack. Since $U(L,Y) \in [0, 2^n - 1]$, $V(L,X) \in [0, 2^n - 1]$, $W(Y,X) \in \left[0, 2^3 - 1\right]$, in the 3D Mobius transform, for each row transform in the X-axis direction, the probability of cracking success is $\frac{1}{2^n}$. Therefore, for the entire X-axis direction; the probability of cracking success is $2^{n - 2^n \times 2^3}$. The coupling of the X-axis, Y-axis, and Z-axis makes it even more difficult to crack, the probability of cracking success is

$2^{n-2^n\times 2^3}2^{n-2^n\times 2^3}2^{3-2^n\times 2^n}$. Thus, the 3D Mobius transform has a relatively good resistance to brute-force attacks.

Consequently, the quantum 3D Mobius scrambling is employed as an encryption means in the encryption scheme to be raised below.

4. Encryption and Decryption Scheme

4.1. Encryption Scheme

Combining 3D Mobius scrambling with the 3D hyper-chaotic Henon map, our proposed quantum image encryption scheme includes five steps. Figure 12 exhibits the encryption procedure.

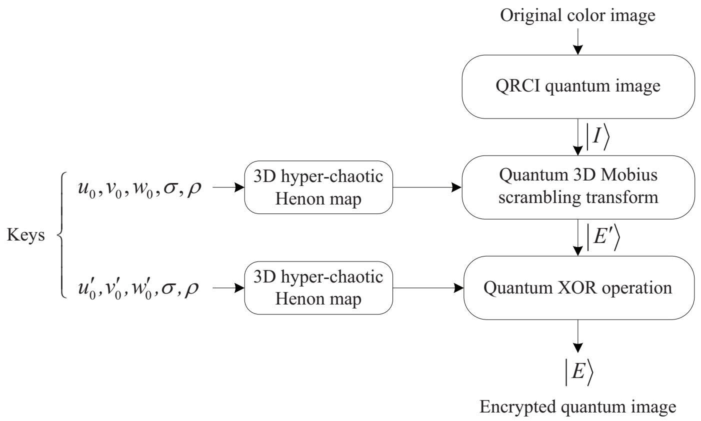

Original color image
QRCI quantum image
$|I\rangle$
Keys
$u_0, v_0, w_0, \sigma, \rho$
3D hyper-chaotic Henon map
Quantum 3D Mobius scrambling transform
$|E'\rangle$
$u_0', v_0', w_0', \sigma, \rho$
3D hyper-chaotic Henon map
Quantum XOR operation
$|E\rangle$
Encrypted quantum image

Figure 12. The encryption procedure.

Input: A classical RGB color image with size $2^n \times 2^n$.

Keys: Two sets of initial values, $u_0, v_0, w_0, u_0', v_0', w_0'$ and two control parameters σ, ρ.

Output: The final ciphertext image $|E\rangle$.

Step 1. The original RGB color image is represented with QRCI as follows:

$$|I\rangle = \frac{1}{\sqrt{2^{2n+3}}} \sum_{L=0}^{2^3-1} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} |R_{LYX} G_{LYX} B_{LYX}\rangle \otimes |LYX\rangle \tag{30}$$

Step 2. This step generates three matrices that control the quantum 3D Mobius scrambling transform.

According to Equation (2), six computation modules are required for each iteration of the 3D hyper-chaotic Henon map, and the circuit is presented in Figure 13.

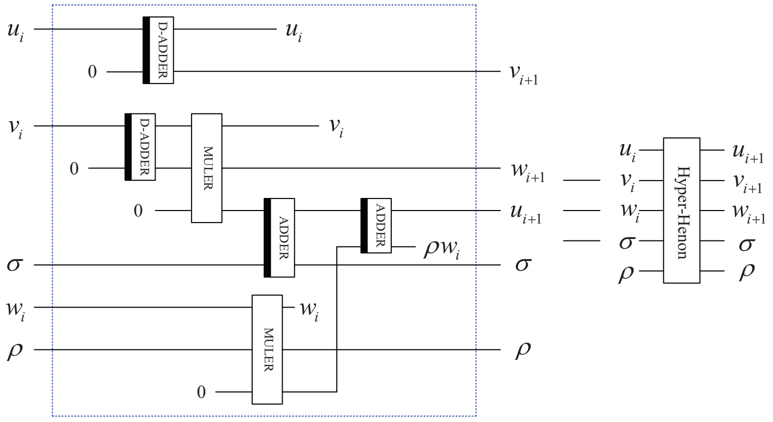


Figure 13. Quantum circuit for implementing one iteration.

By utilizing the complete circuit shown in Figure 14, Equation (2) is iterated $\frac{2^n \times 2^n}{2} + k$ times with the first set of initial values u_0, v_0, and w_0, where k is a positive integer. In general, $k = 2 \times 10^4$. The sequences are taken from the $k+1$ iteration, since the randomness of the beginning part may not be good enough. The constructed sequences $\{u_{k+1}, u_{k+2}, \cdots, u_{k+2^{2n-1}}\}$, $\{v_{k+1}, v_{k+2}, \cdots, v_{k+2^{2n-1}}\}$ and $\{w_{k+1}, w_{k+2}, \cdots, w_{k+2^{2n-1}}\}$ cannot be used directly. They are transformed into integer sequences as shown below:

$$\begin{cases} U_i = floor\left(u_{i+k+1} \times 10^{14}\right) \bmod 2^n \\ V_i = floor\left(v_{i+k+1} \times 10^{14}\right) \bmod 2^n \\ W_j = floor\left(w_{j+k+1} \times 10^{14}\right) \bmod 2^3 \end{cases} \tag{31}$$

where $i = 0, 1, \cdots, \frac{2^3 \times 2^n}{2} - 1$, $j = 0, 1, \cdots, \frac{2^n \times 2^n}{2} - 1$.

Then, the three integer sequences are extended to $[U(L,Y)]_{2^3 \times 2^n}$, $[V(L,X)]_{2^3 \times 2^n}$, $[W(Y,X)]_{2^n \times 2^n}$, and for $\forall X, Y, L$, they satisfy $U(L,Y) = U\left(2^3 - 1 - L, 2^n - 1 - Y\right) \in \{0, 1, \ldots, 2^n - 1\}$, $V(L,X) = V\left(2^3 - 1 - L, 2^n - 1 - X\right) \in \{0, 1, \ldots, 2^n - 1\}$, $W(Y,X) = W(2^n - 1 - Y, 2^n - 1 - X) \in \left\{0, 1, \ldots, 2^3 - 1\right\}$. The obtained integer matrices will be used to control the shift counts.

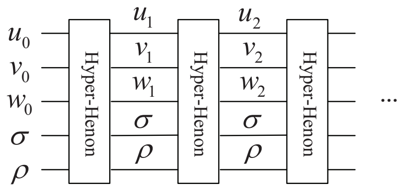


Figure 14. The complete quantum circuit for 3D hyper-chaotic Henon map.

Step 3. By using the obtained three matrices and the quantum 3D Mobius scrambling transform M_b designed in Section 3.3, the scrambled image $|E'\rangle$ will be produced after carrying out the 3D Mobius transform on original image $|I\rangle$:

$$\begin{aligned} \left|E'\right\rangle &= M_b|I\rangle \\ &= \left(I^{\otimes 3} \otimes S\right) \frac{1}{\sqrt{2^{2n+3}}} \sum_{L=0}^{2^3-1} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} |R_{LYX} G_{LYX} B_{LYX}\rangle \otimes |LYX\rangle \\ &= \frac{1}{\sqrt{2^{2n+3}}} \sum_{L=0}^{2^3-1} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} |R_{LYX} G_{LYX} B_{LYX}\rangle \otimes S(|LYX\rangle) \\ &= \frac{1}{\sqrt{2^{2n+3}}} \sum_{L=0}^{2^3-1} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} |R_{LYX} G_{LYX} B_{LYX}\rangle \otimes |L^* Y^* X^*\rangle \end{aligned} \tag{32}$$

where $|L^*\rangle$, $|Y^*\rangle$, and $|X^*\rangle$ can be obtained by calculating Equations (15)–(17) in order.

Different from some classical two-dimensional scrambling transforms, for instance, Arnold/Fibonacci transform [32], 3D Mobius scrambling transform not only disrupts the pixel positions but also disrupts the order of bit-planes. Hence, after the image is transformed, the distribution of its pixel values will be changed, which can improve the security of the cryptosystem. Moreover, the randomness and unpredictability of the parameters in three matrices will make it much harder to decipher the 3D Mobius transform.

Step 4. In this step, we exploit the 3D hyper-chaotic Henon map to construct sequences controlling quantum XOR operations. Similar to step 2, the map shown in Equation (2) is iterated $2^n \times 2^n + k$ times with the second set of initial values u'_0, v'_0, and w'_0. Three chaotic sequences $\left\{u'_{k+1}, u'_{k+2}, \cdots, u'_{k+2^{2n}}\right\}$, $\left\{v'_{k+1}, v'_{k+2}, \cdots, v'_{k+2^{2n}}\right\}$ and $\left\{w'_{k+1}, w'_{k+2}, \cdots, w'_{k+2^{2n}}\right\}$ can be generated. Then, they are calculated as shown below:

$$\begin{cases} U'_i = floor\left(u'_{i+k+1} \times 10^{14}\right) \bmod 2^8 \\ V'_i = floor\left(v'_{i+k+1} \times 10^{14}\right) \bmod 2^8 \\ W'_i = floor\left(w'_{i+k+1} \times 10^{14}\right) \bmod 2^8 \end{cases} \quad (33)$$

where $i = 0, 1, \cdots, 2^{2n} - 1, U'_i, and V'_i, W'_i \in \{0, 1, \cdots, 255\}$.

After that, $\{U'_i\}$, $\{V'_i\}$, $\{W'_i\}$ are stored as an RGB color key image $|K\rangle$. The QRCI representation of $|K\rangle$ is as follows:

$$|K\rangle = \frac{1}{\sqrt{2^{2n+3}}} \sum_{L=0}^{2^3-1} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} \left|U'_{LYX} V'_{LYX} W'_{LYX}\right\rangle \otimes |LYX\rangle \quad (34)$$

Step 5. To further prevent the extraction of original data by unauthorized persons, quantum XOR operations are implemented between the scrambled image $|E'\rangle$ and the key image $|K\rangle$ pixel by pixel, and the final encrypted image $|E\rangle$ will be obtained.

Of course, in order to implement the XOR operation, it should be noted that the positions and bit-planes of $|E'\rangle$ must be equal to that of $|K\rangle$. The quantum circuit to synchronize the positions and bit-planes is given in Figure 15, and they are equal when output $|e\rangle = |1\rangle$.

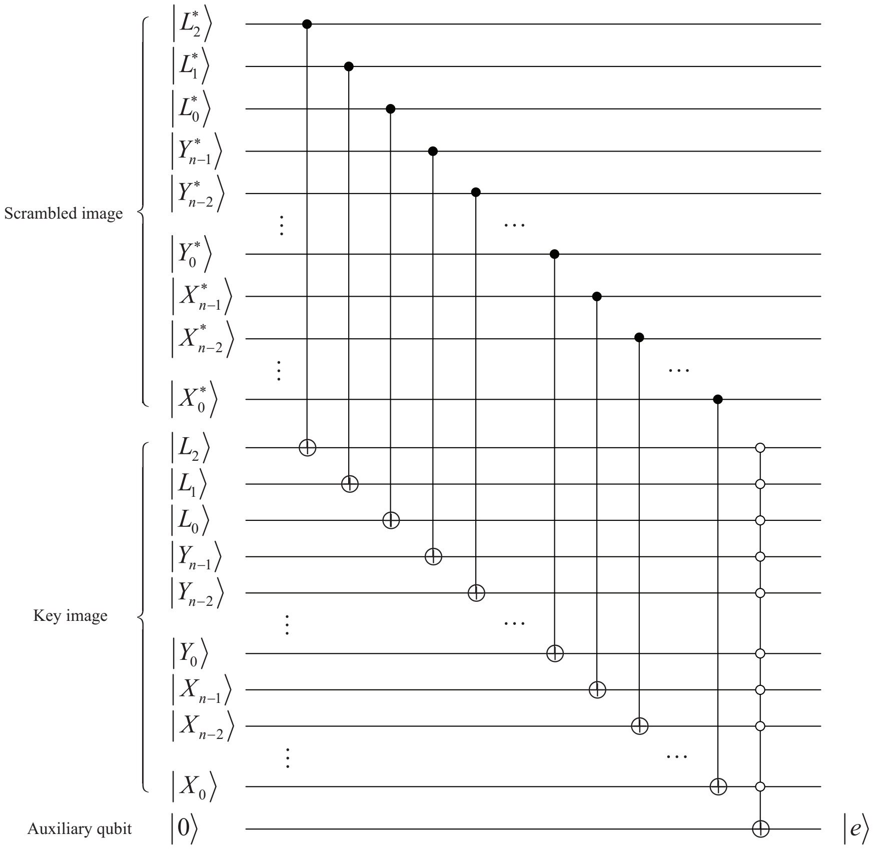


Figure 15. Quantum circuit for synchronizing positions and bit-planes.

The circuit implementing quantum XOR operations is given in Figure 16, in which the output is the final ciphertext image $|E\rangle$.

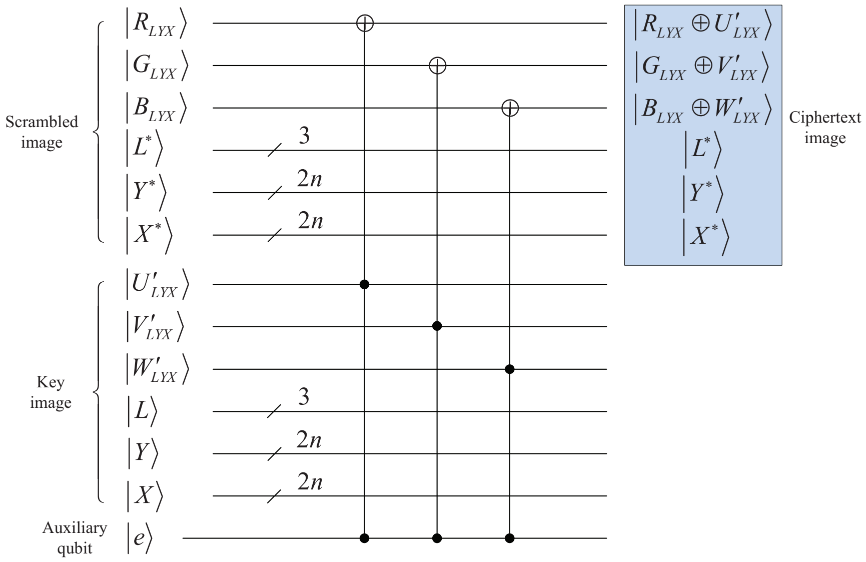


Figure 16. Quantum circuit to implement XOR operation.

4.2. Decryption Scheme

The specific decryption steps are described as below.

Step 1. Taking advantage of correct keys $u'_0, v'_0, andw'_0$, three hyper-chaotic integer sequences $\left\{U'_0, U'_1, \cdots, U'_{2^{2n}-1}\right\}$, $\left\{V'_0, V'_1, \cdots, V'_{2^{2n}-1}\right\}$ and $\left\{W'_0, W'_1, \cdots, W'_{2^{2n}-1}\right\}$ could be obtained with Step 4 in the encryption process. They are stored in a key image $|K\rangle$ based on QRCI representation.

Step 2. The received ciphertext image $|E\rangle$ is XORed with $|K\rangle$ to obtain the scrambled image $|E'\rangle$.

Step 3. According to Step 2 in the encryption process, three hyper-chaotic integer matrices $[U(L,Y)]_{2^3 \times 2^n}$, $[V(L,X)]_{2^3 \times 2^n}$ and $[W(Y,X)]_{2^n \times 2^n}$ which control the shift counts can be constructed.

Step 4. Using the produced three control matrices, the decrypted quantum image represented with the QRCI model can be obtained by executing the inverse quantum 3D Mobius scrambling transform on $|E'\rangle$.

Step 5. The classical image is recovered with quantum measurements. Since QRCI representation stores an image as the superposition of qubit basic states, the classical image can be accurately recovered. In reference [40], the measurement of recovering classical information from the QRCI quantum state was given exhaustively. No detailed explanation of it will be given in this article.

5. Numerical Simulation and Comparative Analysis

The simulations are conducted on a classical computer due to the lack of quantum devices. The selected test images are four 256 × 256 RGB color images, i.e., Lena, Baboon, Splash, and House. According to Equation (2), the map will exhibit a hyper-chaotic behavior when σ and ρ are 1.99 and 0.001, respectively. The initial values are set as $u_0 = 1, v_0 = 0.1$, $w_0 = 0$ and $u'_0 = 1, v'_0 = 1, w'_0 = 1$.

5.1. Visual Effects

Figure 17 shows the simulation results of encryption and decryption. Therein, the four subgraphs in the first row are original images, while the middle row and the last row are encrypted images and decrypted images with correct keys, respectively. Obviously, no meaningful information can be identified from the encrypted images. This verifies that our encryption technique can provide visual protection for the original image.

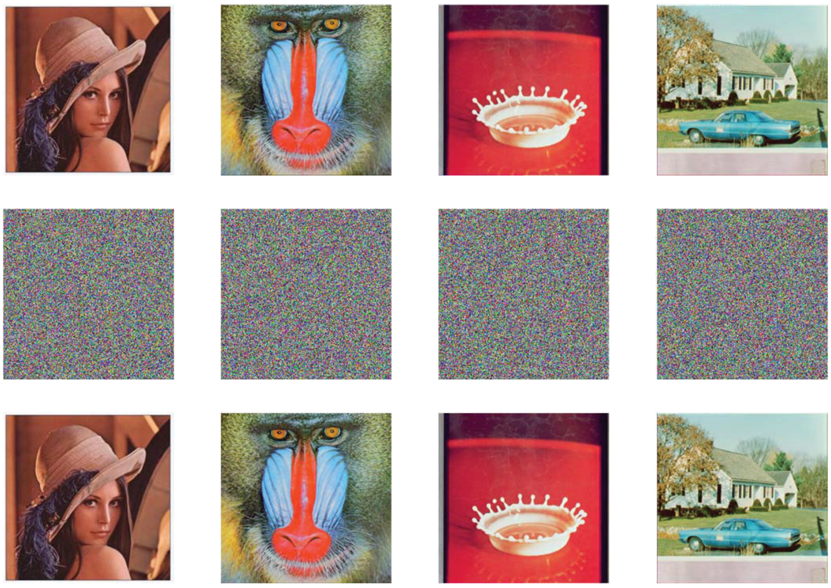


Figure 17. Simulation results.

5.2. Histogram Analysis

The information characteristics of an image can be intuitively reflected by histograms. For a satisfactory ciphertext image, its pixel values must be uniformly distributed [41]. In our proposed encryption scheme, the combination of scrambling and diffusion operations enables a uniform distribution of pixel values from 0 to 255. Lena and Baboon are chosen as test images, and the histogram distributions of RGB three channels are illustrated in Figure 18 and Figure 19, respectively. It manifests that the original image has an uneven histogram distribution, while the histogram of the encrypted image obtained by our scheme becomes uniform.

Therefore, the attacker could not obtain the original image by analyzing the histogram distribution.

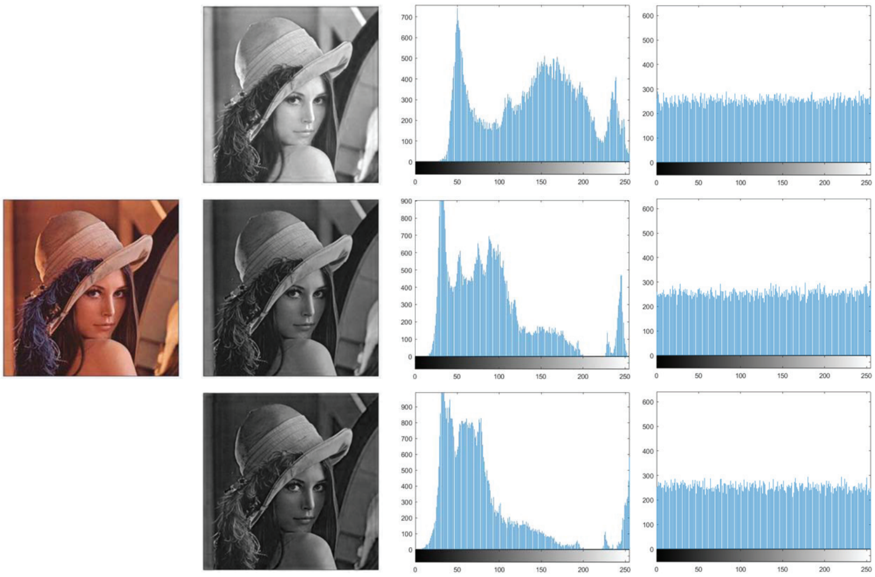


Figure 18. Histograms of Lena.

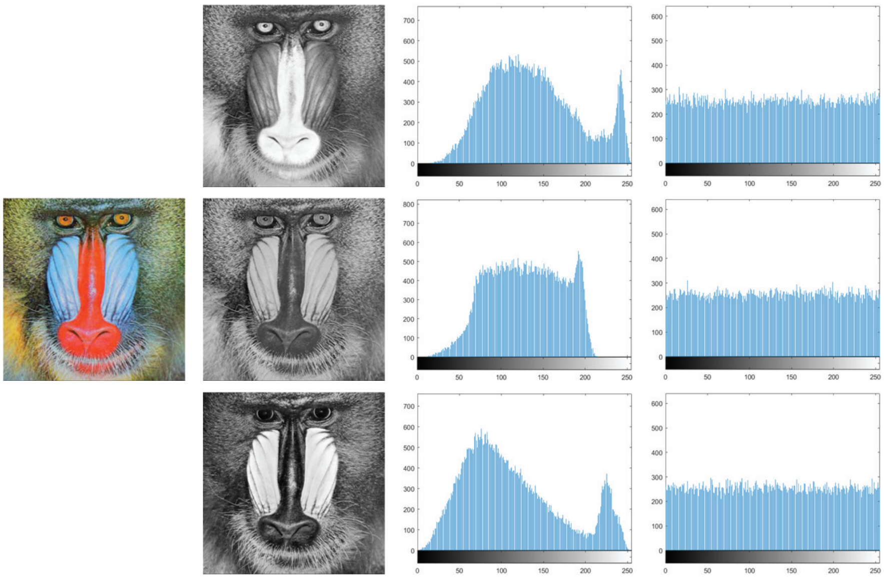


Figure 19. Histograms of Baboon.

The histogram variance [30] which can quantitatively measure the degree of change in pixel distribution is defined as follows:

$$HV = \frac{\sum_{i=0}^{255}\sum_{j=0}^{255}\frac{1}{2}\left(\gamma_i - \gamma_j\right)^2}{256^2} \tag{35}$$

where γ_i and γ_j are the number of pixels with grayscale values of i and j, respectively. Table 3 lists the computed variance values. Compared with the original images, the HV values of encrypted images are much lower, which is observed in Table 3. Hence, our image encryption method is resistant to statistical attacks based on histogram variance analysis.

Table 3. Results of HV values.

Image	Original			Encrypted		
	R	G	B	R	G	B
Lena	2.6138×10^4	6.4845×10^4	9.1647×10^4	238.2891	254.7422	261.3984
Baboon	2.8890×10^4	4.2994×10^4	2.6968×10^4	278.2109	241.6875	265.4297
Splash	1.5125×10^5	1.7515×10^5	3.9784×10^5	240.6875	266.0469	255.7109
House	4.8896×10^4	8.2361×10^4	6.2631×10^4	236.0391	228.6563	279.2969

5.3. Encryption Quality Analysis

(1) Uniform histogram deviation

Uniform histogram deviation (UHD) is commonly used to estimate image cryptosystem encryption quality [42]. UHD is calculated as follows:

$$UHD = \frac{\sum_{\delta=0}^{255}|O - O_\delta|}{M \times N} \tag{36}$$

where $M \times N$ is the size of the image. The histogram of the ciphertext image under index δ is represented by O_δ and O is a uniform histogram. A smaller UHD value indicates a higher encryption quality. The UHD values of the ciphertext images are compiled in Table 4. Apparently, the UHD values of four encrypted images are all close to 0. Therefore, our proposed scheme exhibits acceptable encryption quality.

(2) Irregular deviation

Irregular deviation (ID) is also frequently introduced to evaluate the quality of encrypted images [42].

$$ID = \sum_{\delta=0}^{255} \left| R_\delta - \overline{R} \right| \tag{37}$$

where R_δ refers to the absolute histogram difference between the initial image and its encrypted version, $\overline{R} = 1/256 \sum_{\delta=0}^{255} R_\delta$. The larger the ID value, the higher the quality of the encrypted image. The ID values in Table 4 are all sufficiently large, indicating that our scheme can produce high-quality encrypted images.

(3) Maximum deviation

The maximum deviation (MD) [42] is adopted for describing the extreme error between the original image and its ciphertext. MD can be expressed as shown below:

$$MD = max|P(i,j) - C(i,j)| \tag{38}$$

where $P(i,j)$ and $C(i,j)$ denote the pixel values in the original image and its corresponding encrypted one, respectively. As the MD value increases, the encryption quality also improves. From the results in Table 4, it can be seen that the MD values are very large. Therefore, the encryption quality of our scheme is acceptable.

Table 4. Results of UHD, ID, and MD values.

Encrypted Image		R	G	B
Lena	UHD	0.0508	0.0391	0.0859
	ID	19843	22798	32022
	MD	253	249	254
Baboon	UHD	0.0156	0.0547	0.0469
	ID	17562	11876	18396
	MD	250	233	249
Splash	UHD	0.0391	0.0547	0.0352
	ID	35399	40164	66062
	MD	240	255	240
House	UHD	0.0820	0.0742	0.0313
	ID	25663	27041	32412
	MD	233	243	246

5.4. Correlation Analysis

A good encryption technique should break the correlation between neighboring pixels [43]. In the suggested encryption scheme, the 3D Mobius scrambling transform possesses the capacity to weaken the correlation coefficient among adjacent pixels. The R channel of Lena is selected for testing, and 10,000 pairs of neighboring pixels are randomly chosen in all three directions. Figure 20 represents the correlation distribution results. Therein, the three subgraphs in the first row show the correlations of Lena horizontally, vertically, and diagonally, respectively, and those of the encrypted Lena are shown in the three subgraphs in the second row. The ciphertext image has a uniform pixel distribution, which demonstrates that the proposed encryption technique considerably decreases the correlation.

The data in Table 5 reflect the specific CC values. The CC values of encrypted images are minimized to be close to 0, meaning attackers cannot crack our algorithm relying on correlation analysis.

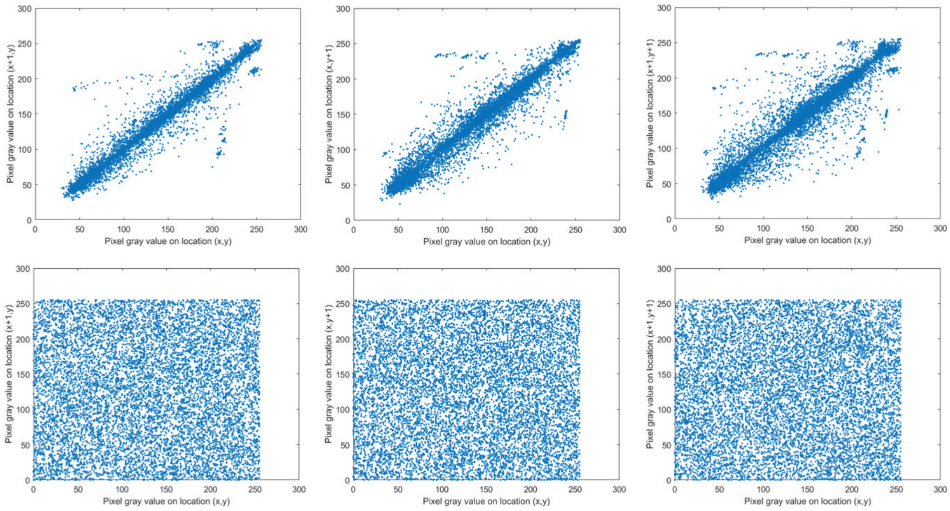


Figure 20. The correlation distributions.

Table 5. Results of CC values.

Image	Horizontal		Vertical		Diagonal	
	Original	Encrypted	Original	Encrypted	Original	Encrypted
Lena (R)	0.9718	0.0043	0.9668	−0.0026	0.9343	0.0017
Lena (G)	0.9644	0.0041	0.9534	0.0055	0.9139	0.0041
Lena (B)	0.9538	−0.0018	0.9490	−0.0025	0.9113	−0.0043
Baboon (R)	0.9270	−0.0031	0.9462	−0.0038	0.9117	0.0011
Baboon (G)	0.8450	−0.0036	0.8689	−0.0011	0.7952	0.0023
Baboon (B)	0.9113	0.0029	0.9207	0.0012	0.8709	0.0068
Splash (R)	0.9971	−0.0021	0.9861	0.0019	0.9857	−0.0051
Splash (G)	0.9805	0.0049	0.9690	0.0041	0.9516	0.0052
Splash (B)	0.9719	−0.0056	0.9675	−0.0036	0.9485	0.0012
House (R)	0.9354	0.0034	0.9369	−0.0040	0.8811	0.0033
House (G)	0.9300	0.0013	0.9164	−0.0019	0.8575	0.0018
House (B)	0.9586	0.0050	0.9608	0.0049	0.9138	0.0052

5.5. Information Entropy

A crucial metric for assessing the randomness of ciphertext images is information entropy. Mathematically, it is calculated as shown below:

$$IE = -\sum_{i=0}^{255} P(i)\log_2 P(i) \tag{39}$$

where $P(i)$ denotes the appearance frequency of gray value i. In general, the perfect IE value is 8. The utilization of 3D Mobius scrambling and XOR coding controlled by chaotic sequences can significantly improve the randomness of encrypted images. The precise IE values of original and encrypted images are provided in Table 6. From the results, the IE values of encrypted images are all approximate to 8. Therefore, our encryption method can effectively resist entropy attacks.

Table 6. Results of IE values.

Image	Original			Encrypted		
	R	G	B	R	G	B
Lena	7.6353	7.2778	7.0656	7.9974	7.9972	7.9971
Baboon	7.6058	7.3581	7.6665	7.9970	7.9973	7.9971
Splash	6.9417	6.9045	6.0601	7.9974	7.9971	7.9972
House	7.4025	7.2317	7.4280	7.9974	7.9975	7.9969

5.6. Spectrum Analysis

The Fourier spectrums of Lena are visualized in Figure 21, in which the three subgraphs in the first row show the spectral distributions of RGB channels of the original Lena, and those of encrypted Lena are displayed in the three subgraphs in the second row. It is evident that the spectrums of ciphertext images have a uniform distribution. In the meantime, the spectrum of each channel is similar to each other. Thus, our proposed encryption technique can stand up to spectrum attacks.

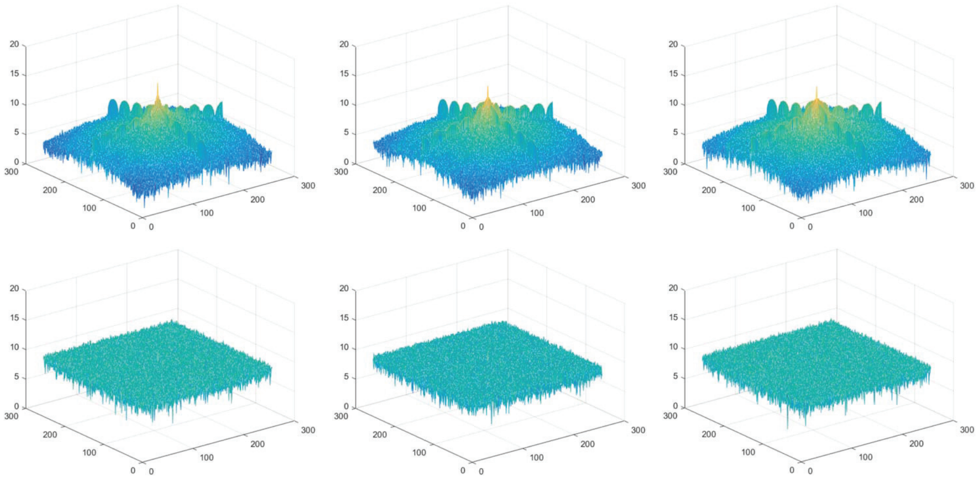


Figure 21. The spectrum distributions.

5.7. Key Sensitivity and Key Space

In this study, all of the scrambling and diffusion operations are controlled by sequences generated by the 3D hyper-chaotic Henon map. Two control parameters and two sets of initial values for this map, i.e., σ, ρ, u_0, v_0, w_0, and u'_0, v'_0, w'_0 are taken as encryption keys. Since the chaotic systems are particularly sensitive to the initial values, the presented cryptosystem achieves a strong key sensitivity. The Lena image is opted for testing the sensitivity of respective keys. Figure 22 gives the results decrypted by using keys with a subtle change.

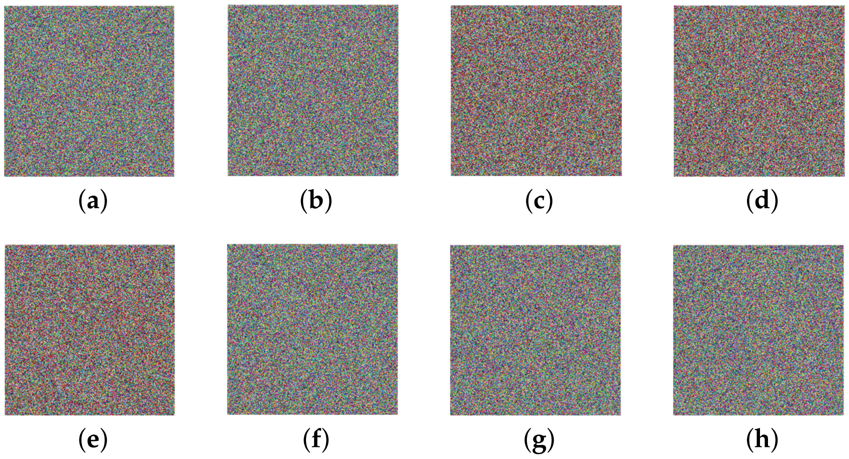


Figure 22. Decrypted images with incorrect keys: (**a**) $\sigma + 10^{-15}$. (**b**) $\rho + 10^{-18}$. (**c**) $u_0 + 10^{-15}$. (**d**) $v_0 + 10^{-15}$. (**e**) $w_0 + 10^{-12}$. (**f**) $u'_0 + 10^{-15}$. (**g**) $v'_0 + 10^{-15}$. (**h**) $w'_0 + 10^{-13}$.

Visibly, noise-like images would be obtained with incorrect keys. Therefore, the decrypted image is available only if all the keys are correct, which indicates this scheme is sensitive to the keys.

In accordance with the sensitivity experiments described above, the total key space is up to 10^{118}, which is about equal to 2^{392}. Therefore, the brute-force attack does not work on deciphering our encryption scheme.

5.8. Noise Attack and Cutting Attack

Suppose a ciphertext image is contaminated with noise:

$$E' = E + sG \tag{40}$$

where E and E' represent ciphertext images before and after contamination, respectively. G is Gaussian noise with zero mean and standard deviation, and s is the noise strength. The ciphertext image of Lena is used for testing, Figure 23 depicts the corresponding decrypted results when s takes the value of 0.25, 0.5, 0.75, and 1. The results indicate that our encryption algorithm is somewhat robust to noise attacks.

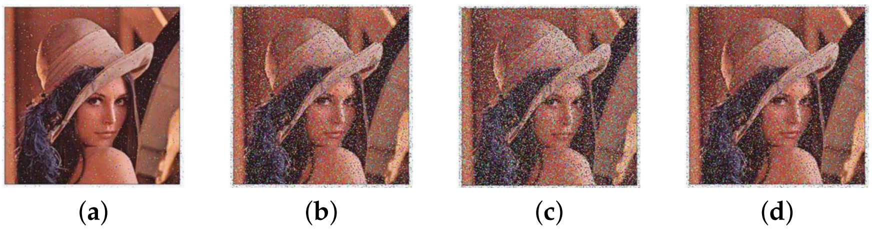


Figure 23. Decrypted images with various noise intensities: (**a**) 0.25. (**b**) 0.5. (**c**) 0.75. (**d**) 1.

To test the performance of our scheme to combat cutting attacks, regions of different sizes are cut from the encrypted Baboon. Figure 24 presents the corresponding decrypted versions. As can be seen, although some details are broken, the primary information is still available. The simulation results allow us to make clear that our proposed algorithm could resist cutting attacks to some degree.

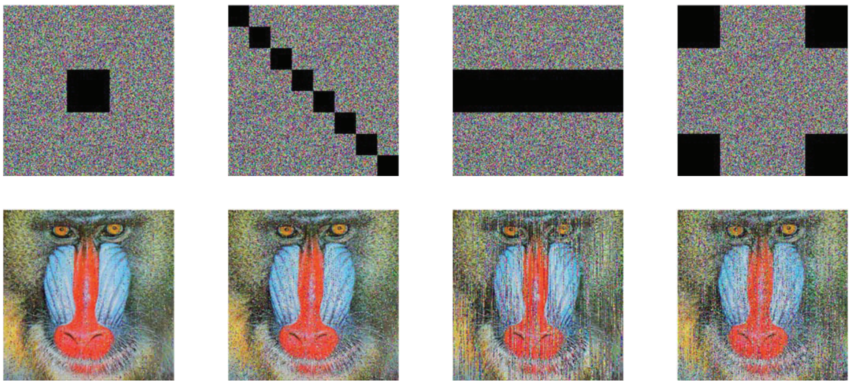


Figure 24. The cutting attack results.

5.9. Computational Complexity

The proposed quantum image encryption scheme's computational complexity is primarily related to the quantum 3D Mobius scrambling transform and quantum XOR operation. The quantum 3D Mobius scrambling transform is made up of basic quantum modules, including ADDER, D-ADDER, MULER, and COMOR. The complexity of each module can be reduced to $O(n)$, as stated by [36,38]. Therefore, the computational complexity of the quantum 3D Mobius scrambling transform is $O(n)$. In Figures 15 and 16, there are $(2n + 3)$ CNOT gates, one $(2n + 3)$-CNOT gate and three Toffoli gates. Since one t-CNOT gate can be decomposed into $2(t - 1)$ Toffoli gates and one CNOT gate, one Toffoli gate can be realized by six CNOT gates [44]. Thus, the quantum XOR operation involves $(26n + 46)$ CNOT gates. Consequently, the whole computational complexity of our proposed encryption scheme is $O(n)$. While in the similar classical image encryption algorithm, all operations are performed on each pixel, so that the complexity is up to $O(2^{2n})$. It is clear that the proposed quantum image encryption scheme has lower computational complexity than its classical counterparts.

5.10. Performance Comparison

This subsection compares our encryption scheme with some latest quantum image encryption algorithms [29,40,45,46]. The comparison contents include the key space, histogram variance, correlation coefficient, and information entropy. Tables 7–10 summarize the comparison results.

Table 7. Key space comparison.

Algorithm	Ours	Ref. [29]	Ref. [40]	Ref. [45]	Ref. [46]
Key space	$10^{118} \approx 2^{392}$	10^{83}	2^{177}	10^{112}	10^{60}

Table 8. Histogram variance comparison.

Image	Red	Green	Blue
Baboon (512 × 512)	4.8324×10^5	7.0917×10^5	4.5314×10^5
Enc-Baboon	931.3	907.2	1175.6
Ref. [29]	1333.1		
Ref. [45]	1130.8		
Splash (512 × 512)	2.4061×10^6	2.7794×10^6	6.3912×10^6
Enc-Splash	1038.7	1048.6	1049.4
Ref. [29]	1164.3		
Peppers (512 × 512)	9.1085×10^5	7.6877×10^5	1.6001×10^6
Enc-Peppers	1142.2	1031.8	950.3
Ref. [45]	4155.3		
Lena (256 × 256)	2.6138×10^4	6.4845×10^4	9.1647×10^4
Enc-Lena	238.3	254.7	261.4
Ref. [40]	242.8	262.1	284.9
Ref. [45]	273.3		

Table 9. Correlation coefficient comparison.

Image	Horizontal	Vertical	Diagonal
Enc-Peppers (R)	0.0044	−0.0033	0.0026
Enc-Peppers (G)	0.0021	−0.0002	0.0036
Enc-Peppers (B)	0.0048	0.0022	−0.0019
Ref. [29]	−0.0067	−0.0038	0.0063
Ref. [46]	−0.0036	−0.0539	0.0455
Enc-Lena (R)	0.0043	−0.0026	0.0017
Enc-Lena (G)	0.0041	0.0055	0.0041
Enc-Lena (B)	−0.0018	−0.0025	−0.0043
Ref. [40] (R)	0.0029	−0.0033	0.0019
Ref. [40] (G)	−0.0025	−0.0059	0.0013
Ref. [40] (B)	−0.0063	0.0046	−0.0036
Ref. [45] (R)	−0.0006	−0.0049	0.0070
Ref. [45] (G)	0.0025	−0.0051	0.0020
Ref. [45] (B)	0.0046	0.0019	0.0047

Table 10. Information entropy comparison.

Image	Red	Green	Blue
Enc-Baboon	7.9970	7.9973	7.9971
Ref. [29]	7.9991		
Ref. [40]	7.9993	7.9993	7.9993
Ref. [45]	7.9972	7.9969	7.9971
Enc-Peppers	7.9972	7.9972	7.9968
Ref. [45]	7.9970	7.9965	7.9962
Ref. [46]	7.9973		

In Table 7, the key space of our scheme is much larger than those of [29,40,45,46] and greatly exceeds the minimal limit of 2^{100}. Thus, our proposed scheme has a significant advantage. It is hard for attackers to decipher the encrypted images by brute-force attack unless they have entirely correct keys. As can be observed from Table 8, the histogram variance values of the encrypted images generated with our proposed scheme are smaller than those in [29,40,45], which illustrates the superior performance of our image encryption scheme. Table 9 presents the comparison concerning the correlation coefficient. Obviously, the correlation coefficients of the encrypted images yielded by our proposed scheme reach 0 more tightly than those in [29,46], and they are close to the values in [40,45], which implies that our encryption operations greatly weaken the correlation among adjacent pixels. From Table 10, the information entropies with our encryption scheme are near to the values in [45,46], while they are smaller than the values in [29,40]. Nonetheless, the information entropy values obtained using our scheme are already very approximate to the ideal value of 8 bits. Hence, the proposed image encryption scheme can effectively thwart the information entropy attack. Overall, the above performance comparisons confirm the effectiveness and merits of the proposed quantum image encryption scheme.

6. Conclusions

In this paper, a quantum image-scrambling algorithm based on the 3D Mobius transform is investigated and its quantum realization circuit is developed, which changes not only the position of pixels but also the gray values. After that, by combining 3D Mobius scrambling with a 3D hyper-chaotic Henon map, an encryption scheme for a QRCI quantum image is proposed. In the permutation stage, the 3D Mobius transform is adopted to scramble bit-planes and pixel positions. In the diffusion stage, the 3D hyper-chaotic Henon map is employed to further improve the scheme's performance, and the generated hyper-chaotic sequences are utilized to control quantum XOR operations. The 3D Mobius transform has more parameters such as the shift counts for folding along different axes than the Arnold/Fibonacci transform. The introduction of a 3D hyper-chaotic Henon map improves our encryption scheme greatly in terms of randomness and unpredictability. This ensures our scheme has good security. Additionally, the entire image encryption process could be implemented in quantum computers, thereby breaking the limitations of classical computers. Simulation results and comparative analysis show the validity and reliability of our proposed encryption scheme. In the future, we hope to define a scrambling operation with better results than the 3D Mobius transform and apply it to quantum image encryption.

Author Contributions: Conceptualization, L.W.; methodology, L.W. and Q.R.; software, L.W.; validation, Q.R. and J.D.; formal analysis, J.D.; data curation, L.W.; writing—original draft preparation, L.W.; writing—review and editing, Q.R. and J.D.; visualization, L.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data are contained within the article.

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

References

1. Deutsch, D. Quantum theory, the Church–Turing principle and the universal quantum computer. *Proc. R. Soc. London. Math. Phys. Sci.* **1985**, *400*, 97–117.
2. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145. [CrossRef]
3. Flamini, F.; Spagnolo, N.; Sciarrino, F. Photonic quantum information processing: A review. *Rep. Prog. Phys.* **2018**, *82*, 016001. [CrossRef] [PubMed]
4. Wendin, G. Quantum information processing with superconducting circuits: A review. *Rep. Prog. Phys.* **2017**, *80*, 106001. [CrossRef]
5. Zhou, N.R.; Tong, L.J.; Zou, W.P. Multi-image encryption scheme with quaternion discrete fractional Tchebyshev moment transform and cross-coupling operation. *Signal Process.* **2023**, *211*, 109107. [CrossRef]
6. Gong, L.H.; Luo, H.X. Dual color images watermarking scheme with geometric correction based on quaternion FrOOFMMs and LS-SVR. *Opt. Laser Technol.* **2023**, *167*, 109665. [CrossRef]
7. Ruan, Y.; Xue, X.; Shen, Y. Quantum image processing: Opportunities and challenges. *Math. Probl. Eng.* **2021**, *2021*, 1–8. [CrossRef]
8. Yan, F.; Iliyasu, A.M.; Venegas-Andraca, S.E. A survey of quantum image representations. *Quantum Inf. Process.* **2016**, *15*, 1–35. [CrossRef]
9. Venegas-Andraca, S.E.; Bose, S. Storing, processing, and retrieving an image using quantum mechanics. In Proceedings of the Quantum Information and Computation. SPIE, Orlando, FL, USA, 21–22 April 2003; Volume 5105, pp. 137–147.
10. Latorre, J.I. Image compression and entanglement. *arXiv* **2005**, arXiv:quant-ph/0510031.
11. Le, P.Q.; Dong, F.; Hirota, K. A flexible representation of quantum images for polynomial preparation, image compression, and processing operations. *Quantum Inf. Process.* **2011**, *10*, 63–84. [CrossRef]
12. Zhang, Y.; Lu, K.; Gao, Y.; Wang, M. NEQR: A novel enhanced quantum representation of digital images. *Quantum Inf. Process.* **2013**, *12*, 2833–2860. [CrossRef]
13. Zhang, Y.; Lu, K.; Gao, Y.; Xu, K. A novel quantum representation for log-polar images. *Quantum Inf. Process.* **2013**, *12*, 3103–3126. [CrossRef]
14. Li, H.S.; Zhu, Q.; Zhou, R.G.; Song, L.; Yang, X.j. Multi-dimensional color image storage and retrieval for a normal arbitrary quantum superposition state. *Quantum Inf. Process.* **2014**, *13*, 991–1011. [CrossRef]
15. Sang, J.; Wang, S.; Li, Q. A novel quantum representation of color digital images. *Quantum Inf. Process.* **2017**, *16*, 42. [CrossRef]
16. Li, H.S.; Fan, P.; Xia, H.Y.; Peng, H.; Song, S. Quantum implementation circuits of quantum signal representation and type conversion. *IEEE Trans. Circuits Syst. Regul. Pap.* **2018**, *66*, 341–354. [CrossRef]
17. Grigoryan, A.M.; Agaian, S.S. New look on quantum representation of images: Fourier transform representation. *Quantum Inf. Process.* **2020**, *19*, 148. [CrossRef]
18. 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*, 5. [CrossRef]
19. Wang, L.; Ran, Q.; Ma, J.; Yu, S.; Tan, L. QRCI: A new quantum representation model of color digital images. *Opt. Commun.* **2019**, *438*, 147–158. [CrossRef]
20. Zhou, R.G.; Wu, Q.; Zhang, M.Q.; Shen, C.Y. Quantum image encryption and decryption algorithms based on quantum image geometric transformations. *Int. J. Theor. Phys.* **2013**, *52*, 1802–1817. [CrossRef]
21. Song, X.H.; Wang, S.; Abd El-Latif, A.A.; Niu, X.M. Quantum image encryption based on restricted geometric and color transformations. *Quantum Inf. Process.* **2014**, *13*, 1765–1787. [CrossRef]
22. 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]
23. Zhou, N.; Hu, Y.; Gong, L.; Li, G. Quantum image encryption scheme with iterative generalized Arnold transforms and quantum image cycle shift operations. *Quantum Inf. Process.* **2017**, *16*, 164. [CrossRef]
24. Gong, L.H.; He, X.T.; Cheng, S.; Hua, T.X.; Zhou, N.R. Quantum image encryption algorithm based on quantum image XOR operations. *Int. J. Theor. Phys.* **2016**, *55*, 3234–3250. [CrossRef]
25. 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]
26. Li, H.S.; Li, C.; Chen, X.; Xia, H. Quantum image encryption based on phase-shift transform and quantum Haar wavelet packet transform. *Mod. Phys. Lett.* **2019**, *34*, 1950214. [CrossRef]
27. Liu, X.; Xiao, D.; Liu, C. Quantum image encryption algorithm based on bit-plane permutation and sine logistic map. *Quantum Inf. Process.* **2020**, *19*, 239. [CrossRef]
28. Zhang, J.; Huang, Z.; Li, X.; Wu, M.; Wang, X.; Dong, Y. Quantum image encryption based on quantum image decomposition. *Int. J. Theor. Phys.* **2021**, *60*, 2930–2942. [CrossRef]
29. 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. [CrossRef]

30. Liu, X.; Liu, C. Quantum image encryption scheme using independent bit-plane permutation and Baker map. *Quantum Inf. Process.* **2023**, *22*, 262. [CrossRef]
31. Gao, J.; Wang, Y.; Song, Z.; Wang, S. Quantum Image Encryption Based on Quantum DNA Codec and Pixel-Level Scrambling. *Entropy* **2023**, *25*, 865. [CrossRef]
32. Jiang, N.; Wu, W.Y.; Wang, L. The quantum realization of Arnold and Fibonacci image scrambling. *Quantum Inf. Process.* **2014**, *13*, 1223–1236. [CrossRef]
33. Jiang, N.; Wang, L.; Wu, W.Y. Quantum Hilbert image scrambling. *Int. J. Theor. Phys.* **2014**, *53*, 2463–2484. [CrossRef]
34. Hou, C.; Liu, X.; Feng, S. Quantum image scrambling algorithm based on discrete Baker map. *Mod. Phys. Lett. A* **2020**, *35*, 2050145. [CrossRef]
35. Vedral, V.; Barenco, A.; Ekert, A. Quantum networks for elementary arithmetic operations. *Phys. Rev. A* **1996**, *54*, 147. [CrossRef]
36. Lu, X.; Jiang, N.; Hu, H.; Ji, Z. Quantum adder for superposition states. *Int. J. Theor. Phys.* **2018**, *57*, 2575–2584. [CrossRef]
37. Kotiyal, S.; Thapliyal, H.; Ranganathan, N. Circuit for reversible quantum multiplier based on binary tree optimizing ancilla and garbage bits. In Proceedings of the 2014 27th International Conference on VLSI Design and 2014 13th International Conference on Embedded Systems, Mumbai, India, 5–9 January 2014; pp. 545–550.
38. Li, H.S.; Fan, P.; Xia, H.; Peng, H.; Long, G.L. Efficient quantum arithmetic operation circuits for quantum image processing. *Sci. China Phys. Mech. Astron.* **2020**, *63*, 280311. [CrossRef]
39. Anandkumar, R.; Kalpana, R. Designing a fast image encryption scheme using fractal function and 3D Henon map. *J. Inf. Secur. Appl.* **2019**, *49*, 102390. [CrossRef]
40. Wang, L.; Ran, Q.; Ding, J. Quantum Color Image Encryption Scheme Based on 3D Non-Equilateral Arnold Transform and 3D Logistic Chaotic Map. *Int. J. Theor. Phys.* **2023**, *62*, 36. [CrossRef]
41. Wang, L.; Ran, Q.; Ma, J. Double quantum color images encryption scheme based on DQRCI. *Multimed. Tools Appl.* **2020**, *79*, 6661–6687. [CrossRef]
42. Zhou, N.R.; Hu, L.L.; Huang, Z.W.; Wang, M.M.; Luo, G.S. Novel multiple color images encryption and decryption scheme based on a bit-level extension algorithm. *Expert Syst. Appl.* **2024**, *238*, 122052. [CrossRef]
43. Ran, Q.; Wang, L.; Ma, J.; Tan, L.; Yu, S. A quantum color image encryption scheme based on coupled hyper-chaotic Lorenz system with three impulse injections. *Quantum Inf. Process.* **2018**, *17*, 1–30. [CrossRef]
44. Wang, J.; Geng, Y.C.; Han, L.; Liu, J.Q. Quantum image encryption algorithm based on quantum key image. *Int. J. Theor. Phys.* **2019**, *58*, 308–322. [CrossRef]
45. Wang, X.; Su, Y.; Luo, C.; Nian, F.; Teng, L. Color image encryption algorithm based on hyperchaotic system and improved quantum revolving gate. *Multimed. Tools Appl.* **2022**, *81*, 13845–13865. [CrossRef]
46. Liu, X. Quantum image encryption based on Baker map and DNA circular shift operation. *Phys. Scr.* **2023**, *98*, 115112. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.