Quantum Information Processing (2021) 20:23
https://doi.org/10.1007/s11128-020-02952-7

Three-level quantum image encryption based on Arnold transform and logistic map

Xingbin Liu[1] · Di Xiao[1] · Cong Liu[2]

Received: 27 July 2020 / Accepted: 24 November 2020 / Published online: 11 January 2021

Abstract

Quantum computation improves the efficiency and security of cryptography by utilizing characteristics of quantum mechanics. In this paper, a novel three-level quantum image encryption algorithm based on Arnold transform and logistic map is proposed. To obtain satisfactory encryption results, three-level encryption procedures including block-level permutation, bit-level permutation and pixel-level diffusion are performed on the original image. First, the classical plaintext image is transformed into quantum form with novel enhanced quantum representation model. Then, quantum Arnold transform (QArT) is used to scramble the image sub-blocks by processing the qubits that denote position information. By iterating block-level permutation procedure with different block-size and different parameter of QArT, the period defect of QArT can be made up to some extent. Next the bit-level permutation is performed by scrambling the bit-plane order according to a sequence generated with logistic map. Finally, the ciphertext image can be obtained by performing bit-level diffusion through XOR operation between bit-level permutated image and a pseudo-random sequence acquired from logistic map. The corresponding quantum circuits realization are given, and simulations results show that the proposed three-level quantum image encryption scheme has high level of security and outperforms its classical counterpart in terms of efficiency.

Keywords Quantum image encryption · Block permutation · XOR operation · Quantum bit-level permutation · Logistic map

✉ Xingbin Liu
xbliu6@163.com

[1] College of Computer Science, Chongqing University, Chongqing 400044, China

[2] Southwest Technology and Engineering Research Institute, Chongqing 40039, China

1 Introduction

With the rapid development of communication and computation technology, information exchange through various kinds of carriers such as text, image, video, and so on has become omnipresent and important in modern life. The images including gray images and color images are widely used to transmit information as they contain rich visual content [1, 2]. However, the high-volume data and redundancy of image also rise the serious issues of secure transmission and storage [3]. To effectively protect image contents and prevent unauthorized access to obtain original image information, a variety of image encryption methods have been introduced in recent years [4–8].

According to actual development status as concerned, the image encryption methods can be roughly classified into two branches, and one kind is traditional image encryption algorithm that runs on a classical computer and the other is quantum image encryption algorithm that needs to be run on a quantum hardware system. For the traditional image encryption algorithm, a lot of research works have been carried out [9]. However, the traditional cryptosystems are threatened as the quantum computation improves the efficiency of cracking. Therefore, the research of quantum image encryption will be more and more crucial in the field of information security [10].

To conveniently store and process quantum images, several representation models for quantum images were designed. Similar to the representation of classical image, a flexible representation of quantum images (FRQI) model [11] was proposed, which stores the color and corresponding position information into quantum superposition states. Afterward, a novel enhanced quantum representation (NEQR) model [12] was proposed by extending FRQI, which used an entangled qubit sequence to exactly represent the color information, and therefore, the original pixel values can be retrieved accurately. In addition, some other quantum image representation models, such as normal arbitrary superposition state (NASS) model [13], multi-channel quantum image (MCQI) model [14], are proposed to improve the efficiency of specific applications.

With the introduction of quantum representation models, numerous quantum image encryption approaches have been proposed [15–19]. The majority of the proposed quantum image encryption algorithms is realized in spatial domain with pixel scrambling and XOR operations. Zhou accomplished the quantum image encryption algorithm through several quantum image geometric transforms, and the quantum circuits were given [20]. Liang utilized logistic map to generate key map, and the original image can be encrypted with XOR operation [21]. Zhu made the original image chaotic by using the proposed dual-scrambling scheme including bit-plane transformation and position transformation [22]. There are also some quantum image encryption algorithms proposed in the transform domain. Yang performed a quantum image encryption method in Fourier transform domain by using the double random phase encoding (DRPE) technique [23]. The DRPE algorithm is improved by Du, and the results are more uniformly mixed [24]. Hu proposed a quantum image encryption algorithm based on Arnold

scrambling and wavelet transforms, which combines the spatial and transform scrambling to achieve good encryption results [25]. Li used quantum Haar wavelet packet transform to encrypt quantum image and obtained satisfactory results [26]. Some quantum multiple image encryption algorithms are proposed to further improve efficiency. Wang proposed a double quantum color image encryption algorithm and verify the validity in the quantum field [27]. Liu used the Arnold transform and qubit random rotation to encrypt two quantum images simultaneously [28]. To effectively encrypt the region of interest, a quantum selective encryption algorithm for medical images is proposed by manipulating bit-planes of original images [29]. Because the chaotic systems have good ergodicity and cross-correlation properties, they are extensively used in the quantum image encryption algorithms. Two-dimensional Henon chaotic mapping is introduced in the quantum image encryption algorithm, and the encryption results have good randomness [30]. A 5D hyper-chaotic system is used in Zhou's scheme to realize higher security since it has more complex dynamic behavior [31]. The Chen's hyper-chaotic system is also applied in the quantum image encryption algorithm to generate pseudo-random sequences [32]. In addition, some scholars proposed several quantum image encryption algorithms by combining the permutation maps and chaotic systems [33, 34].

The aforementioned quantum image encryption algorithms encrypt the original image in bit level or pixel level, and the least processing unit is one bit or one pixel. Actually, the block-level-based classical image encryption algorithms have been presented to improve the security of image encryption algorithms. Wang proposed a chaotic block image encryption algorithm based on dynamic random growth technique [35]. Chai used plain image-related swapping block permutation and block diffusion operations to design a chaos-based image encryption scheme [36]. In addition, Ye proposed a block chaotic image encryption scheme based on self-adaptive modeling [37]. Although the block-level-based image encryption algorithms can enhance the security, they also led to high computational complexity. With the help of parallelism, quantum computation can greatly improve operation efficiency. In order to further improve the efficiency and security of the quantum image encryption, the sub-block scrambling of image is considered and a novel three-level quantum image encryption algorithm including block-level permutation, bit-level permutation and pixel-level diffusion is proposed. First, the original image is represented with NEQR model, and then, the obtained quantum image can be divided into sub-blocks by setting block-size. Then, the image blocks are scrambled by quantum Arnold transform (QArT), and the order of sub-blocks is changed. By setting different block-size and different iteration parameter of QArT, the defects of period can be made up to some extent. Next the bit-level permutation is performed by random scramble the bit-planes order using sequence generated with logistic map. Finally, the ciphertext image can be obtained by performing bit-level diffusion through XOR operation between bit-level permutated image and a pseudo-random sequence acquired from logistic map. As the quantum operation is invertible, the decryption is exactly the inverse process of encryption. Since the NEQR model is adopted, the original information can be accurately recovered with correct keys by quantum measurement. Through the introduction of sub-blocks permutation operation, the encryption process includes a block-level permutation and therefore

the key space is increased. Moreover, by changing the size of sub-blocks and iteration times, the key space can be further expanded. As a result, the security of the algorithm is improved by applying the sub-blocks permutation operation. The main contributions of this method can be summarized as follows: (1) the introduction of block-level scrambling enlarge the period of QArT and further improve the security, (2) the order of bit-level is random scrambled to change pixel values, and (3) the logistic map is used to accomplish pixel-level diffusion and achieve good encryption results. Numerical simulation and performance comparison demonstrate that the proposed method is effective in securing quantum image information and the security is verified by statistical analysis, key space analysis and robustness analysis.

The rest of this paper is organized as follows: In Sect. 2, some fundamental theories including NEQR representation model, QArT, and logistic map are briefly introduced. In Sect. 3, the proposed three-level quantum image encryption scheme is described in detail. To verify the performance, Sect. 4 gives the numerical experiment results and the theoretical security analysis is shown. Finally, conclusions are drawn in Sect. 5.

2 Preliminary knowledge

2.1 NEQR representation model

The fundamental task for quantum image processing is fed the digital image into quantum hardware. The NEQR model is an excellent quantum image representation model [12], which adopts the basic state to store gray-scale values appropriately, and therefore, the original information can be accurately retrieved using quantum measurement.

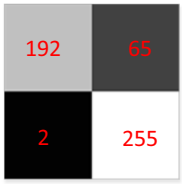
In NEQR model, the pixel value can be stored in a binary sequence, i.e., the gray-scale information is represented as $\{|00000000\rangle, |00000001\rangle, \ldots |11111111\rangle\}$. In addition, the spatial location information is stored in a pair of qubits sequences $|y\rangle$ and $|x\rangle$, which denote the indices of rows and columns. For a $2^n \times 2^n$ digital image, the corresponding NEQR model can be expressed as follows:

$$|I\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |C(y,x)\rangle \otimes |yx\rangle \tag{1}$$

where the gray-scale value in position (y,x) is denoted as $|C(y,x)\rangle = \left|c_{yx}^{q-1} c_{yx}^{q-2} \cdots c_{yx}^{1} c_{yx}^{0}\right\rangle$ and the range of pixel value is $\left[0, 2^{q-1}\right]$. The vertical position and horizontal position are represented with qubits $|yx\rangle$. Thus, the digital image I can be stored into a normalized superposition state $|I\rangle$. Figure 1 shows an example of 2×2 NEQR and its corresponding quantum representation.

2.2 Quantum Arnold transform (QArT)

The classical two-dimensional Arnold transform is generally used as a pre-processing tool to scramble image in watermarking and encryption applications. The matrix form of Arnold transform can be defined as follows:



$$|I\rangle = \frac{1}{2}\left(|192\rangle\otimes|00\rangle + |65\rangle\otimes|01\rangle + |2\rangle\otimes|10\rangle + |255\rangle\otimes|11\rangle\right)$$
$$= \frac{1}{2}\begin{pmatrix} |11000000\rangle\otimes|00\rangle + |01000001\rangle\otimes|01\rangle \\ +|00000010\rangle\otimes|10\rangle + |111111111\rangle\otimes|11\rangle \end{pmatrix}$$

Fig. 1 The NEQR representation of a 2×2 image

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} (\mathrm{mod}\ 2^n),\ x, y = 0, 1, \ldots, 2^n - 1 \tag{2}$$

where (x, y) denotes the coordinate information of original image before scrambling and (x', y') represents the scrambled coordinate. The symbol N denotes the size of image to be processed.

According to the transform equation, the transformed coordinate (x', y') can be obtained as:

$$\begin{cases} x' = (x + y)\ \mathrm{mod}\ \ 2^n \\ y' = (x + 2y)\ \mathrm{mod}\ \ 2^n \end{cases} \tag{3}$$

The classical Arnold transform is extended to the quantum version by Jiang et al., and the QArT can be accomplished with quantum plain adder network and adder modulo N network. The corresponding quantum circuits for QArT is shown in Fig. 2, and the detailed description can be found in [38].

The QArT only changes the information of coordinates and the gray-scale information is remain unchanged. For a quantum image denoted as $|I\rangle$, one iteration of QArT operation can be expressed as:

$$\begin{aligned} |I'\rangle = \mathrm{QArT}(|I\rangle) &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|C(y,x)\rangle\mathrm{QArT}(|yx\rangle) \\ &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|C(y,x)\rangle\mathrm{QArT}(|y\rangle)\mathrm{QArT}(|x\rangle) \end{aligned} \tag{4}$$

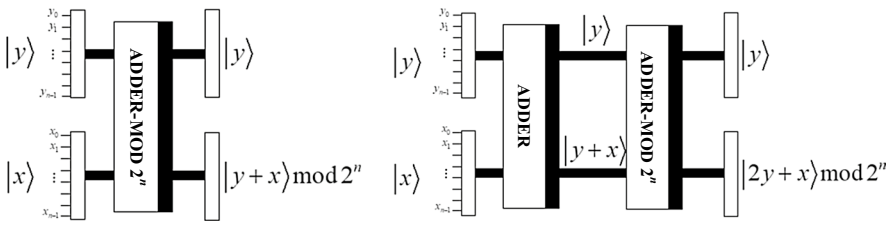


Fig. 2 The quantum circuits for QArT

Similar to the classical Arnold transform, the scrambled coordinates of quantum image $|I\rangle$ can be written as:

$$\begin{cases} |x'\rangle = \mathrm{QArT}(|x\rangle) = |x + y\rangle \bmod 2^n \\ |y'\rangle = \mathrm{QArT}(|y\rangle) = |x + 2y\rangle \bmod 2^n \end{cases} \tag{5}$$

Based on Eq. (5), the inverse QArT can be easily derived as follows:

$$\begin{cases} |x\rangle = \left(2|x'\rangle - |y'\rangle\right) \bmod 2^n \\ |y\rangle = \left(-|x'\rangle + |y'\rangle\right) \bmod 2^n \end{cases} \tag{6}$$

2.3 Logistic map

The chaotic systems are suitable for designing quantum image encryption algorithms as they have excellent random characteristics, such as deterministic, ergodicity, sensitive to initial and control parameters [39]. The logistic map is a commonly used chaotic systems to secure the transmission of images, which is defined as:

$$\chi_{k+1} = \alpha \chi_k \left(1 - \chi_k\right) \tag{7}$$

where $\chi_0 \in (0, 1)$ is initial value of chaotic system called seed and α is control parameter. When $\alpha \in [3.85, 4]$, the logistic map is in chaotic state and the generated sequence is pseudo-random.

3 Three-level quantum image encryption scheme

In this section, the proposed three-level quantum image encryption scheme based on QArT and logistic map is presented in detail, and the flowchart is shown in Fig. 3. The whole scheme includes three main procedures, i.e., block-level permutation, bit-level permutation and pixel-level diffusion. The original image is firstly represented with NEQR model, and then, the image sub-blocks are permutated with QArT. Next, the bit-level permutation is performed by randomly changing the order of bit-planes. Finally, the pixel-level diffusion is accomplished by using XOR operation and logistic map, and thus, the encrypted quantum image is obtained. More details of the proposed quantum image encryption scheme are illustrated in the following subsections.

3.1 Block-level permutation

Suppose the original image with size $2^n \times 2^n$ to be encrypted is denoted as $|I\rangle$ and its NEQR representation can be written as:

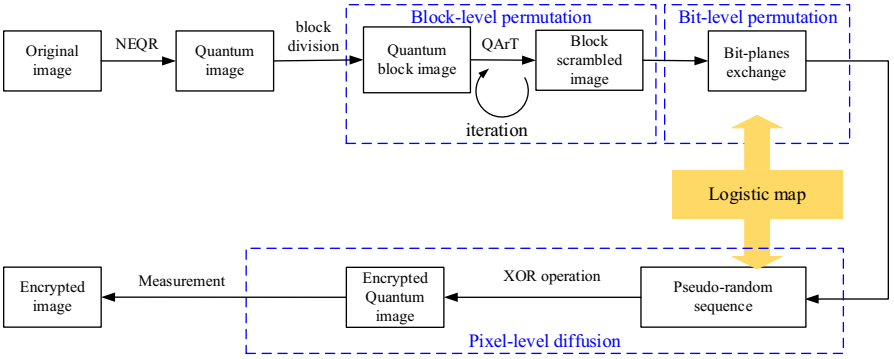


Fig. 3 The flowchart of the proposed quantum image encryption scheme

$$
\begin{aligned}
|I\rangle &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|C(y,x)\rangle \otimes |yx\rangle \\
&= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|C(y,x)\rangle \otimes \left|y_{n-1}y_{n-2}\cdots y_2y_1y_0\right\rangle\left|x_{n-1}x_{n-2}\cdots x_2x_1x_0\right\rangle
\end{aligned} \tag{8}
$$

To effectively accomplish block-level permutation, firstly, the original image should be divided into sub-blocks. By processing the qubits that represent position information in NEQR model, the image blocks can be easily divided. Assume that the block size is set to $2^w \times 2^w$, then keep the least significant w bits unchanged and the indices of image blocks are determined with the other $n-w$ qubits. After division, the total number of blocks is $2^{n-w} \times 2^{n-w}$. Next, the QArT is applied on the $n-w$ qubits which represent position information of image sub-blocks and the permutated block image $|I_b\rangle$ can be obtained. As the block size is $2^w \times 2^w$, the qubits $\left|y_{n-1}y_{n-2}\cdots y_w\right\rangle$ and $\left|x_{n-1}x_{n-2}\cdots x_w\right\rangle$ are transformed using QArT.

$$
\begin{aligned}
|I_b\rangle &= \mathrm{QArT}(|I\rangle) = \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|C(y,x)\rangle \otimes \mathrm{QArT}(|yx\rangle) \\
&= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|C(y,x)\rangle \otimes \mathrm{QArT}\left(\left|y_{n-1}y_{n-2}\cdots y_2y_1y_0\right\rangle\left|x_{n-1}x_{n-2}\cdots x_2x_1x_0\right\rangle\right) \\
&= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|C(y,x)\rangle \otimes \mathrm{QArT}\left(\left|y_{n-1}y_{n-2}\cdots y_w\right\rangle\right)\left|y_{w-1}\cdots y_2y_1y_0\right\rangle \\
&\quad \mathrm{QArT}\left(\left|x_{n-1}x_{n-2}\cdots x_w\right\rangle\right)\left|x_{w-1}\cdots x_2x_1x_0\right\rangle \\
&= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|C(y,x)\rangle \otimes \left|y'_{n-1}y'_{n-2}\cdots y'_wy_{w-1}\cdots y_2y_1y_0\right\rangle\left|x'_{n-1}x'_{n-2}\cdots x'_wx_{w-1}\cdots x_2x_1x_0\right\rangle
\end{aligned} \tag{9}
$$

According to the definition of QArT expressed as Eq. (5), the permutated position qubits $\left|y'_{n-1}y'_{n-2}\cdots y'_w\right\rangle$ and $\left|x'_{n-1}x'_{n-2}\cdots x'_w\right\rangle$ can be obtained as:

$$\begin{cases} \left|y'_{n-1}y'_{n-2}\cdots y'_{w}\right\rangle = \mathrm{QArT}\left(\left|y_{n-1}y_{n-2}\cdots y_{w}\right\rangle\right) = \left(\left|x_{n-1}x_{n-2}\cdots x_{w}\right\rangle + 2\left|y_{n-1}y_{n-2}\cdots y_{w}\right\rangle\right) \bmod 2^{n-w} \\ \left|x'_{n-1}x'_{n-2}\cdots x'_{w}\right\rangle = \mathrm{QArT}\left(\left|x_{n-1}x_{n-2}\cdots x_{w}\right\rangle\right) = \left(\left|x_{n-1}x_{n-2}\cdots x_{w}\right\rangle + \left|y_{n-1}y_{n-2}\cdots y_{w}\right\rangle\right) \bmod 2^{n-w} \end{cases} \tag{10}$$

The corresponding circuit for image sub-block permutation based on QArT is shown in Fig. 4, which is completed with ADDER module and ADDER-MOD module [38].

To further improve the performance of image blocks permutation and overcome the short period defect of QArT, an iteration framework is designed. Through setting different size of image sub-block and different parameter of QArT, the permutation procedures described in Eq. (9)–(10) are executed several times. Thus, the spatial position of original image blocks can be sufficiently scrambled. Take the image "boat" shown in Fig. 5a as example, the result of first-time block-level permutation with parameter $w = 8$ is shown in Fig. 5b and the second-time block-level permutation with parameter $w = 4$ is shown in Fig. 5c. It can be seen from the permutation results that original image is thoroughly scrambled and any useful information cannot be directly obtained.

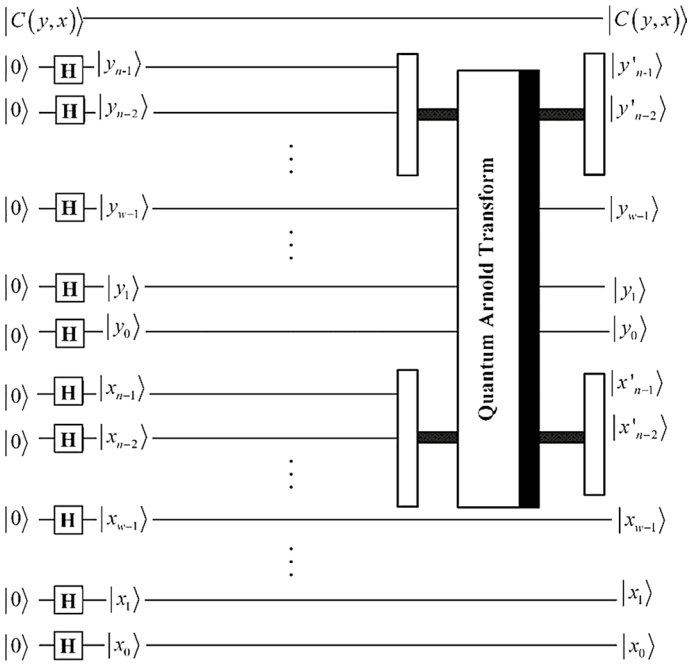
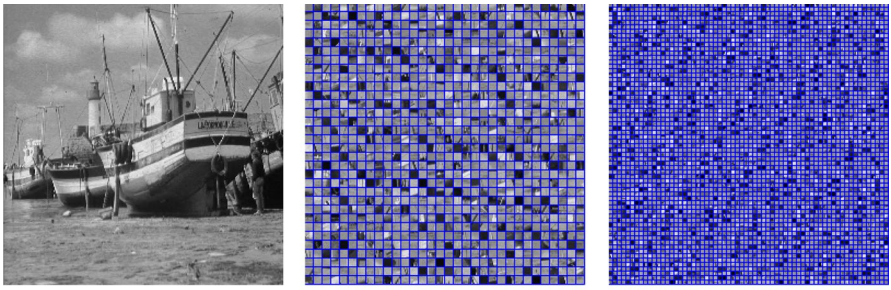


Fig. 4 The quantum circuit for image block permutation based on QArT



(a) Original image **(b)** w=8 **(c)** w=4

Fig. 5 The iterative block-level permutation by using QArT for image "boat"

3.2 Bit-level permutation

After block-level permutation, the position of image blocks has been preliminarily changed. To change pixel value information of the original image, bit-level permutation procedure is performed in this stage. Generally, the pixel value range of gray-scale image is 256, and therefore, 8 bit-planes can be decomposed as shown in Fig. 6.

To achieve bit-level permutation, the order of 8 bit-planes needs to be randomly exchanged and the permutated order is determined with logistic map. By inputting the control parameter α and initial value χ_0 into the logistic map, a chaotic sequence $\{s_1(m) \in (0,1), m = 1, \ldots, N+1, N+2 \ldots, N+8\}$ is obtained. The former N numbers are discarded to avoid transient effect and in the simulation experiment N is set to 10^5. Next, the rest 8 numbers are sorted in ascending order. According to the change of numbers order, the bit-planes make the same change and thus the order is randomly permutated. For example, the generated pseudo-random sequence is $\{0.9782, 0.0854 \ldots 0.0160\}$ and the sorted sequence is $\{0.0040, 0.0160 \ldots 0.0854\}$; then, the permutation order can be obtained as shown in Fig. 7. The corresponding quantum circuit for bit-planes permutation procedure is shown in Fig. 8, where the cross symbol denotes the exchange of bit-planes and it is completed with quantum swap gate.

For specific pixel, the bit-planes permutation operation can be accomplished with controlled quantum swap gate G_{YX} defined as follows:

Fig. 6 The diagram of 8 bit-planes decomposition

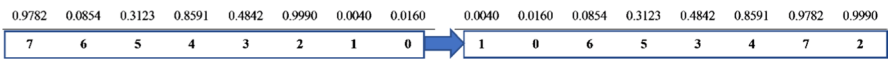


Fig. 7 The diagram of acquiring permutation order of bit-planes

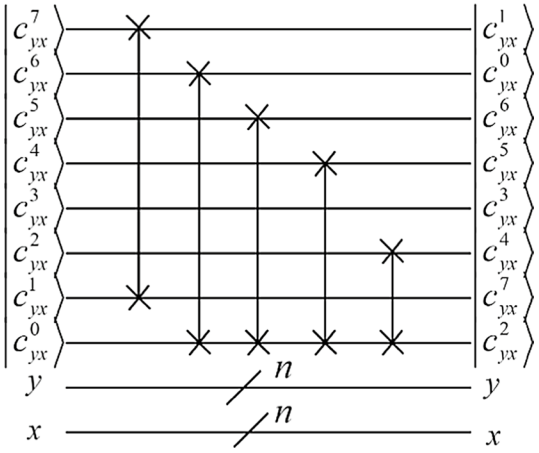


Fig. 8 The quantum circuit for bit-planes permutation

$$\begin{aligned} G_{YX}(|C(y,x)\rangle) &= G_{YX}\left(\left|c_{yx}^{7}c_{yx}^{6}c_{yx}^{5}c_{yx}^{4}c_{yx}^{3}c_{yx}^{2}c_{yx}^{1}c_{yx}^{0}\right\rangle\right) \\ &= \left|c_{yx}^{1}c_{yx}^{0}c_{yx}^{6}c_{yx}^{5}c_{yx}^{3}c_{yx}^{4}c_{yx}^{7}c_{yx}^{2}\right\rangle \end{aligned} \tag{11}$$

Then, the controlled swap gate G_{YX} is used to build a quantum sub-operation H_{YX} as follows to perform the bit-planes permutation.

$$H_{YX} = I \otimes \sum_{y=0}^{2^n-1}\sum_{\substack{x=0 \\ YX\neq yx}}^{2^n-1} |yx\rangle\langle yx| + G_{YX} \otimes |YX\rangle\langle YX| \tag{12}$$

By applying quantum sub-operation H_{YX} on the block-permutated image $|I_b\rangle$, the bit-plane of pixel at position (Y, X) is scrambled.

$$\begin{aligned} &H_{YX}(|I_b\rangle) = H_{YX}(|I_b\rangle) = H_{YX}\left(\frac{1}{2^n}\right) \\ &= \frac{1}{2^n} H_{YX}\left(\sum_{y=0}^{2^n-1}\sum_{\substack{x=0 \\ YX\neq yx}}^{2^n-1} |C(y,x)\rangle \otimes |yx\rangle + |C(Y,X)\rangle \otimes |YX\rangle\right) \\ &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{\substack{x=0 \\ YX\neq yx}}^{2^n-1} |C(y,x)\rangle \otimes |yx\rangle + H_{YX}\left(\left|c_{yx}^{7}c_{yx}^{6}c_{yx}^{5}c_{yx}^{4}c_{yx}^{3}c_{yx}^{2}c_{yx}^{1}c_{yx}^{0}\right\rangle \otimes |YX\rangle\right) \\ &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{\substack{x=0 \\ YX\neq yx}}^{2^n-1} |C(y,x)\rangle \otimes |yx\rangle + \left|c_{yx}^{1}c_{yx}^{0}c_{yx}^{6}c_{yx}^{5}c_{yx}^{3}c_{yx}^{4}c_{yx}^{7}c_{yx}^{2}\right\rangle \otimes |YX\rangle \end{aligned} \tag{13}$$

To achieve bit-planes permutation of all the pixels, the following quantum operation H should be implemented.

$$
\begin{aligned}
H\left(|I_b\rangle\right) &= \prod_{Y=0}^{2^n-1}\prod_{X=0}^{2^n-1} H_{YX}\left(|I_b\rangle\right) \\
&= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\left|c_{YX}^{1}c_{YX}^{0}c_{YX}^{6}c_{YX}^{5}c_{YX}^{3}c_{YX}^{4}c_{YX}^{7}c_{YX}^{2}\right\rangle \otimes |YX\rangle \\
&= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}\left|C'(y,x)\right\rangle|yx\rangle = \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}\left|c_{yx}^{7\prime}c_{yx}^{6\prime}c_{yx}^{5\prime}c_{yx}^{4\prime}c_{yx}^{3\prime}c_{yx}^{2\prime}c_{yx}^{1\prime}c_{yx}^{0\prime}\right\rangle|yx\rangle = \left|I_k\right\rangle
\end{aligned}
\tag{14}
$$

After bit-level permutation, the quantum image is further scrambled and the obtained image is denoted as $|I_k\rangle$. Take the image "boat" as an example, the bit-plane permutated image is shown in Fig. 9, from which can be seen that the visual information is meaningless.

3.3 Pixel-level diffusion

The aim of pixel-level diffusion is to make the pixels distribute uniformly and this stage is completed with logistic map. Firstly, a pseudo-random sequence $\left\{s_2(l) \in (0,1), l = 1, \ldots, N+1, N+2 \ldots N+2^{2n}\right\}$ is generated using Eq. (7), where the control parameter is α set to 3.99999 and the initial value χ_0 is set through the information of plaintext information in order to resist chosen-plaintext attack.

$$
\chi_0 = \frac{\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}\left(|C(y,x)|\right)}{2^8 \times 2^{2n}} \tag{15}
$$

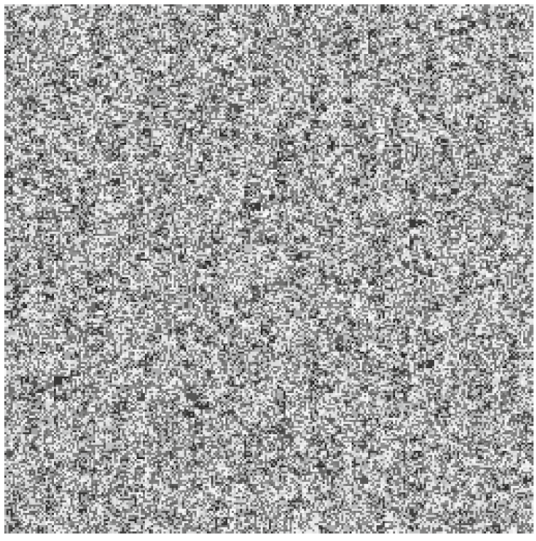


Fig. 9 The bit-level permutation result of image "boat"

Then, the former N numbers are also discarded to avoid transient effect, and then, the remaining elements of sequence $\{s_2(l)\}$ are transformed to integers.

$$S_2(l) = \text{floor}\left(s(l) \times 10^{15}\right) \bmod 256 \tag{16}$$

where the function floor$(\cdot)$ represents the operation of rounded down.

The ciphertext $|I_e\rangle$ can be finally obtained through implementing XOR operation between the pseudo-random sequence $|S_2\rangle$ and bit-level permutated image $|I_k\rangle$. The corresponding quantum realization circuit is shown in Fig. 10.

$$\begin{aligned} |I_e\rangle &= |I_k\rangle \oplus |S_2\rangle \\ &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |C'(y,x) \oplus S_2(y,x)\rangle |yx\rangle \\ &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |E(y,x)\rangle |yx\rangle \\ &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} \left|e_{yx}^7 e_{yx}^6 e_{yx}^5 e_{yx}^4 e_{yx}^3 e_{yx}^2 e_{yx}^1 e_{yx}^0\right\rangle |yx\rangle \end{aligned} \tag{17}$$

3.4 Quantum image decryption scheme

As the quantum operations are invertible, the decryption process is exactly the inverse process of encryption. According to the diagram of quantum image encryption scheme, the corresponding decryption flowchart is shown in Fig. 11 and the detailed decryption procedures are described as follows:

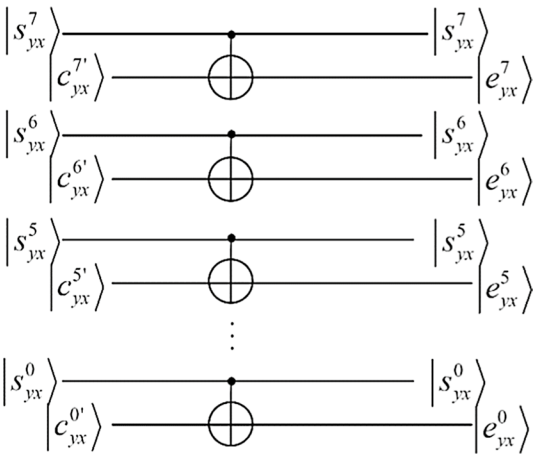


Fig. 10 The quantum circuit for pixel-level diffusion

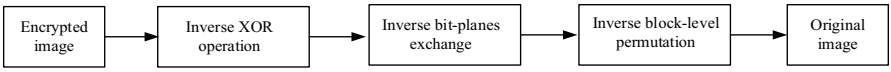


Fig. 11 The decryption process of the proposed scheme

Step 1. By using the same parameter and initial value χ_0 as the encryption scheme, the integer sequence $S_2(l)$ is obtained. Then, the encrypted image $|I_e\rangle$ is XORed with S_2 to retrieve the bit-level permutated image $|I_k\rangle$.

$$\begin{aligned}|I_k\rangle &= |I_e\rangle \oplus |S_2\rangle \\ &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}\left|e_{yx}^7 e_{yx}^6 e_{yx}^5 e_{yx}^4 e_{yx}^3 e_{yx}^2 e_{yx}^1 e_{yx}^0 \oplus S_2(y,x)\right\rangle |yx\rangle \\ &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\left|c_{YX}^1 c_{YX}^0 c_{YX}^6 c_{YX}^5 c_{YX}^3 c_{YX}^4 c_{YX}^7 c_{YX}^2\right\rangle \otimes |YX\rangle\end{aligned} \tag{18}$$

Step 2. The inverse bit-planes exchange operation H^{-1} is implemented on $|I_k\rangle$ to obtain the block-level permutated image $|I_b\rangle$.

$$\begin{aligned}H^{-1}\left(|I_k\rangle\right) &= \prod_{Y=0}^{2^n-1}\prod_{X=0}^{2^n-1} H_{YX}^{-1}\left(|I_k\rangle\right) \\ &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1} G_{YX}^{-1}\left|c_{YX}^1 c_{YX}^0 c_{YX}^6 c_{YX}^5 c_{YX}^3 c_{YX}^4 c_{YX}^7 c_{YX}^2\right\rangle \otimes |YX\rangle \\ &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}\left|c_{yx}^7 c_{yx}^6 c_{yx}^5 c_{yx}^4 c_{yx}^3 c_{yx}^2 c_{yx}^1 c_{yx}^0\right\rangle \otimes |yx\rangle = |I_b\rangle\end{aligned} \tag{19}$$

Step 3. The original image can be recovered by performing inverse QArT on quantum image $|I_b\rangle$ according to the parameters used in the encryption.

$$\begin{aligned}|I\rangle = \mathrm{QArT}^{-1}\left(|I_b\rangle\right) &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|C(y,x)\rangle \otimes \mathrm{QArT}^{-1}\left(\left|y'_{n-1}y'_{n-2}\cdots y'_w y_{w-1}\cdots y_2y_1y_0\right\rangle\left|x'_{n-1}x'_{n-2}\cdots x'_w x_{w-1}\cdots x_2x_1x_0\right\rangle\right) \\ &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|C(y,x)\rangle \otimes \mathrm{QArT}^{-1}\left(\left|y'_{n-1}y'_{n-2}\cdots y'_w\right\rangle\right)|y_{w-1}\cdots y_2y_1y_0\rangle\mathrm{QArT}^{-1}\left(\left|x'_{n-1}x'_{n-2}\cdots x'_w\right\rangle\right)|x_{w-1}\cdots x_2x_1x_0\rangle \\ &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|C(y,x)\rangle \otimes \left|y_{n-1}y_{n-2}\cdots y_w y_{w-1}\cdots y_2y_1y_0\right\rangle\left|x_{n-1}x_{n-2}\cdots x_w x_{w-1}\cdots x_2x_1x_0\right\rangle \\ &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|C(y,x)\rangle \otimes |yx\rangle\end{aligned} \tag{20}$$

4 Numerical simulation results and security analysis

Since the quantum computers are not available at present to store and manipulate quantum states, the experiments are simulated with MATLAB on a classical computer. The quantum states and operations can be easily simulated with complex vectors and unitary matrices. The keys of the proposed scheme include the block size, the iteration parameter of QArT, the order of bit-planes and the parameters of logistic map. The relevant parameters are set as follows: There are two iterations in the stage of block-level permutation, and the block size is set to $w_1 = 8$ and $w_2 = 4$ in the first and second iterations, respectively. The parameters of Arnold in the first and second iteration are set to $r_1 = 20$ and $r_2 = 38$, respectively. In the stage of bit-level permutation, the control parameter of logistic map is set to $\alpha = 3.99999$ and the initial value χ_0 is set to 0.5. The test images "Elaine", "Lake", "Peppers" and "Cameraman" with size of 256×256 are shown in Fig. 12a–d. The corresponding encryption and decryption results of tested images are shown in Fig. 12e–h, i–l, respectively. It can be seen from experimental results that any useful information cannot be recovered from the encrypted images, which verify that the proposed scheme has good encryption effect.

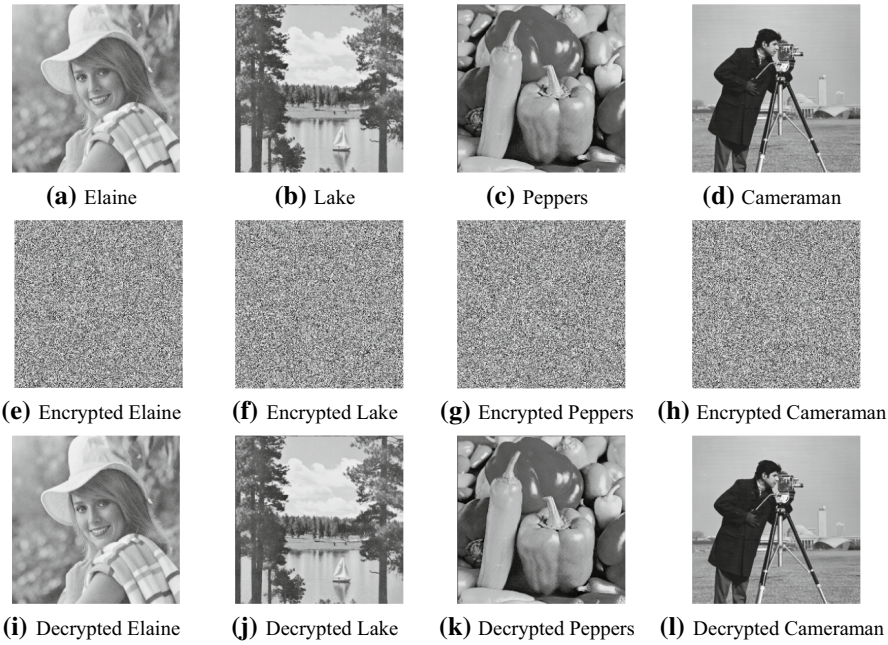


Fig. 12 The encryption and decryption results of tested images

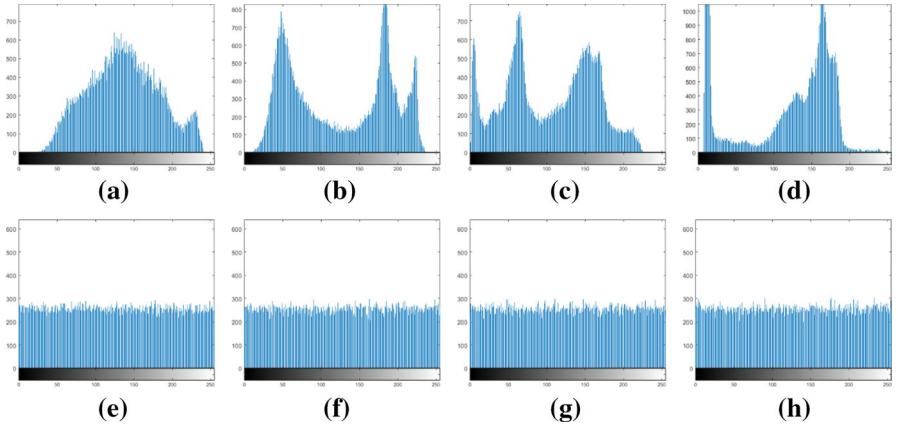


Fig. 13 Histograms of **a** Elaine, **b** Lake, **c** Peppers, **d** Cameraman, **e** Encrypted Elaine, **f** Encrypted Lake, **g** Encrypted Peppers, **h** Encrypted Cameraman

Table 1 The histogram variances of plaintext images and ciphertext images

Images	Plaintext image	Ciphertext image
Elaine	35,301.8359	**211.0625**
Lake	44,650.5937	**269.2578**
Peppers	34,877.9687	**271.0625**
Cameraman	110,973.3046	**283.6589**

4.1 Statistical analysis

4.1.1 Histogram analysis

Image histogram reflects the gray value distribution, which is an important statistical feature. For a good image encryption scheme, the histogram of ciphertext image should be uniform. Figure 13a–d shows the histograms of plaintext images, and corresponding histograms of ciphertext images are shown in Fig. 13e–h. The histograms of the original images are very different, but the histograms of the ciphertext are similar, which indicates that the attackers cannot obtain useful information from statistical analysis.

In addition, the histogram variances defined as follows are used to measure the uniform distribution of plaintext images and ciphertext images.

$$\mathrm{var}(\mathrm{hist}) = \frac{1}{256 \times 256} \sum_{i=0}^{255} \sum_{j=0}^{255} \frac{1}{2} \left(\mathrm{hist}_i - \mathrm{hist}_j\right)^2 \tag{21}$$

where hist_i and hist_j denote the pixel number that gray value equal to i and j, respectively. Table 1 shows the histogram variances of plaintext images and ciphertext images. For the convenience of comparison, the histogram variances of ciphertext

images are highlighted in bold. It can be seen from table that the histograms of plaintext images distribute not even, but the ciphertext images have uniformly distributed histograms. The quantitative results further verify that the proposed scheme can resist histogram attack.

4.1.2 Correlation between adjacent pixels

The correlation between adjacent pixels in a natural image is strong; therefore, the corresponding ciphertext images should have sufficiently low correlation between adjacent pixels. The correlation coefficient (CC) defined as follows is generally calculated to evaluate the correlation between the adjacent pixels in horizontal, vertical and diagonal directions.

$$\mathrm{CC} = \frac{\sum_{u=1}^{2^n} \left(x_u - \bar{x}\right)\left(y_u - \bar{y}\right)}{\sqrt{\sum_{u=1}^{2^n} \left(x_u - \bar{x}\right)^2 \sum_{u=1}^{N} \left(y_u - \bar{y}\right)^2}} \tag{22}$$

where x_u and y_u denote pixel values of a pair adjacent pixels. The $\bar{x}$ and $\bar{y}$ represent the average value of variables x and y. Table 2 lists the CC values of plaintext and ciphertext images in three directions, the CC values of encrypted images are highlighted in bold, from which can be seen that the CC values of original images are close to 1 and the CC values of ciphertext images are close to 0. Therefore, the correlation of the adjacent pixels is decreased in the ciphertext images.

Take the image "Elaine" as an example, by randomly selecting 10,000 pairs of adjacent pixels in original and ciphertext images, the correlation distribution in three directions is shown in Fig. 14. It is obvious seen from Fig. 14d–f that there is almost no correlation between adjacent pixels and therefore, the proposed scheme can resist correlation attack.

Table 2 The CC values of plaintext and ciphertext images in three directions

Correlation coefficient	Horizontal direction	Vertical direction	Diagonal direction
Elaine	0.9693	0.9432	0.9185
Encrypted Elaine	**0.0005**	**− 0.0133**	**0.0419**
Lake	0.9302	0.9298	0.8987
Encrypted Lake	**− 0.0036**	**− 0.0295**	**− 0.0174**
Peppers	0.9479	0.9105	0.8621
Encrypted Peppers	**0.0295**	**0.0187**	**0.0393**
Cameraman	0.9793	0.9789	0.9562
Encrypted Cameraman	**− 0.0279**	**− 0.0062**	**− 0.0089**

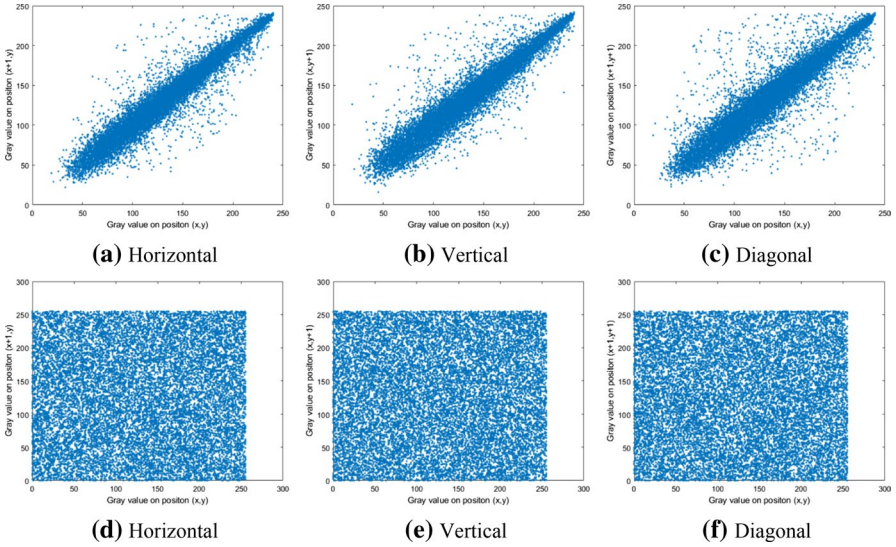


Fig. 14 **a**–**c** Correlation distribution in three directions of original images, **d**–**f** correlation distribution in three directions of ciphertext images

4.1.3 Information entropy

The information entropy (IE) defined as follows can describe the statistical feature of uncertainty. The probability of gray value i is $P(i)$ and the corresponding IE can be calculated as:

$$\mathrm{IE} = -\sum_{i=0}^{255} P(i)\log_2 P(i) \tag{23}$$

If the gray values distribute randomly, the information entropy is close to 8. The information entropy of the plaintext images and ciphertext images is listed in Table 3. For the convenience of comparison, the entropy of ciphertext images are highlighted in bold. It can be seen from table that information entropy encrypted image is very close to ideal value, and therefore, the proposed scheme can resist entropy attack.

Table 3 The information entropy of the plaintext images and ciphertext images

Images	Plaintext image	Ciphertext image
Elaine	7.5046	**7.9977**
Lake	7.4898	**7.9970**
Peppers	7.5693	**7.9970**
Cameraman	7.0097	**7.9969**

4.1.4 Fourier spectrum analysis

To further analyze the statistical property of ciphertext images, the spectrums of which are plotted in Fig. 15. In addition, the spectrums of plaintext images are also depicted and compared. It can be easily seen that after the encryption process, the spectrum amplitude becomes extremely uniform. Therefore, the attackers cannot achieve useful statistical information from Fourier spectrums of ciphertext images.

4.2 Key sensitivity analysis

For a satisfactory image encryption scheme, a slight change of key will lead to the failure of obtaining original information. The image "Lake" is taken as an example to test the key sensitivity. The decrypted image with correct keys shown in Fig. 16a–e shows the decrypted image by slightly changing one key and keep other keys correct. The decryption results by changing the Arnold parameter in two iterations are shown in Fig. 16b, c, from which can be seen that the block information is still cannot recognized. By changing the block size in two iterations, the decrypted images are shown in Fig. 16d, e, from which can be seen that decrypted images are still permutated. The decryption with random bit-planes order is shown in Fig. 16f, and the decrypted images is noise-like. The parameters deviation of logistic map will also cause the noise-like decryption results as shown in Fig. 16g, h, where the deviation of α is 10^{-15} and the deviation of χ_0 is 10^{-16}. Based on the analysis above, it can be seen from experimental results that the keys in the proposed scheme is sensitive.

4.3 Key space analysis

To resist brute-force attack, the key space of the image encryption scheme should be large enough. In the proposed scheme, the total keys include the parameter of QArT, the order of bit-planes and the parameters of logistic map. If the block size is set to

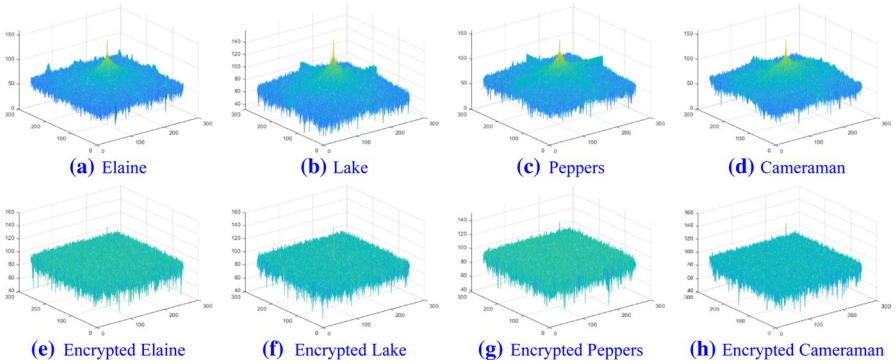


Fig. 15 Spectrums of plaintext and ciphertext images

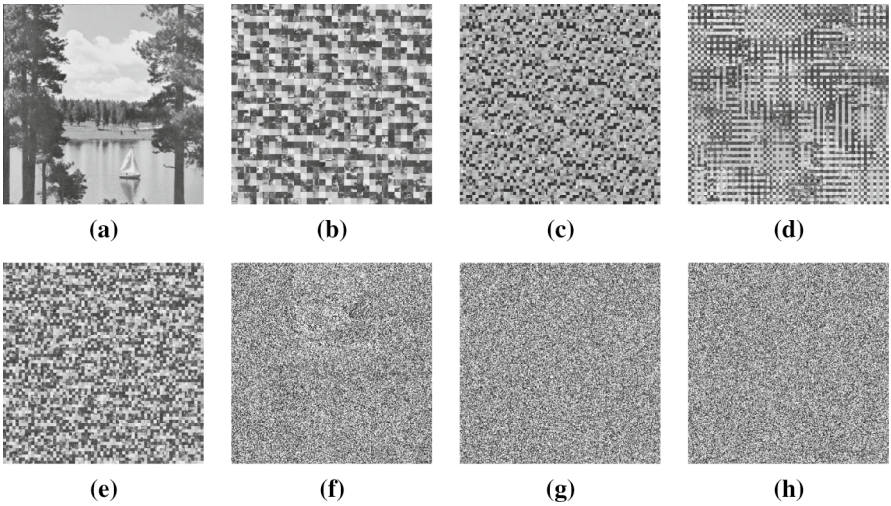


Fig. 16 The decrypted images with correct keys and incorrect keys

4, the period of QArT is 48 for an image sized 256×256. The possible orders of bit-planes are about 8!. The valid precision of logistic map parameters including control parameter and initial value is up to 10^{-15}, and therefore, the key space is more than 10^{30}. As the keys are independent, the overall key space of the proposed scheme is about $48^2 \times 8! \times 10^{30} > 2^{100}$, which is safe under current computation ability.

4.4 Noise attack

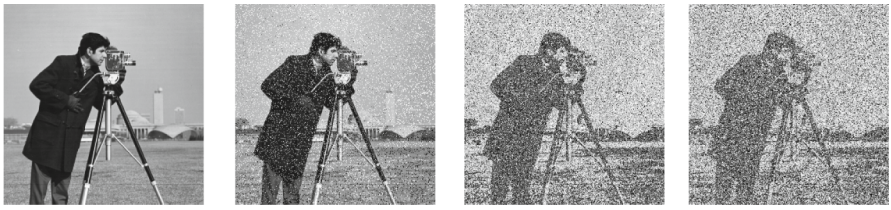
During the transmission process of ciphertext image, it is usually influenced with noises. Therefore, the encryption algorithm should robust to resist noise attack. In the experiment, Gaussian random noise G with zero mean and standard deviation is added on the encrypted image and k is used to represent the noise strength. The ciphertext with noise is denoted as:

$$I'_e = I_e + kG \tag{24}$$

The image cameraman is used to simulate the retrieval result of noisy ciphertext, and the corresponding decrypted images are shown in Fig. 17a–d. The decrypted images are become more and more fuzzy with the increase in k, but the main content can still be recognized. As a result, the proposed quantum image encryption scheme is robust to resist noise attack.

4.5 Computational complexity

The proposed quantum image encryption scheme includes three main procedures, and therefore, the computational complexity mainly depends on the QArT, bit-planes permutation and XOR operation. Generally, the complexity of quantum



(a) $k = 0$ **(b)** $k = 1$ **(c)** $k = 10$ **(d)** $k = 20$

Fig. 17 The decrypted images with different noise strength

algorithm is calculated with the number of logical gates. In the block-level permutation stage, the QArT containing ADDER module and ADDER-MOD module is implemented, where the complexity of ADDER module is $28n - 12$ and complexity of the ADDER-MOD module is about $140n$ [40]. Therefore, the computational complexity of the QArT is $O(n)$. In the bit-plane permutation stage, the swap gates are used and each swap gate contains 3 CNOT gates. As the quantum computation has parallel characteristic, the is also $O(n)$. In the pixel-level permutation, the XOR operation is accomplished with a $2n$ - CNOT gate, which contains $128n - 256$ basic gates. Thus, the computational complexity of bit-level permutation stage is $O(n)$. Therefore, it is easy to draw a conclusion that the whole computational complexity of the proposed scheme is $O(n)$. In comparison, the complexity of same operations in the classical image encryption algorithm is $O\left(2^{2n}\right)$; therefore, the quantum algorithm has a superior performance in terms of computational complexity.

5 Conclusion

In this paper, an efficient three-level quantum image encryption scheme is presented based on QArT and logistic map. To improve the security of the proposed algorithm, three-level quantum image encryption scheme including block-level permutation, bit-level permutation and pixel-level diffusion is designed and corresponding quantum circuits are given. To make up the period defect of QArT, an iteration framework for block-level permutation is proposed. By setting different block-size and different parameter of QArT, the key-space is dramatically increased. The order of bit-level is random scrambled according to the pseudo-random sequence generated with logistic map. In addition, the pixel-level diffusion is accomplished with XOR operation between bit-level permutated image and a pseudo-random sequence acquired from logistic map. The introduction of logistic map not only simplifies the keys transmission but also enhances the security of the proposed scheme. Numerical simulations results and theoretical analysis show that the proposed three-level quantum image encryption scheme has high level of security and efficiency.

The proposed three-level quantum image encryption algorithm achieves good performance in security and efficiency, and this encryption frame can still be improved such as enlarge the key space in block permutation stage. The main emphasis of our

future research will be the design of quantum permutation transforms superior to Arnold transform.

Acknowledgements The work was funded by the National Natural Science Foundation of China (Grant Nos. 61802037, 61572089), 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. cquyjg18219) and the Fundamental Research Funds for the Central Universities (Grant Nos. 106112017CDJQJ188830, 106112017CDJXY180005).

References

1. Cai, J., Gu, S., Zhang, L.: Learning a deep single image contrast enhancer from multi-exposure images. IEEE Trans. Image Process **27**(4), 2049 (2018)
2. Li, Y.C., Zhou, R.G., Xu, R.Q., Luo, J., Hu, W.W.: A quantum deep convolutional neural network for image recognition. Quant. Sci. Technol. **5**(4), 044003 (2020)
3. Li, Y.C., Zhou, R.G., Xu, R.Q., Luo, J., Jiang, S.: A quantum mechanics-based framework for EEG signal feature extraction and classification. IEEE Trans. Emerg. Top Comput. (2020). https://doi.org/10.1109/TETC.2020.3000734
4. Hua, Z., Jin, F., Xu, B., Huang, H.: 2D Logistic-sine-coupling map for image encryption. Signal Process. **149**, 148 (2018)
5. Parvaz, R., Zarebnia, M.: A combination chaotic system and application in color image encryption. Opt. Laser Technol. **101**, 30 (2018)
6. Muhammad, K., Hamza, R., Ahmad, J., et al.: Secure surveillance framework for IoT systems using probabilistic image encryption. IEEE Trans. Ind. Inf. **14**(8), 3679 (2018)
7. Zhou, N., Hu, Y., Gong, L., Li, G.: Quantum image encryption scheme with iterative generalized Arnold transforms and quantum image cycle shift operations. Quant. Inf. Process **16**(6), 164 (2017)
8. Liu, X., Mei, W., Du, H.: Simultaneous image compression, fusion and encryption algorithm based on compressive sensing and chaos. Opt. Comm. **366**, 22 (2016)
9. Özkaynak, F.: Brief review on application of nonlinear dynamics in image encryption. Nonlinear Dyn. **92**(2), 305 (2018)
10. Abura'ed, N., Khan, F.S., Bhaskar, H.: Advances in the quantum theoretical approach to image processing applications. ACM Comput. Surv. **49**(4), 75 (2017)
11. Le, P.Q., Dong, F., Hirota, K.: A flexible representation of quantum images for polynomial preparation, image compression, and processing operations. Quant. Inf. Process **10**(1), 63 (2011)
12. Zhang, Y., Lu, K., Gao, Y., et al.: NEQR: a novel enhanced quantum representation of digital images. Quant. Inf. Process **12**(8), 2833 (2013)
13. Li, H., Zhu, Q., Zhou, R., et al.: Multi-dimensional color image storage and retrieval for a normal arbitrary quantum superposition state. Quant. Inf. Process **13**(4), 991 (2014)
14. Li, H., Song, S., Fan, P., Peng, H., Liang, Y.: Quantum vision representations and multi-dimensional quantum transforms. Inf. Sci. **502**, 42 (2019)
15. 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. Quant. Inf. Process **14**(4), 1193 (2015)
16. Khan, M., Rasheed, A.: Permutation-based special linear transforms with application in quantum image encryption algorithm. Quant. Inf. Process **18**(10), 298 (2019)
17. Zhou, R.G., Sun, Y.J., Fan, P.: Quantum image gray-code and bit-plane scrambling. Quant. Inf. Process **14**(5), 1717 (2015)
18. Li, X.-Z., Chen, W.-W., Wang, Y.-Q.: Quantum image compression-encryption scheme based on quantum discrete cosine transform. Int. J. Theor. Phys. **57**(9), 2904 (2018)
19. 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. **345**, 257 (2016)
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. **52**(6), 1802 (2012)

21. Liang, H.R., Tao, X.Y., Zhou, N.R.: Quantum image encryption based on generalized affine transform and logistic map. Quant. Inf. Process **15**(7), 2701 (2016)
22. Zhu, H.H., Chen, X.B., Yang, Y.X.: A quantum image dual-scrambling encryption scheme based on random permutation. Sci. Chin. Inf. Sci. **62**(12), 229501 (2019)
23. Yang, Y.G., Xia, J., Jia, X., et al.: Novel image encryption/decryption based on quantum fourier transform and double phase encoding. Quant. Inf. Process **12**(11), 3477 (2013)
24. Du, S., Qiu, D., Mateus, P., et al.: Enhanced double random phase encryption of quantum images. Results Phys. **13**, 102161 (2019)
25. Hu, W.W., Zhou, R.G., Luo, J., et al.: Quantum image encryption algorithm based on Arnold scrambling and wavelet transforms. Quant. Inf. Process **19**, 82 (2020)
26. Li, H.S., Li, C.Y., Chen, X., et al.: Quantum image encryption based on phase-shift transform and quantum Haar wavelet packet transform. Mod. Phys. Lett. A **34**(26), 1950214 (2019)
27. Wang, L., Ran, Q., Ma, J.: Double quantum color images encryption scheme based on DQRCI. Multimed. Tools Appl. **79**, 6661 (2020)
28. Liu, X., Xiao, D., Liu, C.: Double quantum image encryption based on Arnold transform and qubit random rotation. Entropy **20**(11), 867 (2018)
29. Heidari, S., Naseri, M., Nagata, K.: Quantum selective encryption for medical images. Int. J. Theor. Phys. **58**, 3908 (2019)
30. Jiang, N., Dong, X., Hu, H., et al.: Quantum image encryption based on Henon mapping. Int. J. Theor. Phys. **58**, 979 (2019)
31. Zhou, N., Chen, W., Yan, X., et al.: Bit-level quantum color image encryption scheme with quantum cross-exchange operation and hyper-chaotic system. Quant. Inf. Process **17**, 137 (2018)
32. Luo, Y., Tang, S., Liu, J., et al.: Image encryption scheme by combining the hyper-chaotic system with quantum coding. Opt. Lasers Eng. **124**, 105836 (2020)
33. Zhou, N.R., Huang, L.X., Gong, L.H., et al.: Novel quantum image compression and encryption algorithm based on DQWT and 3D hyper-chaotic Henon map. Quant. Inf. Process **19**, 284 (2020)
34. Musanna, F., Kumar, S.: Image encryption using quantum 3-D Baker map and generalized gray code coupled with fractional Chen's chaotic system. Quant. Inf. Process **19**(8), 220 (2020)
35. Wang, X., Liu, L., Zhang, Y.: A novel chaotic block image encryption algorithm based on dynamic random growth technique. Opt. Lasers Eng. **66**, 10–18 (2015)
36. Chai, X., Gan, Z., Zhang, M.: A fast chaos-based image encryption scheme with a novel plain image-related swapping block permutation and block diffusion. Multimed. Tools Appl. **76**(14), 15561–15585 (2017)
37. Ye, G., Zhou, J.: A block chaotic image encryption scheme based on self-adaptive modelling. Appl. Soft Comput. **22**, 351–357 (2014)
38. Jiang, N., Wu, W.Y., Wang, L.: The quantum realization of Arnold and Fibonacci image scrambling. Quant. Inf. Process **13**(5), 1223 (2014)
39. Yang, T., Wu, C.W., Chua, L.O.: Cryptography based on chaotic systems. IEEE Trans. Circuits Syst. I Fundam. Theor. Appl. **44**(5), 469 (1997)
40. Jiang, N., Wang, L.: Analysis and improvement of the quantum arnold image scrambling. Quant. Inf. Process **13**(7), 1545 (2014)