


Article

Double Quantum Image Encryption Based on Arnold Transform and Qubit Random Rotation

Xingbin Liu ^{1,*} , Di Xiao ¹ and Cong Liu ²¹ College of Computer Science, Chongqing University, Chongqing 400044, China; dixiao@cqu.edu.cn² Southwest Technology and Engineering Research Institute, Chongqing 40039, China; 3120130321@bit.edu.cn

* Correspondence: xbliu@cqu.edu.cn

Received: 8 October 2018; Accepted: 8 November 2018; Published: 10 November 2018



Abstract: Quantum image encryption offers major advantages over its classical counterpart in terms of key space, computational complexity, and so on. A novel double quantum image encryption approach based on quantum Arnold transform (QAT) and qubit random rotation is proposed in this paper, in which QAT is used to scramble pixel positions and the gray information is changed by utilizing random qubit rotation. Actually, the independent random qubit rotation operates once, respectively, in spatial and frequency domains with the help of quantum Fourier transform (QFT). The encryption process accomplishes pixel confusion and diffusion, and finally the noise-like cipher image is obtained. Numerical simulation and theoretical analysis verify that the method is valid and it shows superior performance in security and computational complexity.

Keywords: information security; Arnold transform; quantum image encryption; quantum Fourier transform; quantum image representation

1. Introduction

Quantum computation has shown great potential for improving information processing speed and enhancing communication security [1–3]. The quantum image encryption technology exploits quantum mechanics principles, such as parallel and entanglement, to further protect the security of information transmission and decrease computational resource [4–7].

Due to the promising prospect of quantum image encryption, various kinds of algorithms are gradually proposed [8–13]. Among the existing algorithms, most of them are designed in spatial domain. For example, Zhou proposed a quantum image encryption algorithm using three geometric transformations, including image translation, image mirror transformation, and image sub-block swapping, which changes pixel position to some extent [14]. However, this method relies solely on geometric transformation, which leads to the increase of correlation of adjacent pixels and therefore the encryption performance is seriously affected. Except using geometric transformation to scramble pixel positions, Song proposed a novel quantum image encryption method by introducing additional color transformations, which realized pixel values diffusion and obtained better encryption results [15]. Moreover, Zhou introduced hyper-chaotic system to encrypt quantum image through XOR operation implemented with control-NOT gate [16]. Li proposed a simple color image encryption method by using 24 qubits to represent color information and employing controlled rotation gates to transform the basic state into balanced superposition state, which makes the encrypted image like a uniform white noise [17].

The quantum version of classical frequency transform tools, such as quantum Fourier transform (QFT) [18], quantum wavelet transform (QWT) [19], quantum discrete cosine transform (QDCT) [20], and promote the development of quantum image processing algorithm in frequency domain [21,22]. These quantum transforms mentioned above have lower computational complexity than their classical

counterpart. Utilizing these quantum transform tools, some efficient quantum image encryption methods are investigated. Yang proposed novel quantum image encryption algorithms based on double random phase encoding framework [23], where the QFT substitutes the Fourier transform and the encryption performance of which surpasses its classical counterparts in terms of statistical analyses, robustness, and computational complexity. After that, Yang extended the quantum double random phase encoding scheme to encrypt color image [24], which introduces color image encryption into quantum scenarios in frequency domain. Recently, Li proposed a quantum encryption and compression scheme based on QDCT and a five-dimensional hyper-chaotic system [25].

Whether the quantum image encryption algorithms devised in spatial domain or frequency domain, image scrambling operation plays an important role. Jiang investigated quantum Arnold transform and Fibonacci transform method, where the quantum circuits are given and computational complexity is analyzed [26,27]. The chaos theory is also widely used in image encryption schemes [28–32]. Diaconu proposed a chaos based image encryption scheme by employing the circular inter-intra permutation strategy [33]. Stoyanov presented a Chebyshev polynomial based image encryption scheme, which shows the advantage in terms of key space [34]. Parvees utilized logistic map and key image to efficiently encrypt large size image [35]. Soon afterwards, Zhou suggested the generalized Arnold transform with feature of chaotic mapping [36,37]. In addition, a generalized quantum affine transform is proposed to scramble images, which can encode pixel positions effectively [38]. Quantum Hilbert scrambling method is also introduced and achieves good permutation effect [39]. These scrambling methods adopt position space scrambling strategies, which do not change color space. To overcome this defect, Zhou proposed a bit-plane scrambling method that is based on Gray-code [40], which simultaneously changes the pixel positions and pixel values, and it even can be used directly to encrypt images. By combining the bit-plane scrambling method and the Hilbert scrambling method, Naseri proposed a quantum gray-scale image encoding scheme, where a randomly generated binary key is used to select encoding scheme [41].

The existing quantum image encryption algorithms mainly focus on single gray or color image, while the research on double quantum image encryption or multiple quantum image encryption is still scarce. In view of this, a double quantum image encryption algorithm that is based on quantum Arnold transform (QAT) and qubit random rotation is proposed. Firstly, the two images to be encrypted are represented through a flexible quantum image representation model called flexible representation for quantum images (FRQI). Next, the two quantum states are scrambled using QAT with different parameters, and one of the scrambled quantum images is encoded into amplitude part and another is encoded into phase part. Then the independent random qubit rotation operates once, respectively, in spatial and frequency domains with the help of quantum Fourier transform (QFT) to accomplish pixel confusion and diffusion. The noise-like cipher image can be finally obtained by performing inverse QFT. The original images can be exactly recovered without cross-talk. The quantum parallel computation speeds up the process of double image encryption and decryption. Numerical simulation results and theoretical analyses demonstrate that the proposed algorithm is effective and the computational complexity is decreased.

2. Preliminary Knowledge

2.1. FRQI Representation Model

The first step of quantum image processing is to design a suitable representation model, which can be run on quantum computers for compiling digital image. Nowadays, several efficient representation models are proposed [3]. The FRQI representation model [42] is widely used, as it is similar with pixel representation in classical computer and accord with human perception of vision.

The FRQI representation model stores gray and geometric information using a normalized quantum state. For a gray image M of size $2^n \times 2^n$, the representation can be expressed, as follows,

$$|M(\theta)\rangle = \frac{1}{2^n} \sum_{i=0}^{2^{2n}-1} |c_i\rangle \otimes |i\rangle, \quad i = 0, 1, 2, \dots, 2^{2n} - 1 \tag{1}$$

$$|c_i\rangle = \cos \theta_i |0\rangle + \sin \theta_i |1\rangle, \quad \theta_i \in [0, \pi/2] \tag{2}$$

where $\theta = (\theta_1, \theta_2, \dots, \theta_{2^{2n}-1})$ is the vector used to encode phase information of gray values and $|i\rangle = |y\rangle|x\rangle = |y_{n-1}y_{n-2} \dots y_0\rangle|x_{n-1}x_{n-2} \dots x_0\rangle$ is used to encode corresponding pixel positions of θ . The symbol \otimes denotes tensor product. There are only $2n + 1$ qubits required when encoding image and the computational complexity of preparation process is $O(2^{4n})$.

2.2. Quantum Arnold Transform (QAT)

The Arnold transform, used as method for image pixel scrambling, is built on the research of ergodic theory and it was extended to quantum image processing in 2014 by Jiang et al. [26]. QAT aims to transform the image into a confused form through changing the coordinates of pixels.

Suppose that the image of size $2^n \times 2^n$ to be scrambled is denoted as $I(x, y)$, where (x, y) represent pixel positions. A two-dimensional Arnold transform is described, as follows,

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod{2^n}, \quad x, y = 0, 1, \dots, 2^n \tag{3}$$

i.e.,

$$\begin{cases} x' = (x + y) \pmod{2^n} \\ y' = (x + 2y) \pmod{2^n} \end{cases} \tag{4}$$

The output (x', y') is the scrambled position information and the inverse transform can be deduced as follows,

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}^{-1} \begin{pmatrix} x' \\ y' \end{pmatrix} \pmod{2^n} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \pmod{2^n} \tag{5}$$

The scrambling period of Arnold transform is associated with the size of image, and some determined values for particular cases are given in Table 1. Although the period of Arnold transform cannot be accurately computed, it can be seen that the period grows with the increase of image size. The quantum circuits shown in Figure 1 are used to accomplish the QAT scrambling. The detailed information of quantum adder module and adder-mod 2^n module is presented in [27].

Table 1. The scrambling period of Arnold transform.

Image Size	Period
16 × 16	12
32 × 32	24
64 × 64	48
128 × 128	96
256 × 256	192

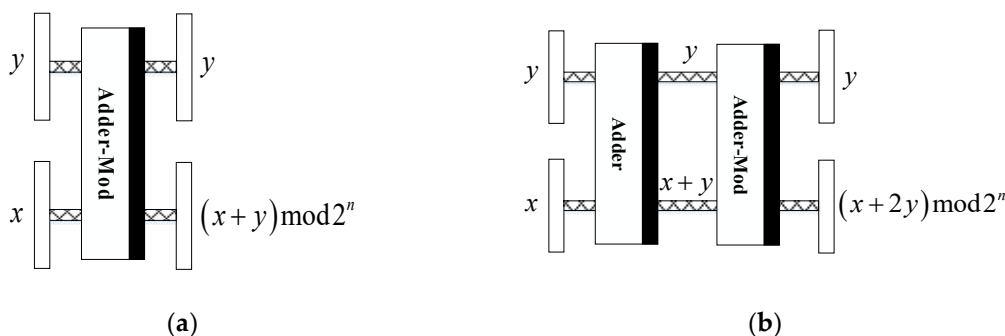


Figure 1. The scrambling circuits for (a) x' and (b) y' .

3. Proposed Double Quantum Image Encryption Scheme

In this section, the proposed double quantum image encryption scheme based on QAT and qubit random rotation is illustrated in detail. Let the two images to be encrypted be respectively denoted as I_1 and I_2 . According to the FRQI representation model, the original images can be represented as follows,

$$\begin{aligned}
 |I_1(\theta)\rangle &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |\alpha_{yx}\rangle \otimes |yx\rangle \\
 |I_2(\omega)\rangle &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |\beta_{yx}\rangle \otimes |yx\rangle
 \end{aligned}
 \tag{6}$$

where the gray values are represented as $|\alpha_{yx}\rangle = \cos \theta_{yx}|0\rangle + \sin \theta_{yx}|1\rangle$, $|\beta_{yx}\rangle = \cos \omega_{yx}|0\rangle + \sin \omega_{yx}|1\rangle$, and $\{\theta_{yx}, \omega_{yx}\} \in [0, \pi/2]$. The whole double quantum image encryption algorithm consists the following five steps.

Step 1. Scramble the two original images $|I_1\rangle$ and $|I_2\rangle$ in spatial domain using QAT to get $|I'_1\rangle$ and $|I'_2\rangle$. The parameters of QAT corresponding to $|I_1\rangle$ and $|I_2\rangle$ are respectively denoted as p_1 and p_2 , which represent the iteration times of scrambling.

$$\begin{aligned}
 |I'_1\rangle &= \text{QAT}_{p_1}(|I_1\rangle) = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |\alpha_{yx}\rangle \otimes \text{QAT}_{p_1}(|yx\rangle) \\
 &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |\alpha_{yx}\rangle \otimes (|y'x'\rangle)
 \end{aligned}
 \tag{7}$$

$$\begin{aligned}
 |I'_2\rangle &= \text{QAT}_{p_2}(|I_2\rangle) = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |\beta_{yx}\rangle \otimes \text{QAT}_{p_2}(|yx\rangle) \\
 &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |\beta_{yx}\rangle \otimes (|y'x'\rangle)
 \end{aligned}
 \tag{8}$$

where $\text{QAT}(|yx\rangle) = |(x+2y) \bmod 2^n|(x+y) \bmod 2^n$. There are a total of p_1 times scrambling operations for quantum image $|I_1\rangle$ and p_2 times for $|I_2\rangle$.

Step 2. Encode the scrambled image $|I'_2\rangle$ into a phase function and the scrambled image $|I'_1\rangle$ is regarded as amplitude. Then, a new complex image $|I'\rangle$ involving all the information of the two original images can be expressed, as follows,

$$\begin{aligned}
 |I'\rangle &= |I'_1\rangle \exp(i\pi |I'_2\rangle) \\
 &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |\alpha_{yx}\rangle \exp(i\pi |\beta_{yx}\rangle) \otimes |y'x'\rangle
 \end{aligned}
 \tag{9}$$

Step 3. Perform qubit random rotation on quantum image $|I'\rangle$ to transform its each gray value angle into a new angle. The rotation matrix $R_{yx}(\phi_{yx})$ defined as follows is used to change angles in spatial domain,

$$R_{yx}(\phi_{yx}) = \begin{bmatrix} \cos \phi_{yx} & -\sin \phi_{yx} \\ \sin \phi_{yx} & \cos \phi_{yx} \end{bmatrix} \quad (10)$$

where ϕ_{yx} is uniformly distributed in the interval $[0, 2\pi]$. The controlled rotation matrix $CR_{YX}(\phi_{YX})$ defined as follows is used to change angles in position (Y, X) ,

$$CR_{YX}(\phi_{YX}) = \mathbf{I} \otimes \sum_{y=0}^{2^n-1} \sum_{\substack{x=0 \\ yx \neq YX}}^{2^n-1} |yx\rangle\langle yx| + R_{YX}(\phi_{YX}) \otimes |YX\rangle\langle YX| \quad (11)$$

The controlled rotation matrix $CR_{YX}(\phi_{YX})$ is a unitary matrix because of $CR_{YX}CR_{YX}^\dagger = \mathbf{I}^{\otimes 2n+1}$. The CR_{YX}^\dagger represents the Hermitian conjugate of CR_{YX} and the symbol \mathbf{I} denotes unit matrix.

In order to complete the rotation of all positions, the products of 2^{2n} controlled rotation matrices are applied on quantum image $|I'\rangle$ and obtain $|E_1\rangle$.

$$\begin{aligned} CR(|I'\rangle) &= \prod_{Y=0}^{2^n-1} \prod_{X=0}^{2^n-1} CR_{YX}(|I'\rangle) \\ &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} R_{yx}(|\alpha_{yx}\rangle \exp(i\pi|\beta_{yx}\rangle)) \otimes |y'x'\rangle \\ &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |f_{yx}\rangle \otimes |y'x'\rangle \\ &= |E_1\rangle \end{aligned} \quad (12)$$

Step 4. Transform the obtained $|E_1\rangle$ into frequency domain using QFT. The QFT is the identical transform of discrete Fourier transform, which is defined as follows,

$$\text{QFT}(|i\rangle) = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi ijk/N} |j\rangle \quad (13)$$

Similar to the rotation in spatial domain, qubit random rotation is employed in the frequency domain. Another rotation matrix $T_{yx}(\psi_{yx})$ defined as follows is used,

$$T_{yx}(\psi_{yx}) = \begin{bmatrix} \cos \psi_{yx} & -\sin \psi_{yx} \\ \sin \psi_{yx} & \cos \psi_{yx} \end{bmatrix} \quad (14)$$

where ψ_{yx} is also uniformly distributed in the interval $[0, 2\pi]$. The controlled rotation matrix $CT_{YX}(\psi_{YX})$ is defined, as follows,

$$CT_{YX}(\psi_{YX}) = \mathbf{I} \otimes \sum_{y=0}^{2^n-1} \sum_{\substack{x=0 \\ yx \neq YX}}^{2^n-1} |yx\rangle\langle yx| + T_{YX}(\psi_{YX}) \otimes |YX\rangle\langle YX| \quad (15)$$

The controlled rotation matrix $CT_{YX}(\psi_{YX})$ is also a unit matrix and $CT_{YX}CT_{YX}^\dagger = \mathbf{I}^{\otimes 2n+1}$.

The rotation of frequency domain can be accomplished using the product of 2^{2n} controlled rotation matrices operate on quantum image $|E_1\rangle$ and obtain $|E_2\rangle$.

$$\begin{aligned}
 CT(QFT(|E_1\rangle)) &= \prod_{Y=0}^{2^n-1} \prod_{X=0}^{2^n-1} CT_{YX}(QFT(|E_1\rangle)) \\
 &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} (QFT(|\alpha_{yx}\rangle \exp(i\pi|\beta_{yx}\rangle))) \otimes |y'x'\rangle \\
 &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} T_{yx}(QFT(|f_{yx}\rangle)) \otimes |y'x'\rangle \\
 &= |E_2\rangle
 \end{aligned}
 \tag{16}$$

Step 5. Execute the inverse quantum Fourier transform (iQFT) and the final encrypted quantum image $|E\rangle$ is obtained.

$$\begin{aligned}
 |E\rangle &= iQFT(|E_2\rangle) \\
 &= \frac{1}{2^n} iQFT \left(\sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} T_{yx}(QFT(R_{yx}(|\alpha_{yx}\rangle \exp(i\pi|\beta_{yx}\rangle))) \otimes |y'x'\rangle) \right)
 \end{aligned}
 \tag{17}$$

The decryption scheme is just the inverse of the aforementioned encryption scheme as the quantum transformations used are unitary and invertible. The keys including parameters of QAT p_1 and p_2 , two rotation matrices $R(\phi)$ and $T(\psi)$ are needed to correctly decrypt the cipher image. Corresponding to the encryption procedure, the decryption process can be expressed, as follows.

Step 1. Perform QFT on the encrypted quantum image $|E\rangle$ and obtain $|E_2\rangle$,

$$QFT(|E\rangle) = QFT(iQFT(|E_2\rangle)) = |E_2\rangle
 \tag{18}$$

Step 2. Execute quantum rotation on $|E_2\rangle$ using the key $T(\psi)$.

$$\begin{aligned}
 CT^{-1}(|E_2\rangle) &= \prod_{Y=0}^{2^n-1} \prod_{X=0}^{2^n-1} CT_{YX}^\dagger(|E_2\rangle) \\
 &= \prod_{Y=0}^{2^n-1} \prod_{X=0}^{2^n-1} CT_{YX}^\dagger \left(\frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} T_{yx}(QFT(|f_{yx}\rangle)) \otimes |y'x'\rangle \right) \\
 &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} T_{yx}^{-1} T_{yx}(QFT(|f_{yx}\rangle)) \otimes |y'x'\rangle \\
 &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} QFT(|f_{yx}\rangle) \otimes |y'x'\rangle \\
 &= QFT(|E_1\rangle)
 \end{aligned}
 \tag{19}$$

Step 3. Apply iQFT on the result that was obtained in previous step and $|E_1\rangle$ is attained. Then, the qubit rotation is operated on $|E_1\rangle$ with the key $R_{yx}(\phi_{yx})$. This step can be expressed as follows,

$$iQFT(QFT(|E_1\rangle)) = |E_1\rangle
 \tag{20}$$

$$\begin{aligned}
 CR^{-1}(|E_1\rangle) &= \prod_{Y=0}^{2^n-1} \prod_{X=0}^{2^n-1} CR_{YX}^\dagger(|E_1\rangle) \\
 &= \prod_{Y=0}^{2^n-1} \prod_{X=0}^{2^n-1} CR_{YX}^\dagger \left(\frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} R_{yx}(|f_{yx}\rangle) \otimes |y'x'\rangle \right) \\
 &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} R_{yx}^{-1} R_{yx}(|f_{yx}\rangle) \otimes |y'x'\rangle \\
 &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |f_{yx}\rangle \otimes |y'x'\rangle \\
 &= |I'\rangle
 \end{aligned}
 \tag{21}$$

Step 4. Extract two quantum images $|I'_1\rangle$ and $|I'_2\rangle$ from $|I'\rangle$,

$$\begin{cases} |I'_1\rangle = \text{abs}(|I'\rangle) \\ |I'_2\rangle = \text{angle}(|I'\rangle)/\pi \end{cases} \quad (22)$$

where $\text{abs}(\cdot)$ and $\text{angle}(\cdot)$ denote the extraction of amplitude and phase, respectively.

Step 5. Execute inverse QAT (iQAT) on quantum images $|I'_1\rangle$ and $|I'_2\rangle$ with keys p_1 and p_2 , thus the original images $|I_1\rangle$ and $|I_2\rangle$ are decrypted.

$$\begin{aligned} |I_1\rangle &= \text{iQAT}_{p_1}(|I'_1\rangle) \\ &= \text{iQAT}_{p_1} \left(\frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |\alpha_{yx}\rangle \otimes (|y'x'\rangle) \right) \\ &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |\alpha_{yx}\rangle \otimes \text{iQAT}_{p_1}(|y'x'\rangle) \\ &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |\alpha_{yx}\rangle \otimes |yx\rangle \end{aligned} \quad (23)$$

$$\begin{aligned} |I_2\rangle &= \text{iQAT}_{p_2}(|I'_2\rangle) \\ &= \text{iQAT}_{p_2} \left(\frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |\beta_{yx}\rangle \otimes (|y'x'\rangle) \right) \\ &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |\beta_{yx}\rangle \otimes \text{iQAT}_{p_2}(|y'x'\rangle) \\ &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |\beta_{yx}\rangle \otimes |yx\rangle \end{aligned} \quad (24)$$

where iQAT_{p_1} denotes operate p_1 times iQAT on pixel position $|y'x'\rangle$ and iQAT_{p_2} operates in a similar way. The iQAT can be expressed, as follows,

$$\begin{aligned} \text{iQAT}(|y'x'\rangle) &= \text{iQAT}(|y'\rangle|x'\rangle) \\ &= |(-x' + y') \bmod 2^n\rangle |(2x' - y') \bmod 2^n\rangle \\ &= |y\rangle|x\rangle = |yx\rangle \end{aligned} \quad (25)$$

4. Numerical Simulation and Discussion

Due to the lack of quantum hardware to implement the proposed double image encryption algorithm, numerical simulations are made on a classical computer with the MATLAB software (R2017a, MathWorks, Natick, MA, USA). The quantum states and quantum transformations can be simulated using complex vectors and unitary matrices. Therefore, the MATLAB is good at dealing with linear algebra is selected as the simulation tool. The size of all the original images is 256×256 and the period of QAT is 192. The image is scrambled when the parameter of QAT is not exactly equal to the multiple of period. The randomly selected iteration times of QAT can be severed as keys and they are set to $p_1 = 42$ and $p_2 = 73$ in the experiment. The rotation matrices $R(\phi)$ and $T(\psi)$ are randomly generated. Three pairs of original images and corresponding cipher images are shown in Figure 2, from which can be seen that the encrypted images are noise-like and security analyses are given in the following subsections.

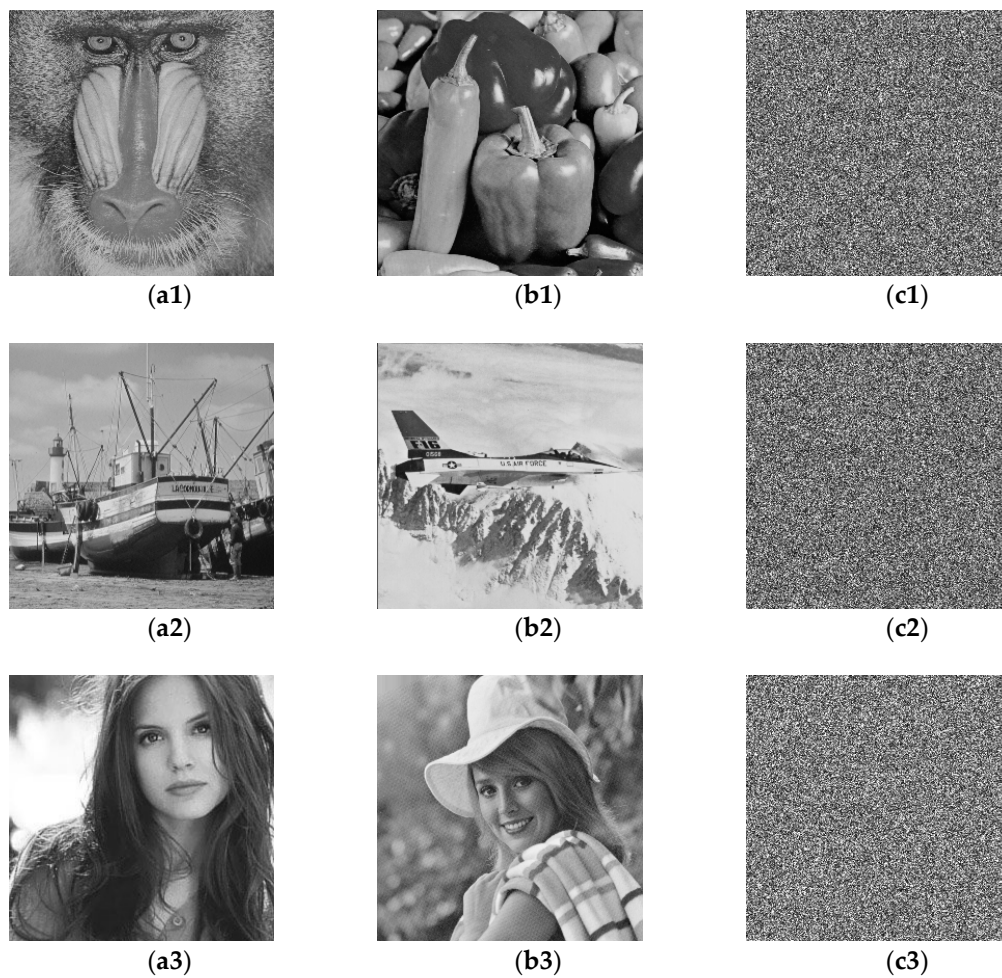


Figure 2. Three pairs of original images and corresponding cipher images.

4.1. Histogram Analysis

The gray histogram is generally used to view the pixel distribution by counting the frequency of pixels in all gray levels. The histograms corresponding to Figure 2 are plotted in Figure 3, from which it can be seen that the histogram of each original image is different from each other, but the histograms of all the cipher images are similar. In addition, the histograms of the cipher images are smoother. Therefore, there is no clue for eavesdroppers performing statistical attack or differential attack on the encrypted images and any useful information cannot be obtained.

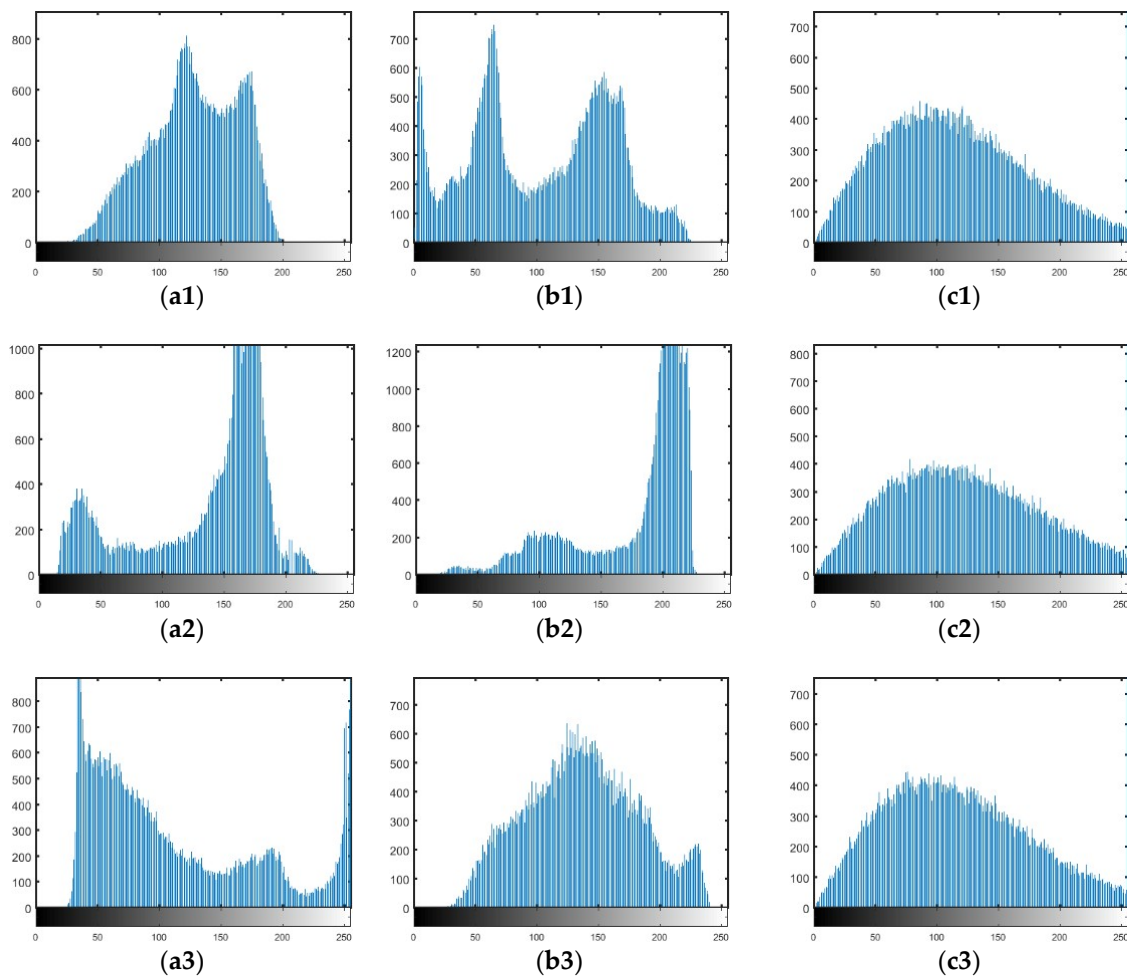


Figure 3. The histograms of original images and cipher images.

4.2. Correlation Analysis

The adjacent pixels in natural images are highly correlated while such correlation should be break for an ideal image encryption scheme. To verify the confusion and diffusion effect of the proposed double quantum image encryption algorithm, the correlation coefficients (CC) in horizontal, vertical, and diagonal directions are computed. Moreover, the correlation distributions are plotted.

The CC value of adjacent pixels is defined, as follows,

$$CC = \frac{\sum_{l=1}^N (u_l - \bar{u})(v_l - \bar{v})}{\sqrt{\sum_{l=1}^N (u_l - \bar{u})^2 \sum_{l=1}^N (v_l - \bar{v})^2}} \tag{26}$$

where u and v represent two adjacent pixel values. The \bar{u} and \bar{v} denote mean value, i.e., $\bar{u} = \sum_{l=1}^N u_l / N$ and $\bar{v} = \sum_{l=1}^N v_l / N$.

Take the images shown in Figure 2 as example to test the correlation of adjacent pixels, and the CC values in three directions are listed in Table 2. It can be seen that the CC values in the cipher image are close to 0 in three directions, which means that the correlation is greatly decreased in cipher images.

Table 2. Correlation coefficients of original images and cipher images.

Correlation Coefficient	Horizontal	Vertical	Diagonal
Figure 2(a1)	0.5720	0.6781	0.5722
Figure 2(b1)	0.9557	0.9231	0.8861
Figure 2(c1)	−0.0368	−0.0111	0.0135
Figure 2(a2)	0.8702	0.6628	0.6315
Figure 2(b2)	0.9045	0.9315	0.8633
Figure 2(c2)	−0.0351	0.0396	−0.0260
Figure 2(a3)	0.9939	0.9859	0.9791
Figure 2(b3)	0.9548	0.9565	0.9079
Figure 2(c3)	0.0004	−0.0121	0.0128

In addition, in order to visualize the correlation distribution of original images and the cipher image, 16,000 pairs of adjacent pixels are randomly selected from each direction. Take the images in third group as example, the distributions in horizontal, vertical, and diagonal directions are respectively shown in Figure 4a–i. The first row shows the horizontal distributions and second row shows the vertical distribution, and the diagonal direction is shown in the last row. From the distribution, figures of adjacent pixels can be seen that the proposed algorithm breaks the high correlation in original images and therefore the eavesdroppers cannot obtain information from the statistical analysis.

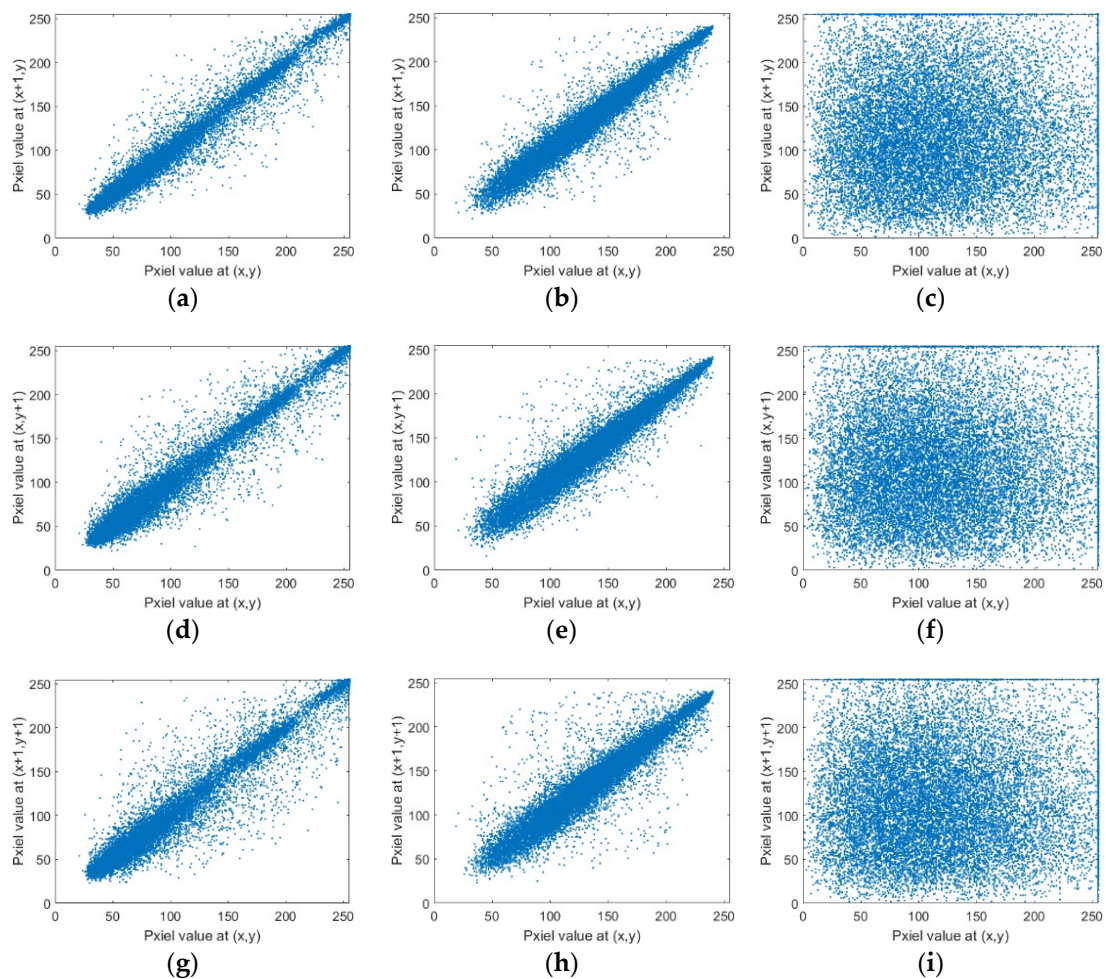


Figure 4. The distribution of adjacent pixels in horizontal, vertical and diagonal directions.

4.3. Information Entropy

The information entropy can reflect the spatial feature of gray distribution, which is defined using the probability of gray value. As the gray level of experimental images is 0–255, suppose that the probability of gray value i is $P(i)$, then the information entropy IE can be calculated as

$$IE = -\sum_{i=0}^{255} P(i) \log_2 P(i) \quad (27)$$

The value of IE grows with the degree of confusion and the ideal value for encrypted image should be 8. Table 3 lists the IE values of original images and cipher images, from which can be seen that information entropy is increased. The results of information entropy coincided with the correlation analysis.

Table 3. The information entropy of original and cipher images.

Images	IE
Figure 2(a1)	7.1273
Figure 2(b1)	7.5693
Figure 2(c1)	7.7459
Figure 2(a2)	7.1208
Figure 2(b2)	6.7040
Figure 2(c2)	7.7289
Figure 2(a3)	7.4457
Figure 2(b3)	7.5046
Figure 2(c3)	7.7578

4.4. Noise Robustness

The images are usually interfered with noises during processing or transmission, which decrease the quality of decrypted images. In order to value the robustness of anti-noise of the proposed algorithm, Gaussian noises with different intensity are added to the encrypted images. Take the second group of image as example, let E denote the encrypted image and E' represents the noisy encrypted image, then the noise adding process can be expressed as

$$E' = E + kG \quad (28)$$

where G denotes $(0, 1)$ Gaussian noise and k is noise intensity. The decrypted images with different noise intensity are shown in Figure 5a–f. Although the noise intensity increases to 120, the original information can still be recognized.

In addition, the mean square error (MSE) is introduced to quantitative compare the difference of between the decrypted image and the original image. The MSE is defined as

$$MSE = \frac{\sum_{i=1}^{2n} \sum_{j=1}^{2n} (D(i, j) - I(i, j))^2}{2^n \times 2^n} \quad (29)$$

where $D(i, j)$ and $I(i, j)$ denote the decrypted image and the original image, respectively. The MSE curves under different intensities of noise are plotted in Figure 6. In combination with the decrypted images that are shown in Figure 5, it can be seen that the proposed algorithm performs good in resisting noise attacks. It also can be concluded that the QAT scrambling process improves the performance of anti-noise in some degree.

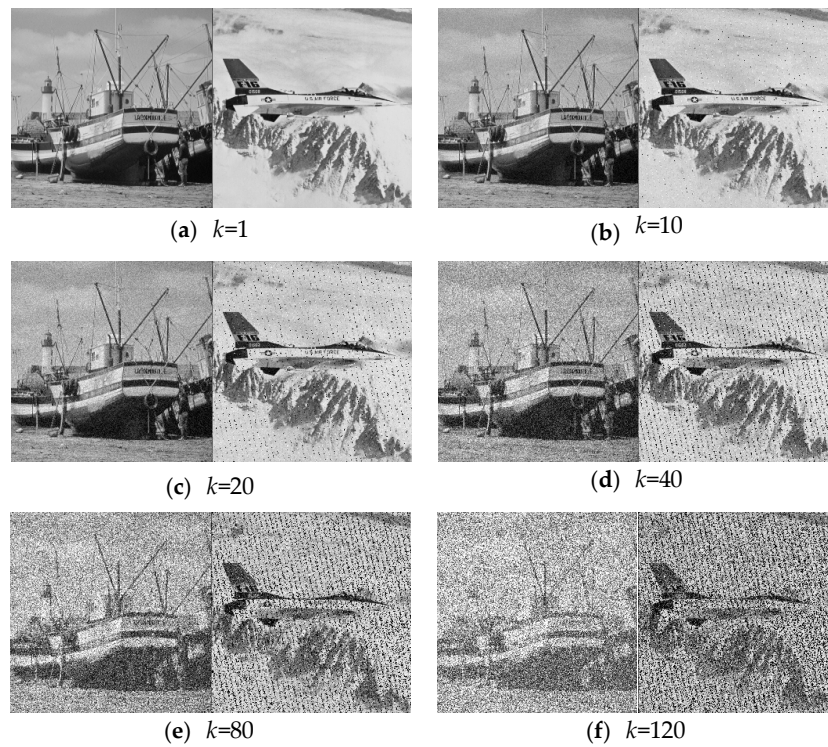


Figure 5. The recovered results of different noise intensity attack.

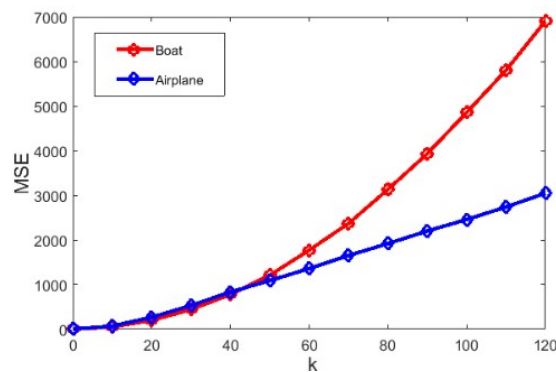


Figure 6. The mean square error (MSE) curves under different intensities of noise.

4.5. Key Sensitivity Analysis

For a good image cryptosystem, the cipher key should be sensitive to secure it against brute-force attack. In the proposed algorithm, the keys include two independent random rotation matrices and two parameters of QAT. Take the first group of image as an example, the decrypted images with correct keys are shown in Figure 7a. Figure 7b shows the decrypted images with incorrect random rotation matrix $R(\phi)$, from which can be seen that the recovered images are blurry. Figure 7c shows the decrypted images with incorrect random rotation matrix $T(\psi)$, from which can be seen that the recovered images are noise-like and any useful information cannot be obtained. The decrypted images with incorrect parameters of QAT are shown in Figure 7d,e, where the deviations of parameters are 3 and 8 respectively. Obviously, the original image can be successfully recovered when all the keys are correct.

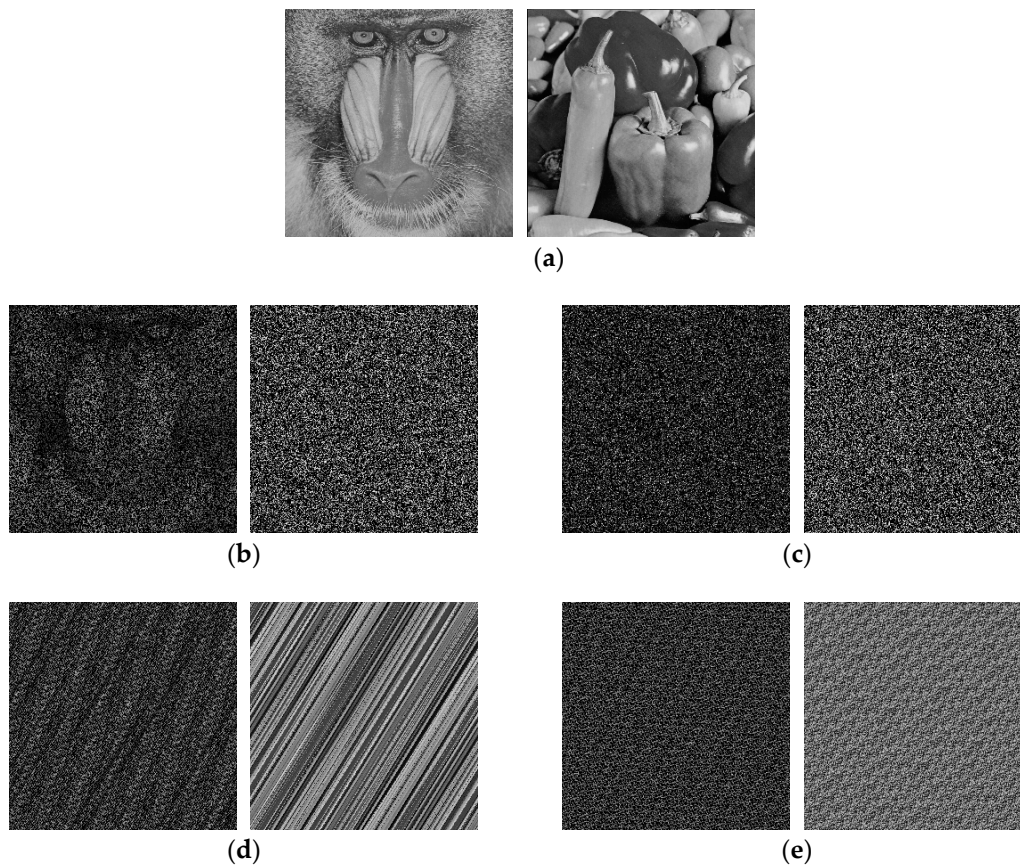


Figure 7. The decryption result with (a) correct keys, (b) incorrect random rotation matrix $R(\phi)$, (c) incorrect random rotation matrix $T(\psi)$, (d) incorrect quantum Arnold transform (QAT) parameters, and (e) another pair of incorrect QAT parameters.

In addition, the key space of the proposed algorithm is analyzed. To resist brute-force attack, the key space should be larger than 2^{100} under current computation ability. As the keys used are independent, the total key space is the product of a single key space. The key space for QAT is about 2^{15} . The key space for random rotation matrix depends on the size of image, which is larger than $2^{256 \times 256}$. Therefore, the key space is large enough to ensure the security of the proposed algorithm. In addition, the key space of the proposed algorithm is compared with several state of art image encryption algorithms [26,27,32–34]. The comparison results that are shown in Table 4 indicate that the proposed algorithm has a larger key space.

Table 4. The key space comparison results.

Encryption Algorithms	Key Space
Proposed algorithm	$2^{256 \times 256 + 15}$
Reference [28]	2^{298}
Reference [29]	2^{299}
Reference [34]	2^{375}
Reference [35]	10^{248}
Reference [36]	10^{58}

4.6. Computational Complexity Analysis

The computational complexity of the proposed algorithm and classical counterpart is analyzed in this subsection. The complexity of quantum algorithm depends on the basic logical element such as Control-NOT gate and NOT gate. The complexity of quantum adder is about $28n$ [25]. The adder-mod

module includes five adder modules and therefore the complexity of QAT is about $140n$. As the proposed algorithm uses twice QAT and the computational complexity in QAT scrambling is estimated to $280n$. In addition, the quantum circuits of QFT including $n(n-1)/2$ basic gates and random rotation operation has a $O(n)$ complexity. Therefore, the complexity of the proposed algorithm is $O(n^2)$. The computational complexity of each step and overall complexity is shown in Table 5. By contrast, if this algorithm runs on a classical computer, all the operations are performed on every pixel, then the complexity of Arnold transform and angle rotation is 2^{2n} . Besides, the computational complexity of Fourier transform is $O(n2^{2n})$. Therefore, the complexity of the classical algorithm is $O(n2^{2n})$, which is more complex than the quantum one. In a conclusion, the proposed double quantum image encryption algorithm performs better than its classical counterpart in the aspect of computational complexity.

Table 5. The computational complexity of each step and overall complexity.

Step 1	Step 2	Step 3	Step 4	Step 5	Overall Complexity
$O(n)$	$O(n)$	$O(n)$	$O(n^2)$	$O(n^2)$	$O(n^2)$

5. Conclusions

In this paper, a double quantum gray image encryption algorithm that is based on QAT and quantum random rotation is proposed. The main contribution of this paper lies in encrypting double quantum gray images by combining quantum permutation and qubits angle random rotation, which further improves the encryption efficiency. The original two images can be completely retrieved without distortion and cross-talk through using correct keys. The key space of the proposed method is larger than the compared methods, which ensures the security to resist brute-force attack. Experimental results and theoretical analysis show that the proposed algorithm is robustness to resist statistical attack and noise attack. Moreover, the proposed algorithm is superior compared with its counterpart in terms of computational complexity.

There are also some disadvantages in the proposed scheme, such as the histogram of the ciphertext image, is not uniformly distributed. In addition, the color image usually presents abundant information, so color image encryption should be paid more attention. We will focus on solving disadvantages and putting forward double color image encryption schemes in our future research.

Author Contributions: X.L. designed methodology and performed the experiments. D.X. made helpful suggestions for the paper. C.L. worked on the formula derivation. All authors read and approved the final manuscript.

Funding: The work was funded by the National Natural Science Foundation of China (Grant No. 61572089, 61802037), the China Postdoctoral Science Foundation(Grant No. 2018m640899), the Chongqing Special Postdoctoral Science Foundation (XmT2018032), the Chongqing Research Program of Basic Research and Frontier Technology (Grant No. cstc2017jcyjBX0008), the Chongqing Postgraduate Education Reform Project (Grant No. yjg183018), the Chongqing University Postgraduate Education Reform Project (Grant No. cqyjg18219) and the Fundamental Research Funds for the Central Universities (Grant Nos. 106112017CDJQJ188830, 106112017CDJXY180005).

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

References

- Abura'ed, N.; Khan, F.S.; Bhaskar, H. Advances in the Quantum Theoretical Approach to Image Processing Applications. *ACM Comput. Surv.* **2017**, *49*, 75. [[CrossRef](#)]
- Yan, F.; Iliyasu, A.M.; Le, P.Q. Quantum Image Processing: A Review of Advances in its Security Technologies. *Int. J. Quantum Inf.* **2017**, *15*, 1730001. [[CrossRef](#)]
- Yan, F.; Iliyasu, A.; Jiang, Z. Quantum computation-based image representation, processing operations and their applications. *Entropy* **2014**, *16*, 5290–5338. [[CrossRef](#)]

4. 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*, 188. [[CrossRef](#)]
5. Abd El-Latif, A.A.; Abd-El-Atty, B.; Hossain, M.S.; Rahman, M.A.; Alamri, A.; Gupta, B.B. Efficient quantum information hiding for remote medical image sharing. *IEEE Access* **2018**, *6*, 21075–21083. [[CrossRef](#)]
6. Yang, Y.G.; Pan, Q.X.; Sun, S.J.; Xu, P. Novel image encryption based on quantum walks. *Sci. Rep.* **2015**, *5*, 7784. [[CrossRef](#)] [[PubMed](#)]
7. Yang, Y.-G.; Tian, J.; Lei, H.; Zhou, Y.-H.; Shi, W.-M. Novel quantum image encryption using one-dimensional quantum cellular automata. *Inf. Sci.* **2016**, *345*, 257–270. [[CrossRef](#)]
8. Abd El-Latif, A.A.; Abd-El-Atty, B.; Talha, M. Robust encryption of quantum medical images. *IEEE Access* **2018**, *6*, 1073–1081. [[CrossRef](#)]
9. 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](#)]
10. Gong, L.-H.; He, X.-T.; Tan, R.-C.; Zhou, Z.-H. Single channel quantum color image encryption algorithm based on HSI model and quantum Fourier transform. *Int. J. Theor. Phys.* **2017**, *57*, 59–73. [[CrossRef](#)]
11. Hu, Y.; Xie, X.; Liu, X.; Zhou, N. Quantum multi-image encryption based on iteration Arnold transform with parameters and image correlation decomposition. *Int. J. Theor. Phys.* **2017**, *56*, 2192–2205. [[CrossRef](#)]
12. Li, H.-S.; Li, C.; Chen, X.; Xia, H.-Y. Quantum image encryption algorithm based on NASS. *Int. J. Theor. Phys.* **2018**. [[CrossRef](#)]
13. 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](#)]
14. 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.* **2012**, *52*, 1802–1817. [[CrossRef](#)]
15. 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](#)]
16. 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](#)]
17. Li, P.; Zhao, Y. A simple encryption algorithm for quantum color image. *Int. J. Theor. Phys.* **2017**, *56*, 1961–1982. [[CrossRef](#)]
18. Jozsa, R. Quantum algorithms and the Fourier transform. *Proc. R. Soc. Lond. A Math. Phys. Eng. Sci.* **1998**, *454*, 323–337. [[CrossRef](#)]
19. Fijany, A.; Williams, C.P. Quantum wavelet transforms: fast algorithms and complete circuits. *Quantum Comput. Quantum Commun.* **1999**, *1509*, 10–33.
20. Tseng, C.C.; Hwang, T.M. Quantum Circuit Design of 8×8 Discrete Cosine Transform Using its Fast Computation Flow Graph. In Proceedings of the 2004 IEEE Asia-Pacific Conference on Circuits and Systems, Tainan, Taiwan, 6–9 December 2004; pp. 801–804.
21. Hamza, A.B.; Krim, H. Jensen-Rényi divergence measure: Theoretical and computational perspectives. In Proceedings of the 2003 IEEE International Symposium on Information Theory, Yokohama, Japan, 29 June–4 July 2003; p. 257.
22. Abdallah, E.E.; Hamza, A.B.; Bhattacharya, P. MPEG video watermarking using tensor singular value decomposition. In Proceedings of the Springer International Conference on Image Analysis and Recognition, Montreal, QC, Canada, 22–24 August 2007.
23. Yang, Y.-G.; Xia, J.; Jia, X.; Zhang, H. Novel image encryption/decryption based on quantum Fourier transform and double phase encoding. *Quantum Inf. Process.* **2013**, *12*, 3477–3493. [[CrossRef](#)]
24. 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. *Inf. Sci.* **2014**, *277*, 445–457. [[CrossRef](#)]
25. 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](#)]
26. Jiang, N.; Wang, L. Analysis and improvement of the quantum Arnold image scrambling. *Quantum Inf. Process.* **2014**, *13*, 1545–1551. [[CrossRef](#)]
27. Jiang, N.; Wu, W.Y.; Wang, L. The quantum realization of Arnold and Fibonacci image scrambling. *Quantum Inf. Process.* **2014**, *13*, 1223–1236. [[CrossRef](#)]
28. Stoyanov, B.; Kordov, K. Image encryption using chebyshev map and rotation equation. *Entropy* **2015**, *17*, 2117–2139. [[CrossRef](#)]

29. Fan, H.; Li, M. Cryptanalysis and improvement of chaos-based image encryption scheme with circular inter-intra-pixels bit-level permutation. *Math. Probl. Eng.* **2017**, *2017*, 8124912. [[CrossRef](#)]
30. Parvees, M.M.; Samath, J.A.; Raj, I.K.; Bose, B.P. A colour byte scrambling technique for efficient image encryption based on combined chaotic map: Image encryption using combined chaotic map. In Proceedings of the 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, India, 3–5 March 2016; pp. 1067–1072.
31. Karawia, A. Encryption algorithm of multiple-image using mixed image elements and two dimensional chaotic economic map. *Entropy* **2018**, *20*, 801. [[CrossRef](#)]
32. Li, S.; Ding, W.; Yin, B.; Zhang, T.; Ma, Y. A novel delay linear coupling logistics map model for color image encryption. *Entropy* **2018**, *20*, 463. [[CrossRef](#)]
33. Diaconu, A.V. Circular inter-intra pixels bit-level permutation and chaos-based image encryption. *Inf. Sci.* **2016**, *355*, 314. [[CrossRef](#)]
34. Stoyanov, B.; Kordov, K. Novel image encryption scheme based on chebyshev polynomial and duffing map. *Sci. World J.* **2014**, *2014*, 283639. [[CrossRef](#)] [[PubMed](#)]
35. Parvees, M.M.; Samath, J.A.; Bose, B.P. Protecting large size medical images with logistic map using dynamic parameters and key image. *Int. J. Netw. Secur.* **2017**, *19*, 984.
36. 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](#)]
37. 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](#)]
38. Liang, H.-R.; Tao, X.-Y.; Zhou, N.-R. Quantum image encryption based on generalized affine transform and logistic map. *Quantum Inf. Process.* **2016**, *15*, 2701–2724. [[CrossRef](#)]
39. Jiang, N.; Wang, L.; Wu, W.Y. Quantum Hilbert image scrambling. *Int. J. Theor. Phys.* **2014**, *53*, 2463–2484. [[CrossRef](#)]
40. Zhou, R.-G.; Sun, Y.-J.; Fan, P. Quantum image gray-code and bit-plane scrambling. *Quantum Inf. Process.* **2015**, *14*, 1717–1734. [[CrossRef](#)]
41. Naseri, M.; Abdolmaleky, M.; Parandin, F.; Fatahi, N.; Farouk, A.; Nazari, R. A new quantum gray-scale image encoding scheme. *Commun. Theor. Phys.* **2018**, *69*, 215. [[CrossRef](#)]
42. 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](#)]



© 2018 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).