Novel quantum secret image sharing scheme*

Gao-Feng Luo(罗高峰)[1,2,3], Ri-Gui Zhou(周日贵)[1,3,†], and Wen-Wen Hu(胡文文)[1,3]

[1] College of Information Engineering, Shanghai Maritime University, Shanghai 201306, China
[2] College of Information Engineering, Shaoyang University, Shaoyang 422000, China
[3] Research Center of Intelligent Information Processing and Quantum Intelligent Computing, Shanghai 201306, China

(Received 3 December 2018; revised manuscript received 11 January 2019; published online 5 March 2019)

In this paper, we propose a novel quantum secret image-sharing scheme which constructs m quantum secret images into $m+1$ quantum share images. A chaotic image generated by the logistic map is utilized to assist in the construction of quantum share images first. The chaotic image and secret images are expressed as quantum image representation by using the novel enhanced quantum representation. To enhance the confidentiality, quantum secret images are scrambled into disordered images through the Arnold transform. Then the quantum share images are constructed by performing a series of quantum swap operations and quantum controlled-NOT operations. Because all quantum operations are invertible, the original quantum secret images can be reconstructed by performing a series of inverse operations. Theoretical analysis and numerical simulation proved both the security and low computational complexity of the scheme, which has outperformed its classical counterparts. It also provides quantum circuits for sharing and recovery processes.

Keywords: quantum image processing, secret image sharing, quantum computation, quantum circuit

PACS: 03.67.–a, 89.70.–a, 02.70.–c, 03.67.Lx **DOI:** 10.1088/1674-1056/28/4/040302

1. Introduction

Recent years have witnessed a rapid development in information technology. However, security problems of digital images are a major problem in transmitting vital images. A large number of real-time image processing tasks have brought new challenges to classical computers. Fortunately, quantum computation[1] brings hope for traditional information processing. A quantum computer has been demonstrated to have bright prospects as compared with the classical computer, particular with respect to Feynman's computation model,[2] Shor's integer factoring algorithm,[3] and Grover's database searching algorithm.[4]

With the development of quantum computation, an emerging branch, *i.e.*, quantum image processing (QIP)[5,6] is attracting more and more attention. It focuses on extending classical image processing tasks and operations to the quantum computation framework. Available literature on QIP can be classified into two groups. In the first, methods to represent quantum images have been proposed, such as a flexible representation of quantum images,[7] a novel enhanced quantum representation (NEQR) of the digital image model,[8] and a normal arbitrary quantum superposition state.[9] In the second, QIP algorithms have been investigated, such as quantum image scaling,[10,11] quantum image matching,[12,13] quantum image steganography,[14–16] and quantum image watermarking.[17–20] In particular, quantum image encryption[21–24] has begun to draw increasing attention in recent years. For example, in Ref. [21], a novel image encryption scheme based on quantum walks was proposed, which opens the door towards introducing quantum computation into image encryption. In Ref. [22], a novel quantum grayscale image encryption algorithm based on one-dimensional quantum cellular automata was proposed. The proposal has outperformed its classical counterpart in terms of security and computational complexity.

Just as the research on quantum image encryption has become an attractive field, quantum secret sharing,[25–28] which is an important branch of quantum communication,[29] also attracts increasing attention nowadays. From a historical viewpoint, Naor and Shamir[30] presented a visual secret-sharing scheme first which encrypts a secret binary image into n meaningless share images such that the information of the secret image can be decrypted by superimposing all n share images. After that, secret sharing has become a favorite research topic, especially quantum schemes. Theoretically, as a quantum image is still a quantum state, it can also be shared. Quantum secret image sharing, different from traditional secret sharing, is sharing entangled states of a quantum image. To the best of our knowledge, few papers have been published on this issue previously. For example, a novel and flexible quantum image secret-sharing scheme was proposed,[31] which generates shares via measurement operations on the secret image. Two efficient remote medical image-sharing schemes were

*Project supported by the National Key Research and Development Plan (Grant Nos. 2018YFC1200200 and 2018YFC1200205), the National Natural Science Foundation of China (Grant No. 61463016), and the "Science and Technology Innovation Action Plan" of Shanghai in 2017 (Grant No. 17510740300).

†Corresponding author. E-mail: rgzhou@shmtu.edu.cn

© 2019 Chinese Physical Society and IOP Publishing Ltd

proposed,[32] which utilize quantum information hiding techniques. Obviously, the research on quantum image sharing is deficient at present. Inspired by the above-mentioned schemes of quantum image processing techniques, this paper mainly focuses on quantum secret image sharing, which constructs m quantum secret images into $m+1$ quantum share images.

The rest of this paper is organized as follows. Section 2 gives some preliminaries related to the work. Section 3 is devoted to the proposed scheme. Simulation-based experiments and an analysis are presented in Section 4. Finally, Section 5 draws conclusions.

2. Preliminaries

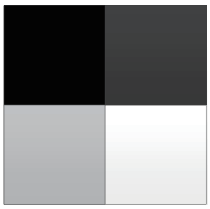
2.1. NEQR

The novel enhanced quantum image representation (NEQR) of digital images[8] using two entangled qubit sequences integrates quantum image information, including coordinates position and color information, into a normalized superposition quantum state. For a $2^n \times 2^n$ quantum image with grayscale ranged $[0, 2^q - 1]$, the representative expression of the NEQR image is expressed as:

$$\begin{aligned} |I\rangle &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|f(Y,X)\rangle|YX\rangle \\ &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\bigotimes_{i=0}^{q-1}\left|C_{YX}^{i}\right\rangle|YX\rangle, \end{aligned} \tag{1}$$

where the q-qubit sequence $\left|C_{YX}^{i}\right\rangle = \left|c_{YX}^{q-1}\cdots c_{YX}^{1}c_{YX}^{0}\right\rangle$ encodes the color information and two n-qubit sequences of $|Y\rangle = |y_{n-1}\cdots y_1 y_0\rangle$ and $|X\rangle = |x_{n-1}\cdots x_1 x_0\rangle$ encode the position information in the vertical and horizontal directions, respectively.

To represent a quantum grayscale image, NEQR needs eight qubits encoding the pixel information, which have 256 grayscale densities. Figure 1 shows a quantum grayscale image and its NEQR expression.



$$\begin{aligned} |I\rangle &= \frac{1}{2}\big(|0\rangle\otimes|00\rangle + |200\rangle\otimes|10\rangle + |100\rangle\otimes|01\rangle + |255\rangle\otimes|11\rangle\big) \\ &= \frac{1}{2}\big(|00000000\rangle\otimes|00\rangle + |11001000\rangle\otimes|10\rangle \\ &\quad + |01100100\rangle\otimes|01\rangle + |11111111\rangle\otimes|11\rangle\big) \end{aligned}$$

Fig. 1. 2×2 quantum image and its NEQR expression (figure adapted from Ref. [8]).

2.2. Logistic map

As a classical algorithm, the logistic map plays an essential role in image encryption because of its high sensitivity to initial conditions, system parameters, and pseudo-random property. In the proposed quantum secret image-sharing scheme, the logistic map is used to generate pseudo-numbers, which are defined as

$$X_{\delta+1} = \mu X_\delta (1 - X_\delta), \tag{2}$$

where $\delta = 0, 1, \ldots, n$, X_0 is the initial value, $X_0 \in [0,1]$, $0 \le \mu \le 4$. When $3.57 \le \mu \le 4$, it can generate pseudo-random numbers within the range $(0,1)$.

2.3. Arnold transform

Arnold transform aims to transform an image into a meaningless one through permutation of the positions of the pixels into new positions. Assume that $I(X,Y)$ is an original image with a size of $2^n \times 2^n$, (X,Y) and (X',Y') are corresponding coordinates of pixels for the original image and the scrambled image, respectively. The Arnold transform can be defined as:

$$\begin{bmatrix} X' \\ Y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} X \\ Y \end{bmatrix} \bmod 2^n, \tag{3}$$

where $X' = (X+Y) \bmod 2^n, Y' = (X+2Y) \bmod 2^n$. The inverse Arnold transformation is

$$\begin{aligned} \begin{bmatrix} X \\ Y \end{bmatrix} &= \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}^{-1} \begin{bmatrix} X' \\ Y' \end{bmatrix} \bmod 2^n \\ &= \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} X' \\ Y' \end{bmatrix} \bmod 2^n. \end{aligned} \tag{4}$$

2.4. Basic quantum gate operations and related circuits

(i) Controlled-NOT operation

In quantum computers, the basic controlled operation is the controlled-NOT (CNOT), which is a quantum gate with two qubits, namely the control qubit and the target qubit (Fig. 2). In terms of the computational basis, the action of the CNOT is given by $|A\rangle|B\rangle \to |A\rangle|A \oplus B\rangle$. That is, if the control qubit is set to $|1\rangle$, the target qubit is flipped, otherwise the target qubit is left alone.

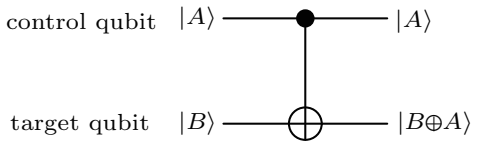


Fig. 2. Quantum CNOT gate.

(ii) Quantum swap gate

The quantum swap gate is a two-qubit gate, which can exchange two qubits. The corresponding quantum circuit is shown in Fig. 3.

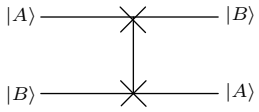


Fig. 3. Quantum swap gate.

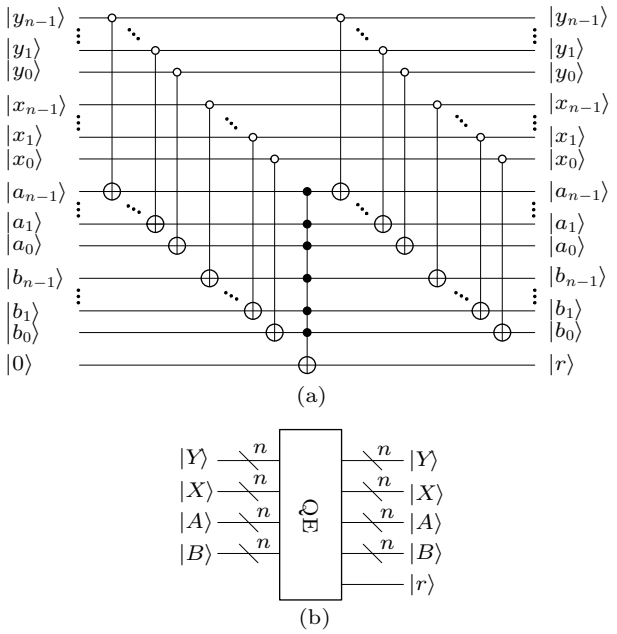


Fig. 4. (a) QE circuit and (b) simplified module of QE.

Zhou *et al.* designed the quantum equal (QE) circuit for comparing two qubit sequences.[33] The concrete quantum circuit and its simplified module are illustrated in Fig. 4, where $|Y\rangle = |y_{n-1}\ldots y_1 y_0\rangle$, $|X\rangle = |x_{n-1}\ldots x_1 x_0\rangle$, $|A\rangle = |a_{n-1}\ldots a_1 a_0\rangle$, $|B\rangle = |b_{n-1}\ldots b_1 b_0\rangle$. The output qubit $|r\rangle$ represents the compare result. If $|r\rangle = |1\rangle$, $|YX\rangle = |AB\rangle$; otherwise, $|YX\rangle \neq |AB\rangle$. Obviously, the QE module can be utilized to decide whether the coordinates of two quantum images of the same size are equal or not.

3. Proposed scheme

In this section, we will first provide a high-level description of our scheme. The intuition of our scheme using three phases including qubit scrambling, qubit swapping, and the qubit CNOT operation, is to share multiple quantum secret images. In the first phase, the original quantum secret images are scrambled by Arnold transform, which is often used as the image preprocessing method in information hiding. Furthermore, since a grayscale image can be decomposed into eight binary images, a quantum grayscale image also consists of eight binary qubits (*i.e.*, eight qubit planes). To make the shares random, qubit planes are swapped with the participation of the quantum chaos image. Finally, to enhance the security, the quantum CNOT operation is employed, which makes the secret completely random and secure. The process of quantum secret image sharing and recovery is outlined in Fig. 5. More specific details are discussed subsequently.

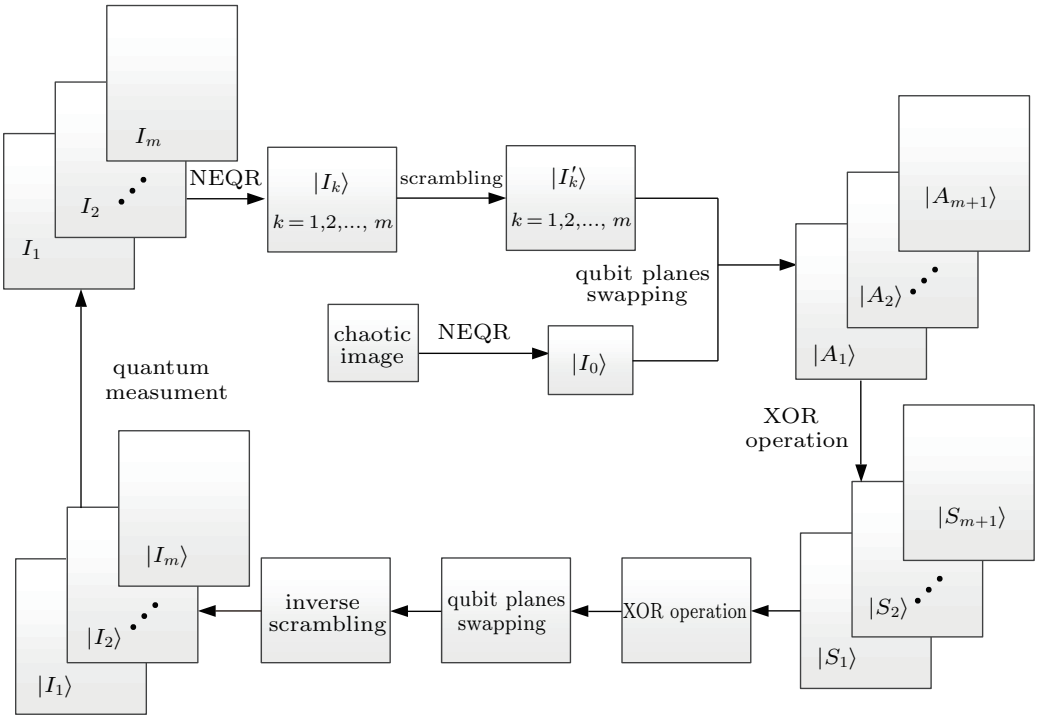


Fig. 5. Quantum secret image-sharing framework.

3.1. Sharing process

3.1.1. Preparation

Assume there are m secret images, named I_1, I_2, …, I_m, with the same dimensions $2^n \times 2^n$ and 8-bit grayscale. These secret images can be transformed into quantum states by using NEQR as follows:

$$\begin{aligned}&|I_k\rangle\\ &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|f_k(Y,X)\rangle|YX\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\bigotimes_{i=0}^{7}\left|C_{kYX}^{i}\right\rangle|YX\rangle\\ &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\left|C_{kYX}^{7}C_{kYX}^{6}C_{kYX}^{5}C_{kYX}^{4}C_{kYX}^{3}C_{kYX}^{2}C_{kYX}^{1}C_{kYX}^{0}\right\rangle|YX\rangle,\end{aligned} \tag{5}$$

where $k = 1,2,\ldots,m$. $|Y\rangle = |y_{n-1}\cdots y_1 y_0\rangle$ and $|X\rangle = |x_{n-1}\cdots x_1 x_0\rangle$ encode the position information in vertical and horizontal directions, respectively.

Meanwhile, in the proposed scheme, a meaningless chaotic image created by the logistic map is prepared. For logistic map $X_{\delta+1} = \mu X_\delta(1-X_\delta)$ and a given initial value X_0 and μ, we do 2^{2n} iterations. 2^{2n} numbers ranged $(0,1)$ are obtained. Then the normalization processing is carried out to generate a random matrix $R_o\{(i,j)\in[0,255], i=0,1,\ldots,2^n-1$, and $j=0,1,\ldots,2^n-1$. All values ranged [0, 255] would be viewed as the grayscale information of the chaotic image I_0. The chaotic image can be transformed into quantum states by using NEQR as follows:

$$\begin{aligned}|I_0\rangle &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|f_0(Y,X)\rangle|YX\rangle\\ &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\bigotimes_{i=0}^{7}\left|C_{0YX}^{i}\right\rangle|YX\rangle.\end{aligned} \tag{6}$$

Thus, m quantum secret images and a quantum chaotic image are prepared and utilized to construct $m+1$ quantum share images.

3.1.2. Arnold scrambling

To enhance the confidentiality, the original quantum secret image $|I_k\rangle$ $(k=1,2,\ldots,m)$ is scrambled into a disordered image $|I'_k\rangle$. In the proposed scheme, the main aim is to scramble the position of each pixel of the secret image. The quantum Arnold image scrambling in previous works[34,35] showed that it is a simple image scrambling method, with low computational complexity. Hence, Arnold scrambling is suitable for the proposed scheme. According to the classical Arnold transform introduced above, the quantum representation of the Arnold transform can be deduced. Here we define the Arnold transform as A (inverse Arnold transform as A^{-1}), the scrambled quantum secret image as $|I'_k\rangle$, and the process of scrambling can be defined as:

$$\begin{aligned}|I'_k\rangle = A|I_k\rangle &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\bigotimes_{i=0}^{7}\left|C_{kYX}^{i}\right\rangle A|YX\rangle\\ &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\bigotimes_{i=0}^{7}\left|C_{kYX}^{i}\right\rangle A|Y\rangle A|X\rangle\\ &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\bigotimes_{i=0}^{7}\left|C_{kYX}^{i}\right\rangle|Y'X'\rangle,\end{aligned} \tag{7}$$

where

$$\begin{cases}|Y'\rangle = |X+2Y\rangle \bmod 2^n,\\ |X'\rangle = |X+Y\rangle \bmod 2^n.\end{cases} \tag{8}$$

3.1.3. Qubit plane swapping

In this process, qubit planes of the scrambled quantum secret images and the quantum chaotic image are swapped in a predefined order. First, the coordinates of the quantum chaotic image $|I_0\rangle$ are compared with those of the scrambled quantum secret images $|I'_1\rangle$, $|I'_2\rangle$, …, and $|I'_m\rangle$ through QE modules. The quantum circuit for comparing the coordinates is designed as shown in Fig. 6, where the output qubits $|r_j\rangle$ $(j=1,2,\ldots,m)$ act as the control qubits. If all of the output qubits satisfy $|r_j\rangle = |1\rangle$, that is, the coordinate values of a certain pixel in all of the quantum images are equal, the following steps are performed.

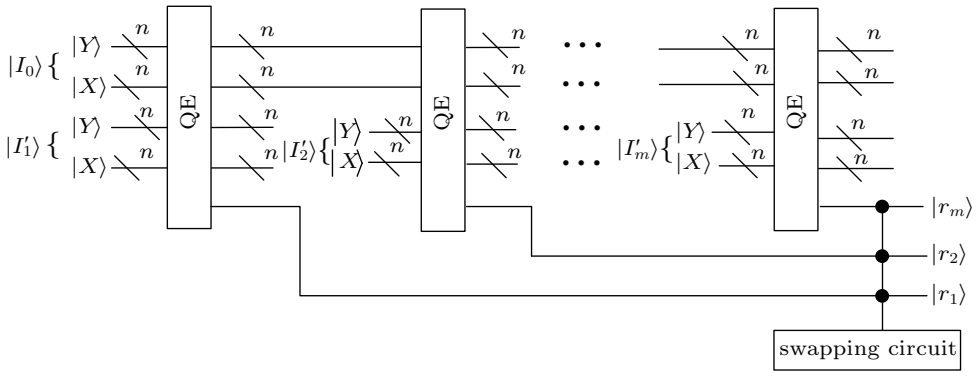


Fig. 6. Quantum circuit for the comparison with coordinates.

Step 1 Swap four most significant qubit (MSQb) planes of $|I_0\rangle$ with four least significant qubit (LSQb) planes of $|I'_1\rangle$.

Step 2 Swap four MSQb planes of $|I'_1\rangle$ with four LSQb planes of $|I'_2\rangle$.

Step 3 Swap four MSQb planes of $|I'_k\rangle$ with four LSQb planes of $|I'_{k+1}\rangle$ $(k = 2, \ldots, m-1)$.

Step 4 Swap four MSQb planes of $|I'_m\rangle$ with four LSQb planes of $|I_0\rangle$.

The quantum swapping circuit is illustrated in Fig. 7. It is not difficult to find that all the shares appear to be random after the swapping process of qubit planes. For convenience, we call them immediate shares, $|A_1\rangle$, $|A_2\rangle$, ..., and $|A_{m+1}\rangle$.

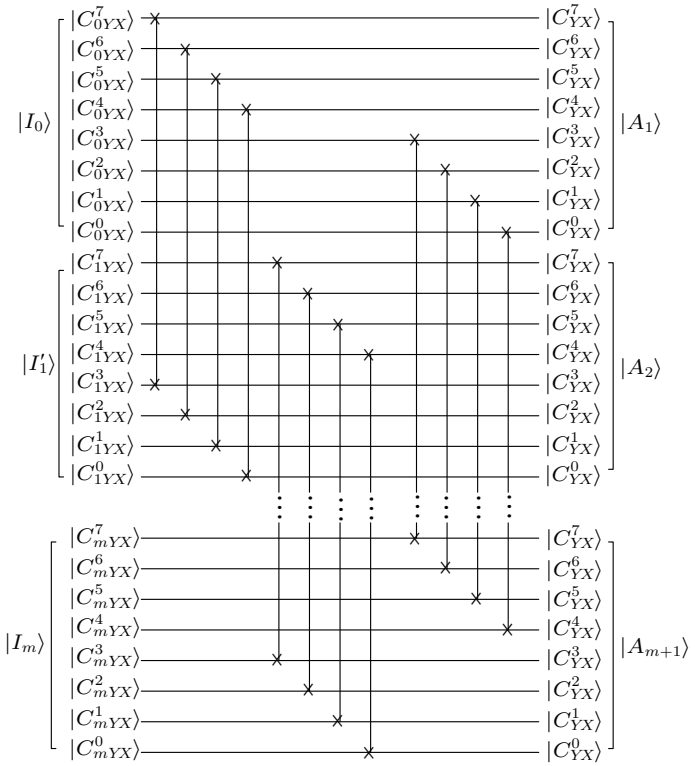


Fig. 7. Swapping circuit.

3.1.4. Quantum controlled-NOT operation

To obtain the final quantum share images, the quantum controlled-NOT operation (introduced in Subsection 2.4) is utilized to realize a quantum image XOR operation. We define

$$|S_1\rangle = |A_1\rangle, \quad |S_2\rangle = |A_1\rangle \oplus |A_2\rangle,$$
$$|S_3\rangle = |A_2\rangle \oplus |A_3\rangle, \ldots, \tag{9}$$

that is,

$$\begin{aligned} &|S_k\rangle = |A_k\rangle \ \text{ If } \ k = 1, \\ &|S_k\rangle = |A_{k-1}\rangle \oplus |A_k\rangle \ \text{ If } \ k = 2, 3, \ldots, m+1. \end{aligned} \tag{10}$$

For a quantum image with a size of $2^n \times 2^n$, the quantum controlled-NOT operations on grayscale information of every pixel can be divided into 2^{2n} sub-operations T_{YX}. It can be constructed by the controlled-NOT operation U_{YX} as follows:

$$T_{YX} = \left(I \otimes \sum_{y=0}^{2^n-1} \sum_{\substack{x=0 \\ yx \neq YX}}^{2^n-1} |yx\rangle \langle yx| \right) + U_{YX} \otimes |YX\rangle \langle YX|, \tag{11}$$

where T_{YX} is a unitary matrix and satisfies $T_{YX} T_{YX}^{\dagger} = I^{\otimes(2n+1)}$, and $T_{YX}^{\dagger}$ is the Hermitian conjugation matrix of T_{YX}. Obviously, each sub-operation can only implement the XOR operation on the grayscale information for its corresponding pixel. The XOR operations for quantum images are defined as

$$T = \prod_{Y=0}^{2^n-1} \prod_{X=0}^{2^n-1} T_{YX}. \tag{12}$$

As mentioned above, QE modules are also used to compare the coordinates of $|A_1\rangle$, $|A_2\rangle$, ..., and $|A_{m+1}\rangle$. The output qubits of the QE module act as the control qubits of the quantum image XOR operation circuit, which is shown in Fig. 8.

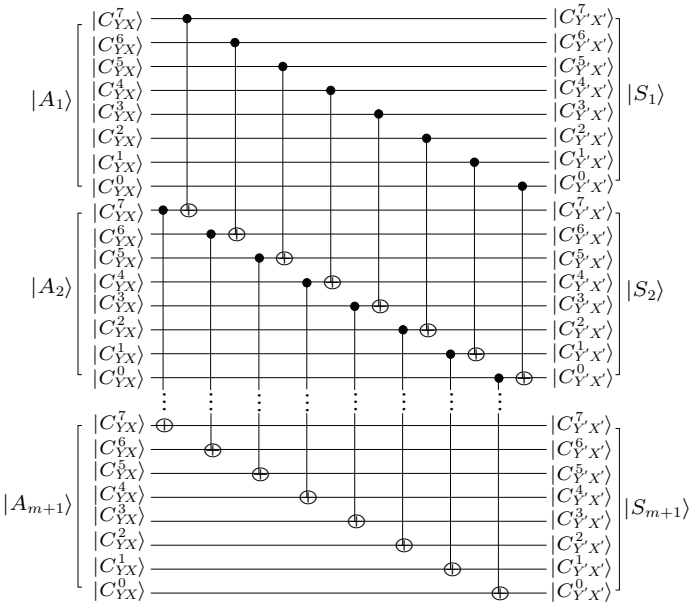


Fig. 8. Quantum image XOR operation.

3.2. Recovery process

All $m+1$ quantum share images collected together are used to reconstruct the original quantum secret images. The recovery process consists of four steps.

Step 1 To obtain the immediate shares, the controlled-NOT operation is also utilized to realize the quantum image XOR operation, as follows:

$$|A_1\rangle = |S_1\rangle, \quad |A_2\rangle = |S_1\rangle \oplus |S_2\rangle,$$
$$|A_3\rangle = |S_1\rangle \oplus |S_2\rangle \oplus |S_3\rangle \oplus \ldots, \tag{13}$$

that is

$$|A_k\rangle = |S_1\rangle \oplus |S_2\rangle \oplus \ldots \oplus |S_k\rangle, \tag{14}$$

where $k = 1, 2, \ldots, m+1$.

Step 2 Execute the reverse operation for qubit plane swapping, and the scrambled quantum secret images $|I'_1\rangle$, $|I'_2\rangle$, …, and $|I'_m\rangle$ are obtained.

Step 3 Perform the inverse Arnold transform A^{-1} on quantum images $|I'_1\rangle$, $|I'_2\rangle$, …, and $|I'_m\rangle$, the original quantum secret images $|I_1\rangle$, $|I_2\rangle$, …, and $|I_m\rangle$ are obtained.

Step 4 Quantum images $|I_1\rangle$, $|I_2\rangle$, …, and $|I_m\rangle$ are measured to obtain m classical digital images with 8-bit grayscale and a size of $2^n \times 2^n$.

3.3. A simple example

To demonstrate the computation steps in the sharing and recovery processes, we give a trivial example for $m = 2$. That is, two quantum secret images would be utilized to construct three quantum share images. Assume there are one chaos quantum image ($|I_0\rangle$) with a size of 2×2, and two scrambled quantum secret images ($|I'_1\rangle$ and $|I'_2\rangle$) with a size of 2×2, as shown in Figs. 9(a), 9(b), and 9(c), respectively.

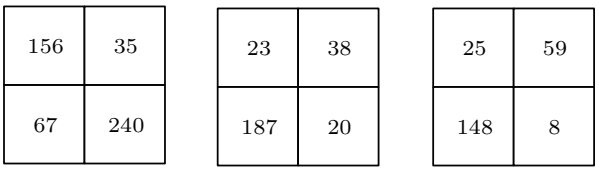


Fig. 9. An example of three quantum images.

The pixel values in their qubit form are shown as follows:

$$\begin{aligned}
&|I_0\rangle \ \{|\underline{1001}\ \overbrace{1100}\rangle, |0010\ 0011\rangle, |0100\ 0011\rangle, |1111\ 0000\rangle\},\\
&|I'_1\rangle \{|\underline{0001}\ \underline{0111}\rangle, |0010\ 0110\rangle, |1011\ 1011\rangle, |0001\ 0100\rangle\},\\
&|I'_2\rangle \{|\overbrace{0001}\ \underline{1001}\rangle, |0011\ 1011\rangle, |1001\ 0100\rangle, |0000\ 1000\rangle\}.
\end{aligned} \tag{15}$$

After the swapping circuit is executed, the intermediate quantum images are formed as follows:

$$\begin{aligned}
|A_1\rangle &= \{|\underline{0111}\ \overbrace{0001}\rangle, |0110\ 0011\rangle, |1011\ 1001\rangle, |0100\ 0000\rangle\},\\
|A_2\rangle &= \{|\underline{\underline{1001}}\ \underline{1001}\rangle, |1011\ 0010\rangle, |0100\ 0100\rangle, |1000\ 1111\rangle\},\\
|A_3\rangle &= \{|\overbrace{1100}\ \underline{\underline{0001}}\rangle, |0011\ 0010\rangle, |0011\ 1011\rangle, |0000\ 0001\rangle\}.
\end{aligned} \tag{16}$$

To describe the swapping process clearly, four MSQbs and LSQbs of the first pixel are tagged in Eqs. (15) and (16). Finally, three quantum share images $|S_1\rangle$, $|S_2\rangle$, and $|S_3\rangle$ can be obtained by using the quantum image XOR operation. The results are as follows:

$$\begin{aligned}
|S_1\rangle &= \{|0111\ 0001\rangle, |0110\ 0011\rangle, |1011\ 1001\rangle, |0100\ 0000\rangle\} = \{|113\rangle, |99\rangle, |185\rangle, |64\rangle\},\\
|S_2\rangle &= \{|1110\ 1000\rangle, |1101\ 0001\rangle, |1111\ 1101\rangle, |1100\ 1111\rangle\} = \{|232\rangle, |209\rangle, |253\rangle, |207\rangle\},\\
|S_3\rangle &= \{|0101\ 1000\rangle, |1000\ 0000\rangle, |0111\ 1111\rangle, |1000\ 1110\rangle\} = \{|88\rangle, |128\rangle, |127\rangle, |142\rangle\}.
\end{aligned} \tag{17}$$

Since all quantum secret images are distinct and the quantum chaotic image is random, the obtained quantum share images are also random and distinct. Thus, $|S_1\rangle$, $|S_2\rangle$, and $|S_3\rangle$ do not reveal any information of the original quantum secret images.

In summary, compared with the traditional secret image-sharing schemes, which involve complex computation, the proposed scheme constructs the shares only using some basic quantum gate operations. Using quantum parallel processing, the computational efficiency is considerably improved. In addition, the proposed scheme can share m secret images rather than one image only, that is, m quantum secret images can be shared at once by means of sharing $m+1$ quantum share images. Theoretically, it is simple and efficient.

4. Simulation and analysis

To demonstrate the feasibility of the proposed scheme, the simulations were conducted using MATLAB 2014b on a classical computer. In the numerical simulations, to generate the chaotic quantum image I_0 (Fig. 10(a)), the parameters in the logistic map are set as $X_0 = 0.7078$, $\mu = 3.95$. The Lena image (I_1) and Peppers image (I_2) with a size of 256×256 and 8-bit grayscale are used as the quantum secret images (Figs. 10(b) and 10(c)). Figures 10(d)–10(f) show three quantum share images: S_1, S_2, and S_3, respectively. Figures 10(g) and 10(h) show the reconstructed secret images.

4.1. Security analysis

In this subsection, we analyze the security of the proposed quantum image-sharing scheme from two aspects. On the one hand, we analyze the security issue based on statistical properties. On the other hand, we analyze the security issue based on quantum effects.

4.1.1. Statistical analysis

First, as we know, the image histogram reflects the pixel distribution of an image. An idea share image should have a uniform frequency distribution. The histograms of the secret images and share images are shown in Fig. 11. It can be seen that the histograms of share images are significantly different from the histogram of the original secret images. Hence, it does not provide any useful statistic data in the share images to trigger any statistical attacks to the proposed scheme.

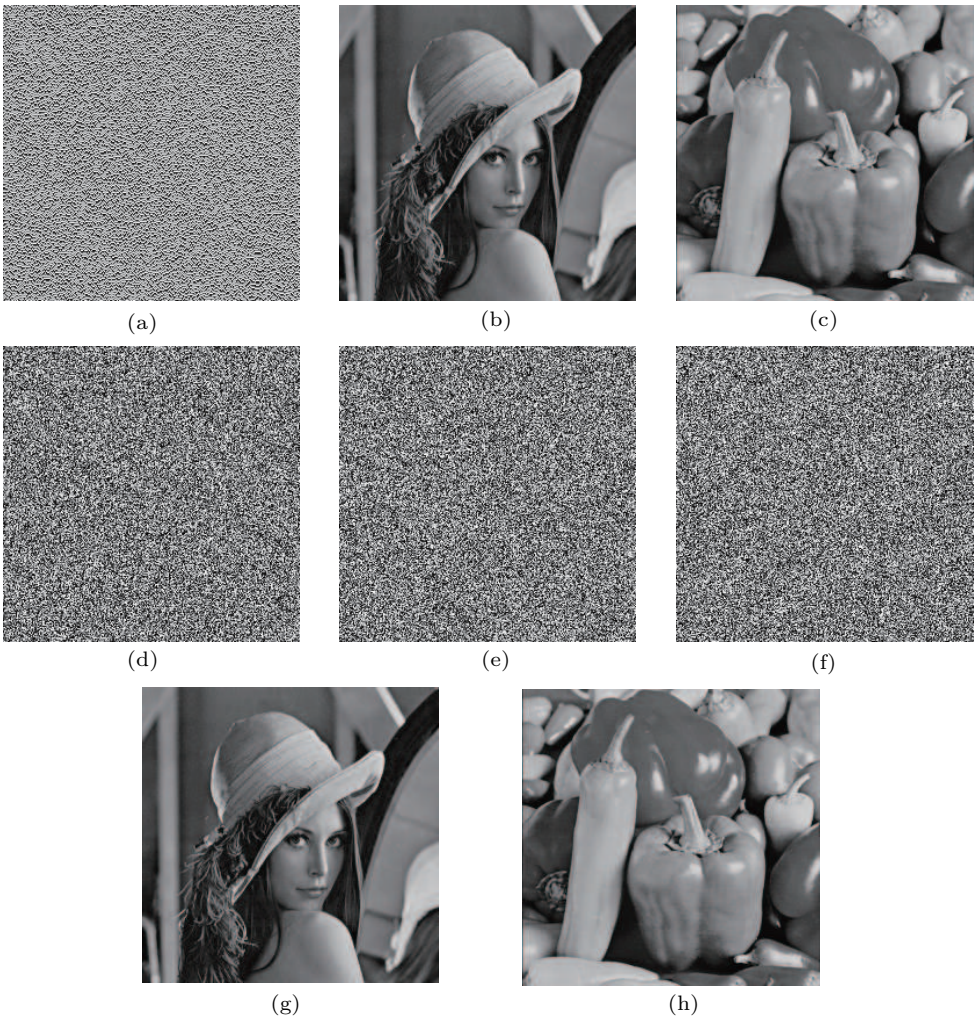


Fig. 10. (a) Chaotic image, (b) secret image Lena, (c) secret image Peppers, (d)–(f) three share images, and (g)–(h) reconstructed images.

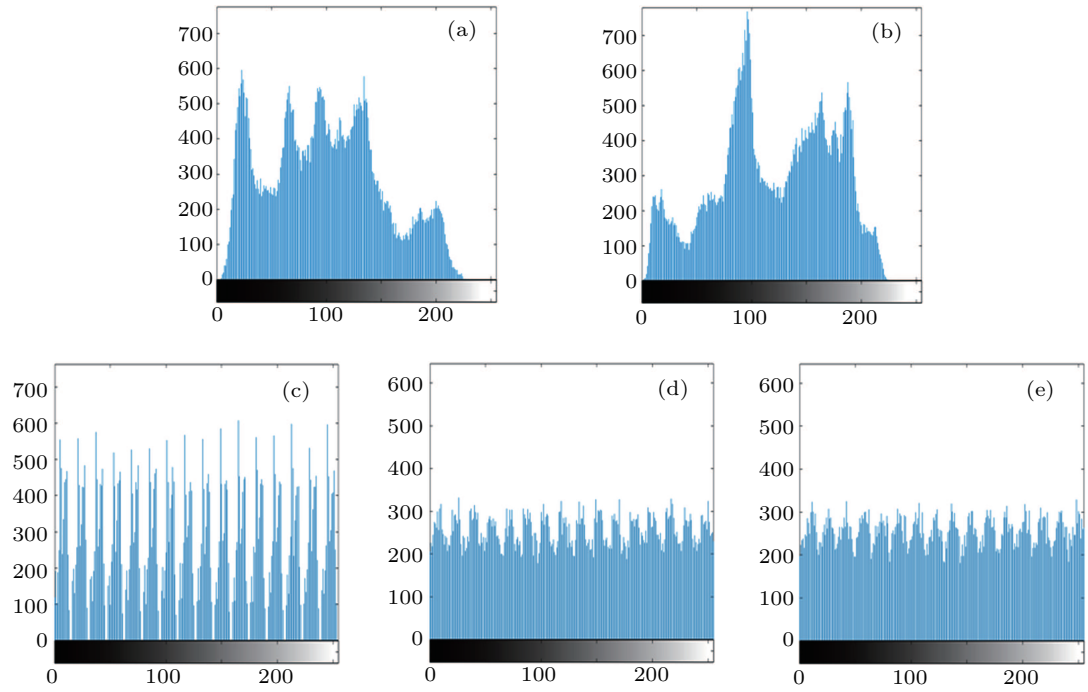


Fig. 11. (a)–(b) The histogram of the secret images Lena and Peppers, (c)–(f) the histogram of the three share images.

Second, since the correlation reflects the degree of similarity of two variables, each pixel in the original image is highly correlated with its adjacent pixels in general. The correlation coefficient $R(x,y)$ of adjacent pixels is simply defined by the following equation:

$$R(x,y) = \frac{E(x-E(x))E(y-E(y))}{\sqrt{D(x)D(y)}}, \tag{18}$$

where $E(x)$ and $D(x)$ denote the expectation and variance of the pixel grayscale values, respectively. To get the correlation of two adjacent pixels, 8000 pairs of two adjacent pixels (in the horizontal, vertical, and diagonal directions) are selected randomly from the original secret images and share images. The real correlation coefficients are shown in Table 1. It is easy to see that the correlations of the share images are close to 0 in each direction, while those of the original images are close to 1 in each direction. That is, the attacker cannot acquire any useful information via statistical analysis. The correlation distributions of horizontally, vertically, and diagonally adjacent pixels in the secret image Lena and one of the share images (S_2) are demonstrated in Fig. 12.

Table 1. Correlation coefficients of adjacent pixels.

Correlation coefficient	Horizontal direction	Vertical direction	Diagonal direction
Secret image Lena (I_1)	0.9282	0.9594	0.8981
Secret image Peppers (I_2)	0.9534	0.9657	0.9293
Share image (S_1)	0.0092	–0.0052	–0.0257
Share image (S_2)	–0.0156	–0.0021	0.0413
Share image (S_3)	–0.0057	0.0121	0.0174

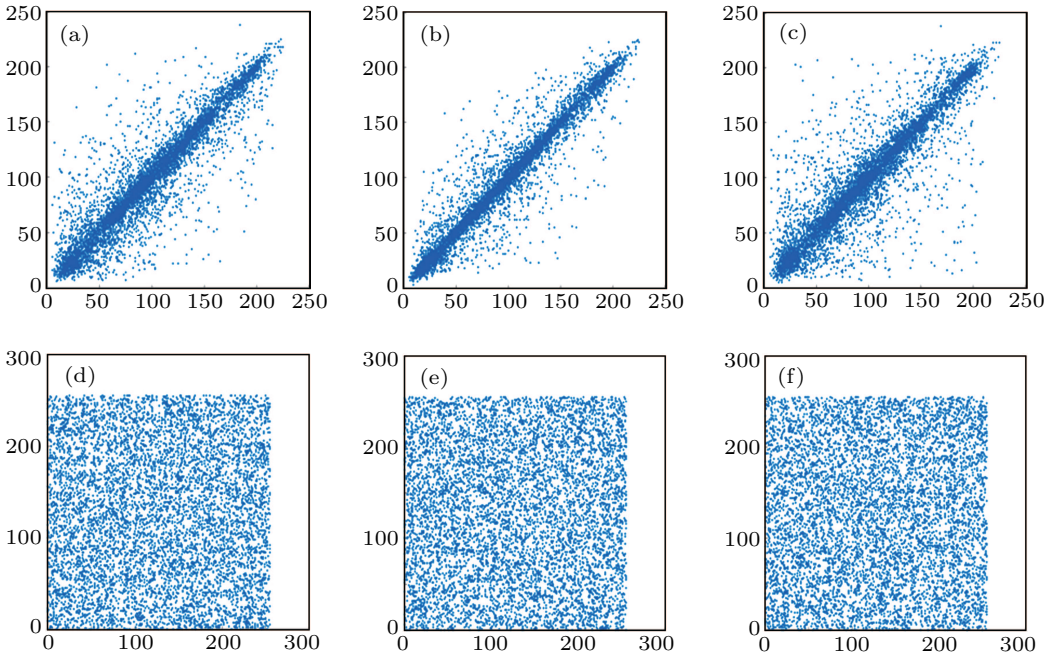


Fig. 12. Distribution of two horizontal direction, vertical direction, and diagonal direction adjacent pixels, (a)–(c) the secret image Lena, (d)–(f) the share image S_2.

4.1.2. Security analysis based on quantum effects

In the classical secret image-sharing scheme, the share images are easily affected by different types of noise and known attacks during transmission. It is necessary to discuss the security of the proposed scheme based on quantum effects.[22] As we know, the quantum no-cloning theorem forbids cloning an unknown quantum state accurately. When it is measured, an unknown quantum state will collapse. The no-cloning theorem provides another perspective on the lack of accessibility suffered by quantum information in comparison to classical information. Therefore, the characteristics of quantum mechanics can ensure the security of the proposed scheme to some extent. Although it seems unconditional security can be achieved in quantum communication in theory, when the quantum share images transmit in a practical quantum channel, the quantum states are destroyed by decoherence and quantum noise easily. Some strategies, such as quantum error correction[36] and quantum error rejection,[37,38] can be used in this case. That is, these solutions could be useful for the transmission of quantum share images theoretically. Through this method, the original quantum secret images can be reconstructed even if several qubits are flipped or lost.

4.2. Computational complexity

The quantum circuit complexity depends on the number of basic quantum gates.[36,39] It has been pointed that one Toffoli gate can be simulated by six CNOT gates and one swap gate can be simulated by three CNOT gates. In this paper, we choose the CNOT gate as the basic unit. The circuit complexity of the n-CNOT ($n \geq 3$, where n denotes the number of the control qubit) gate is $12n-9$,[10] and the complexity of single QE and Arnold scrambling is $O(n)$.[33] The quantum circuit of coordinate comparison module is shown in Fig. 6. It is easy to see that the numbers of the QE module and the output qubits are m. The complexity of the coordinate comparison quantum circuit is also $O(n)$. According to Fig. 7, there are $4\times(m+1)$ quantum swap gates, that is, $12(m+1)$ CNOT gates. For each swap gate, there are m control qubits. Hence, the numbers of m-CNOT gate are $12(m+1)$. The complexity of the quantum swap circuit is $12(m+1)(12m-9)$. Similarly, the numbers of m-CNOT gates are $8m$ according to Fig. 8. The complexity of the quantum image XOR operation is $8m(12m-9)$. Obviously, since m denotes the numbers of quantum secret images, the total complexity of the proposed scheme is $O(n)$.

However, for a classical image with a size of $2^n\times 2^n$, the number of pixels that need to be processed is 2^{2n}. For example, the classical image XOR operations can be realized by using 2^{2n} operations. The total computational complexity is no less than $O(2^{2n})$. This implies that the proposed quantum secret image-sharing scheme has the advantage over its classical counterparts in terms of computational complexity.

5. Conclusions

We have proposed a novel quantum secret image-sharing scheme which constructs m quantum secret images into $m+1$ quantum share images. The quantum image-sharing process can be realized by some basic quantum gate operations. Because all quantum operations are invertible, the quantum image recovery process is the inverse of the sharing process. Theoretical analysis and simulation experiments have shown that the proposal has outperformed its classical counterparts in terms of security and computational complexity. Moreover, multiple quantum secret images can be shared simultaneously without involving complex quantum operations, and the proposal is simple and efficient to implement due to quantum parallel processing. In the future, quantum secret image-sharing techniques may be used for real application, such as medical image sharing between two remote hospitals.

Acknowledgments

The authors would like to thank the editor and anonymous reviewers for their constructive comments.

References

[1] Fan H 2018 *Acta Phys. Sin.* **67** 120301 (in Chinese)
[2] Feynman R P 1982 *Int. J. Theor. Phys.* **21** 467
[3] Shor P W 1994 *Proceedings of 35th Annual Symposium on Foundations of Computer Science* pp. 124–134
[4] Grover L K 1996 *Proceedings of the 28th Annual ACM symposium on the Theory of Computing* pp. 212–219
[5] Beach G, Lomont C and Cohen C 2003 *Proceedings of the 32nd Applied Imagery Pattern Recognition Workshop* pp. 39–44
[6] Caraiman S and Manta V 2012 *IEEE International Conference on System Theory*
[7] Le P Q, Dong F and Hirota K 2011 *Quantum Inform. Process.* **10** 63
[8] Zhang Y, Lu K, Gao Y and Wang M 2013 *Quantum Inform. Process.* **12** 2833
[9] Li H S, Zhu Q, Zhou R G, Song L and Yang X 2014 *Quantum Inform. Process.* **13** 991
[10] Jiang N, Wang J and Mu Y 2015 *Quantum Inform. Process.* **14** 4001
[11] Zhou R G, Hu W, Fan P and Ian H 2017 *Sci. Rep.* **7** 2511
[12] Jiang N, Dang Y and Wang J 2016 *Quantum Inform. Process.* **15** 3543
[13] Luo G, Zhou R G, Liu X, Hu W and Luo J 2018 *Int. J. Theor. Phys.* **57** 2447
[14] Li P and Liu X 2018 *Int. J. Quantum Inform.* **16** 1850020
[15] Jiang N, Zhao N and Wang L 2016 *Int. J. Theor. Phys.* **55** 107
[16] Li P and Lu A 2018 *Int. J. Theor. Phys.* **57** 1516
[17] Luo G, Zhou R G, Luo J, Hu W, Zhou Y and Ian H 2019 *Quantum Inform. Process.* **18** 49
[18] Luo G, Zhou R G, Hu W, Luo J, Liu X and Ian H 2018 *Quantum Inform. Process.* **17** 299
[19] Hu W, Zhou R G, Luo J and Liu B 2019 *Quantum Inform. Process.* **18** 16
[20] Qu Z G, He H X and Li T 2018 *Chin. Phys. B* **27** 010306
[21] Yang Y G, Pan Q X, Sun S and Xu P 2015 *Sci. Rep.* **5** 7784
[22] Yang Y G, Tian J, Lei H, Zhou Y H and Shi W M 2016 *Inform. Sci.* **345** 257
[23] Li P and Zhao Y 2017 *Int. J. Theor. Phys.* **56** 1961
[24] Zhou N, Chen W, Yan X and Wang Y 2018 *Quantum Inform. Process.* **17** 137
[25] Yang Y G, Cao W F and Wen Q Y 2010 *Chin. Phys. B* **19** 050306
[26] Zhu Z C, Zhang Y Q and Fu A M 2012 *Chin. Phys. B* **21** 010307
[27] Liang J W, Cheng Z, Shi J J and Guo Y 2016 *Acta Phys. Sin.* **65** 160301 (in Chinese)
[28] Zhu Z C, Hu A Q and Fu A M 2016 *Int. J. Theor. Phys.* **55** 2342
[29] Long G L, Sheng Y B and Yin L G 2018 *Physics* **47** 413 (in Chinese)
[30] Naor M and Shamir A 1995 *Lect. Notes Comput. Sci.* **950** 1
[31] Song X, Wang S, Sang J, Yan X and Niu X 2014 *IEEE Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing* pp. 215–218
[32] El-latif A A A, Abd-el-atty B and Hossain M S 2018 *IEEE Access* **6** 21075
[33] Zhou R G, Hu W and Fan P 2017 *Quantum Inform. Process.* **16** 212
[34] Jiang N, Wu W Y and Wang L 2014 *Quantum Inform. Process.* **13** 1223
[35] Jiang N and Wang L 2014 *Quantum Inform. Process.* **13** 1545
[36] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[37] Kalamidas D 2005 *Phys. Lett. A* **343** 331
[38] De D B and Ramos R V 2006 *Phys. Lett. A* **352** 206
[39] Barenco A, Bennett C H, Cleve R, Divincenzo D P, Margolus N, Shor P, Sleator T, Smolin J A and Weinfurter H 1995 *Phys. Rev. A* **52** 3457