Int J Theor Phys (2017) 56:2192–2205
DOI 10.1007/s10773-017-3365-z

Quantum Multi-Image Encryption Based on Iteration Arnold Transform with Parameters and Image Correlation Decomposition

Yiqun Hu[1] · Xinwen Xie[1,3] · Xingbin Liu[1] · Nanrun Zhou[1,2]

Received: 16 December 2016 / Accepted: 30 March 2017 / Published online: 6 April 2017

Abstract A novel quantum multi-image encryption algorithm based on iteration Arnold transform with parameters and image correlation decomposition is proposed, and a quantum realization of the iteration Arnold transform with parameters is designed. The corresponding low frequency images are obtained by performing 2-D discrete wavelet transform on each image respectively, and then the corresponding low frequency images are spliced randomly to one image. The new image is scrambled by the iteration Arnold transform with parameters, and the gray-level information of the scrambled image is encoded by quantum image correlation decomposition. For the encryption algorithm, the keys are iterative times, added parameters, classical binary and orthonormal basis states. The key space, the security and the computational complexity are analyzed, and all of the analyses show that the proposed encryption algorithm could encrypt multiple images simultaneously with lower computational complexity compared with its classical counterparts.

Keywords Discrete wavelet transform · Iteration Arnold transform with parameters · Quantum image correlation decomposition · Quantum multi-image encryption · Quantum computation

✉ Nanrun Zhou
znr21@163.com; nrzhou@ncu.edu.cn

[1] Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China

[2] Department of Electrical and Computer Engineering, University of Pittsburgh, Pittsburgh, PA 15261, USA

[3] XLIM (UMR CNRS 7252), University of Poitiers, Poitiers, France

1 Introduction

The rapid progress of quantum computation and quantum computer attracts people to investigate quantum data security. Combining quantum computing method with digital image processing techniques is an effective method to solve the current image processing problems. Quantum computation has been applied in many fields of information sciences [1].

As an important form of quantum information, quantum images will make the applications of quantum computer more extensive and comprehensive. A series of methods representing quantum images have been proposed [2–7]. Le et al. proposed a flexible representation of quantum images (FRQI) [3], which captured information about colors and their corresponding positions in one image into quantum states. Meanwhile, Le designed a method on how to get the quantum states and analyzed the computational complexity of quantum image preparation. On the basis of the type proceed color transform [4], simple geometric transform [8, 9] and image watermarking [10], Zhang et al. proposed a novel enhanced quantum representation (NEQR) model for digital images [11], which improved the storage model of color information in FRQI and put not only position but also color in qubits.

Consequently, some new quantum algorithms were developed as new theoretical tools for quantum image encryption [12–25]. For instance, Liao et al. improved the efficiency of quantum steganography with noisy depolarizing channels by modifying the twirling procedure and adding quantum teleportation [13]. Hua et al. proposed a quantum image encryption algorithm based on image correlation decomposition [19], where the correlation among image pixels is established by utilizing the superposition and measurement principle of quantum states and a whole quantum image is divided into a sequence of sub-images. Gong et al. proposed a quantum image encryption algorithm based on quantum image XOR operations [25]. Jiang et al. proposed a quantum realization of Arnold and Fibonacci image scrambling [26]. After that, Jiang et al. analyzed and improved the quantum Arnold image scrambling [27], and proposed a better scheme to decrease the network complexity apparently. Zhou et al. proposed a quantum image encryption algorithm based on generalized Arnold transform and double random phase encoding [28], which scrambled the pixels by the generalized Arnold transform and the gray-level information of images was encoded by the double random-phase operations. In the field of classical image encryption, there were some good multi-image encryption algorithms [29–33]. Kong et al. presented a multi-image encryption algorithm based on optical wavelet transform and multichannel fractional Fourier transform [30] and the scheme could make full use of multi-resolution decomposition of wavelet transform and multichannel processing of multi-channel fractional Fourier transform. Liao et al. proposed reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels, which reduces the average extracted-bit error rate when the block size is appropriate [31].

In this paper, a quantum version of the iteration Arnold transform with parameters and a quantum multi-image encryption algorithm by combining iteration Arnold transform with parameters with quantum image correlation decomposition are designed. Due to the multi-resolution decomposition property of DWT, images are decomposed into sub-images of different frequencies and the energy of image is focused on the low-frequency part by performing DWT. Therefore, these low-frequency parts could be reassembled. Then the iteration Arnold transform with parameters is performed on the new image to scramble image

by shuffling the positions of image pixels. Finally, quantum image correlation decompos ition is performed on the scrambled image. At the same time, Pauli-x gate, Pauli-z gate, phase shift gate are used to encode color information of quantum image.

The rest of this paper is organized as follows. In Section 2, the flexible representation model for quantum images and the discrete wavelet transform are reviewed. The quantum realization of image scrambling by the iteration Arnold transform with parameters is designed in Section 3. In Section 4, the quantum multi-image encryption and decryption algorithm is introduced. Section 5 is devoted to the theoretical analyses on key space, security and computational complexity. Finally, a conclusion is drawn in Section 6.

2 Flexible Representation for Quantum Images and Wavelet Transform

2.1 The Flexible Representation for Quantum Images

Classical image is represented by a matrix with the same size of the image, i.e., the number of pixels, and each pixel contains the position information and the grayscale value. Inspired by this, a quantum flexible representation for images on quantum computers capturing information about positions and grayscale values has been proposed. The flexible representation for quantum images can be expressed as:

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

$$|g(y,x)\rangle = \cos\theta_i \, |0\rangle + \sin\theta_i \, |1\rangle \tag{2}$$

where $\theta_i \in \left[0, \frac{\pi}{2}\right]$ $(i = yx = 0, 1, \ldots, 2^{2n} - 1)$, $|0\rangle$ and $|1\rangle$ are two-dimensional computational basis quantum states, $\theta = \left(\theta_0, \theta_1, \ldots, \theta_{2^{2n}-1}\right)$ is the vector of angles encoding colors, $|g(y,x)\rangle$ encodes the color information of the quantum image, $|i\rangle = |yx\rangle$ encodes the position information of the quantum image, $|x\rangle = |x_{n-1}x_{n-2}\ldots x_0\rangle$ encodes the first n-qubit along the horizontal location while $|y\rangle = |y_{n-1}y_{n-2}\ldots y_0\rangle$ encodes the second n-qubit along the vertical location, and n is the number of quantum bits required for encoding.

2.2 Discrete Wavelet Transform

Wavelet transform is another breakthrough in mathematics after Fourier transform with profound theoretical meaning and widespread applications. Now wavelet transform plays an important role in the field of signal analysis, image processing, computer recognition, data compression, and etc. The discrete wavelet transform (DWT), a special case of wavelet transform, provides a compact representation of a signal in time and frequency domains. The energy of image is focused on the low-frequency part after DWT. In a general two-dimensional DWT, the data are decomposed into four parts firstly, shown in Fig. 1, where LL_1 and HH_1 are respectively the low-frequency and the high-frequency parts and the other two are the diagonal parts.

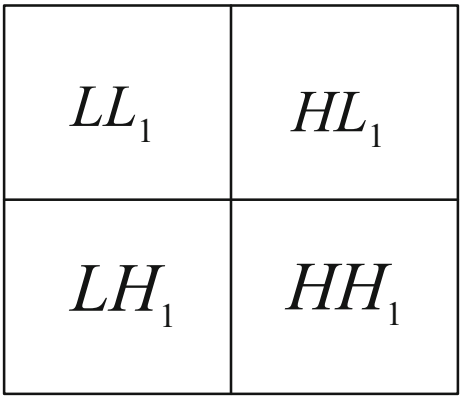

Fig. 1 Discrete wavelet decomposition

3 Realization of Iteration Arnold Transform with Parameters

3.1 Quantum Representation of Iteration Arnold Transform with Parameters

The Arnold transform, also called Arnold's cat map, was discovered by V. I. Arnold Dyson et al. [34] and it has been used in image scrambling widely. The two-dimensional Arnold transform A in the form of matrix is defined as

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod} N) = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod} N) \tag{3}$$

The iteration Arnold transform A^i with parameters in the form of matrix is defined as

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A^i \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} ku \\ kv \end{bmatrix} (\mathrm{mod} N) = \begin{bmatrix} f_{2i-1} & f_{2i} \\ f_{2i} & f_{2i+1} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} ku \\ kv \end{bmatrix} (\mathrm{mod} N) \tag{4}$$

where $x, y, x', y' \in \{0, 1, \ldots, N-1\}$, f_i is defined by Fibonacci spectrum as $f_{i+2} = f_{i+1} + f_i$, $f_1 = 1$, $f_2 = 1$. x and y are the pixel coordinates of the original image, x' and y' are the pixel coordinates of the scrambled image after the iteration Arnold transform with parameters. N is the size of the original image. Generally, the original image is considered as a square image. u, v and k are the joined parameters. Its inverse transform A^{-i} is

$$\begin{bmatrix} x \\ y \end{bmatrix} = A^{-i} \begin{bmatrix} x' - ku \\ y' - kv \end{bmatrix} (\mathrm{mod} N) = \begin{bmatrix} f_{2i+1} & -f_{2i} \\ -f_{2i} & f_{2i-1} \end{bmatrix} \begin{bmatrix} x' - ku \\ y' - kv \end{bmatrix} (\mathrm{mod} N) \tag{5}$$

The iteration Arnold transform with parameters in the form of pixel coordinates can be expressed as

$$\begin{cases} x' = (f_{2i-1}x + f_{2i}y + ku) \bmod N \\ y' = (f_{2i}x + f_{2i-1}y + kv) \bmod N \end{cases} \tag{6}$$

According to the classical iteration Arnold transform with parameters, the quantum representation of the iteration Arnold transform with parameters can be described as

$$\begin{cases} |x'\rangle = |f_{2i-1}x + f_{2i}y + ku\rangle \bmod 2^n \\ |y'\rangle = |f_{2i}x + f_{2i-1}y + kv\rangle \bmod 2^n \end{cases} \tag{7}$$

3.2 Quantum Circuit Architecture of Iteration Arnold Transform with Parameters

Quantum network is a device operating quantum algorithm or processing quantum information. A plain adder is used to calculate the sum of two numbers. The addition of two quantum registers $|a\rangle$ and $|b\rangle$ can be written as $|a, b\rangle \rightarrow |a, a+b\rangle$. The adder modulo 2^n is a quantum network to calculate the sum of two numbers stored in the corresponding quantum registers. It can be written as $|a, b\rangle \rightarrow |a, (a+b) \bmod 2^n\rangle$, where a, b are the inputs while $(a+b) \bmod 2^n$ is the output. In the iteration Arnold transform with parameters, the networks $|x'\rangle$ and $|y'\rangle$ for the iteration Arnold transform with parameters are independent, which can be realized by connecting several quantum ADDER-MOD2^n circuits [26]. Therefore, the quantum ADDER-MOD2^n network is basic to realize the iteration Arnold transform with parameters in quantum computer.

Assume that x, y, u and v are all n-qubit binary numbers, $x = x_{n-1}x_{n-2}\ldots x_0$, $y = y_{n-1}y_{n-2}\ldots y_0$, $u = u_{n-1}u_{n-2}\ldots u_0$, $v = v_{n-1}v_{n-2}\ldots v_0$, $x_i, y_i, u_i, v_i \in \{0, 1\}$, $i = n-1, n-2, \ldots, 0$. The realization of $|x'\rangle$ is divided into $f_{2i-1} + f_{2i} + k$ steps, as shown in Fig. 2. The ADDER-MOD2^n network is used to obtain $f_{2i-1}x \bmod 2^n$ from the first step to the $(f_{2i-1}-1)$-th step. In the f_{2i-1}-th step, x is replaced by y, and from the $(f_{2i-1}+1)$-th step to the $(f_{2i-1}+f_{2i}-1)$-th step, the ADDER-MOD2^n network is employed to obtain $(f_{2i-1}x + f_{2i}y) \bmod 2^n$. In the $(f_{2i-1}+f_{2i})$-th step, y is replaced by u, and from the $(f_{2i-1}+f_{2i}+1)$-th step to the last step, the ADDER-MOD2^n network is exploited to obtain $(f_{2i-1}x + f_{2i}y + ku) \bmod 2^n$.

$$
\begin{aligned}
|x, x\rangle &\rightarrow \left|x, 2x \bmod 2^n\right\rangle \rightarrow \cdots \rightarrow \left|x, f_{2i-1}x \bmod 2^n\right\rangle \rightarrow \left|y, f_{21-1}x \bmod 2^n\right\rangle \\
&\rightarrow \left|y, (f_{2i-1}x + y) \bmod 2^n\right\rangle \rightarrow \cdots \rightarrow \left|y, (f_{2i-1}x + f_{2i}y) \bmod 2^n\right\rangle \\
&\rightarrow \left|u, (f_{2i-1}x + f_{2i}y) \bmod 2^n\right\rangle \rightarrow \cdots \rightarrow \left|u, (f_{2i-1}x + f_{2i}y + ku) \bmod 2^n\right\rangle \quad (8)
\end{aligned}
$$

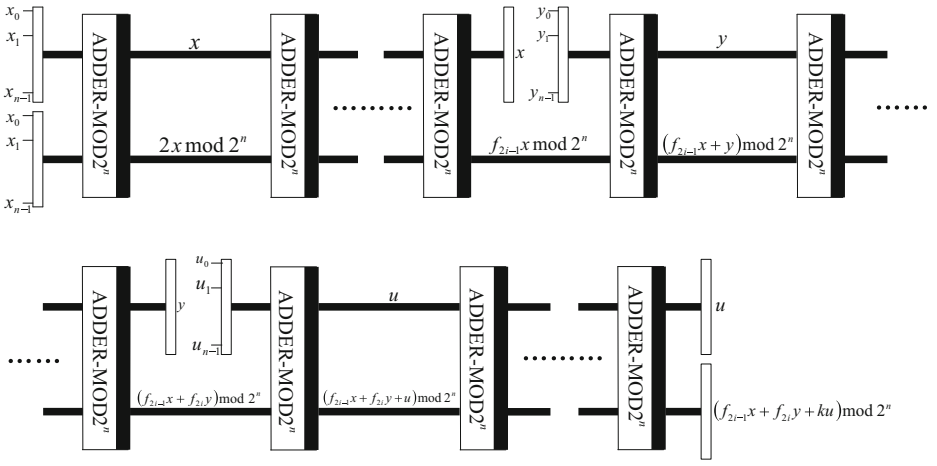

Fig. 2 $|x'\rangle$ network for the iteration Arnold transform with parameters

The realization of $|y'\rangle$ is divided into $f_{2i} + f_{2i-1} + k$ steps, as shown in Fig. 3.

$$\begin{aligned} |x, x\rangle &\rightarrow \left|x, 2x \bmod 2^n\right\rangle \rightarrow \cdots \rightarrow \left|x, f_{2i}x \bmod 2^n\right\rangle \rightarrow \left|y, f_{2i}x \bmod 2^n\right\rangle \\ &\rightarrow \left|y, (f_{2i}x + y) \bmod 2^n\right\rangle \rightarrow \cdots \rightarrow \left|y, (f_{2i}x + f_{2i-1}y \bmod 2^n\right\rangle \\ &\rightarrow \left|v, (f_{2i}x + f_{2i-1}y) \bmod 2^n\right\rangle \rightarrow \cdots \rightarrow \left|v, (f_{2i}x + f_{2i-1}y + kv \bmod 2^n\right\rangle \end{aligned} \tag{9}$$

4 Quantum Multi-Image Encryption and Decryption Algorithm

4.1 Quantum Multi-Image Encryption Algorithm

Assume that the four images to be encrypted are I_1, I_2, I_3 and I_4. The proposed multi-image encryption algorithm consists of the following steps, and the encryption procedure is shown in Fig. 4.

Step 1. By performing discrete wavelet transform on the four images of size $2^n \times 2^n$, respectively, the corresponding low frequency image LL_i $(i = 1, 2, 3, 4)$ of size $2^{n-1} \times 2^{n-1}$ can be obtained.

$$LL_i = \mathrm{DWT}\,(I_i) \tag{10}$$

Randomly build up an image from the corresponding low frequency images. Then the new image can be expressed as:

$$|Q\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |f(y,x)\rangle\, |yx\rangle \tag{11}$$

$$|f(y,x)\rangle = \cos\psi_i\, |0\rangle + \sin\psi_i\, |1\rangle\,,\ \psi_i \in \left[0, \frac{\pi}{2}\right],\ i = yx = 0, 1, \ldots, 2^{2n} - 1 \tag{12}$$

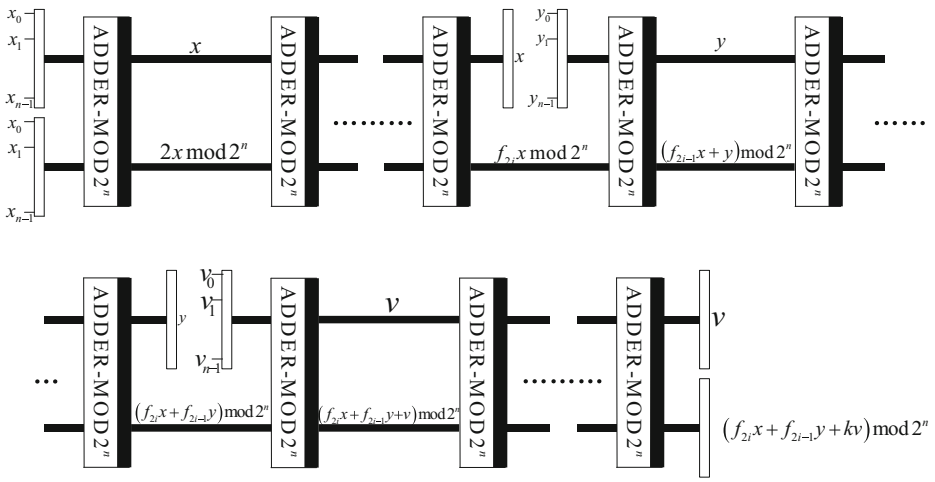

Fig. 3 $|y'\rangle$ network for the iteration Arnold transform with parameters

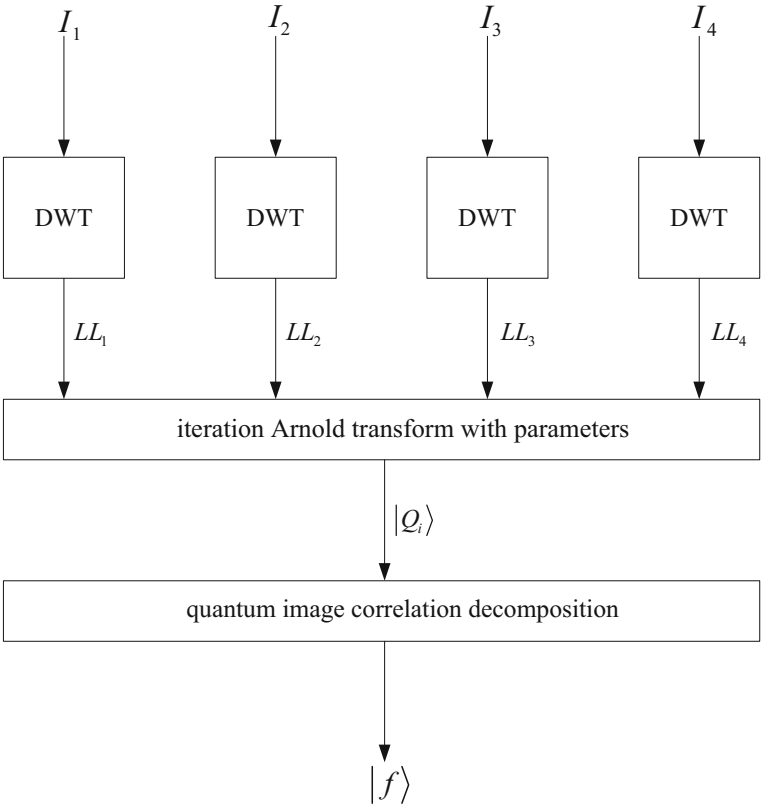

Fig. 4 The quantum multi-image encryption algorithm procedure

where the new image is a classical image of size $2^n \times 2^n$.

Step 2. To obtain $|Q_i\rangle$, one performs the iteration Arnold transform with parameters on $|Q\rangle$ for i times, where $|x'\rangle$ represents the horizontal location information and $|y'\rangle$ represents the vertical location information of the scrambled image $|Q_i\rangle$. The quantum version of the iteration Arnold transform with parameters is defined as

$$\begin{aligned} |Q_i\rangle &= A^i\,|M\rangle = \frac{1}{2^n}\sum_{y=0}^{2^n-12^n-1}\sum_{x=1}|g(y,x)\rangle\, A^i\,|yx\rangle \\ &= \frac{1}{2^n}\sum_{y=0}^{2^n-12^n-1}\sum_{x=0}|g(y,x)\rangle\, A^i\,|y\rangle\, A^i\,|x\rangle \\ &= \frac{1}{2^n}\sum_{y=0}^{2^n-12^n-1}\sum_{x=0}|g(y,x)\rangle\,|y'\rangle|x'\rangle \end{aligned} \tag{13}$$

where

$$\begin{cases} |x'\rangle = |f_{2i-1}x + f_{2i}y + ku\rangle \bmod 2^n \\ |y'\rangle = |f_{2i}x + f_{2i-1}y + kv\rangle \bmod 2^n \end{cases} \tag{14}$$

Step 3. $|Q_i\rangle$ is divided into a range of sub-images $|Q_1\rangle, |Q_2\rangle, \cdots |Q_{l-i}\rangle$ by performing the quantum image correlation decomposition technology [20]. Then we divide $|Q_i\rangle$ into three segments $|Q_{i1}\rangle$, $|Q_{i2}\rangle$ and $|Q_{i3}\rangle$.

Step 4. To encode the color information of the quantum image, quantum bit gates are performed on these sub-images. Pauli-x gate, Pauli-z gate and phase shift gate are successively performed on the three segments. Pauli-x gate C_j is performed on $|Q_{i1}\rangle$. Pauli-x gate C_j is controlled by a classical binary number a_w, where $a_w \in \{0, 1\}$, $w = 0, 1, \ldots, 2^{2n} - 1$. Binary sequence $A = a_0 a_1 \ldots a_{2^{2n}-1}$ is the key. Pauli-x gate C_j is used to construct a $2n + 1$ qubit-based unitary transform H_j.

$$H_j = \left(C_j\right)^{a_w} = \begin{cases} C_j, & a_w = 1; \\ I, & a_w = 0. \end{cases} \tag{15}$$

$$C_j = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{16}$$

A $2n + 1$ qubit-based unitary transform B_j could be constructed with unitary transform H_j.

$$B_j = I \otimes \sum_{y=0}^{2^n-1} \sum_{\substack{x=0 \\ yx \neq j}}^{2^n-1} |yx\rangle \langle yx| + H_j \otimes |j\rangle \langle j| \tag{17}$$

The Pauli-x matrix B_j is a unitary matrix since $B_j B_j^{\dagger} = I^{\otimes 2n+1}$. If we apply a $2n + 1$ qubits unitary transform B on the quantum image $|Q_{i1}\rangle$, then $|f_{i1}\rangle$ will be obtained.

$$\begin{aligned} B\,|Q_{i1}\rangle &= \prod_{y=0}^{2^n-1} \prod_{x=0}^{2^n-1} B_j\,|Q_{i1}\rangle \\ &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} \left(\cos\theta_{yx}\,|1\rangle + \sin\theta_{yx}\,|0\rangle\right)|yx\rangle \\ &= |f_{i1}\rangle \end{aligned} \tag{18}$$

Pauli-z gate D_m is performed on $|Q_{i2}\rangle$. D_m is controlled by a classical binary number e_o, where $e_m \in \{0, 1\}$, $m = 0, 1, \ldots, 2^{2n} - 1$. Binary sequence $E = e_0 e_1 \ldots e_{2^{2n}-1}$ is the key. Pauli-z gate D_m is used to construct a $2n+1$ qubit-based unitary transform S_m.

$$S_m = (D_m)^{e_m} = \begin{cases} D_m, & e_m = 1; \\ I, & e_m = 0. \end{cases} \tag{19}$$

$$D_m = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \tag{20}$$

Unitary transform S_m is used to construct a $2n + 1$ qubit-based unitary transform R_m.

$$R_m = I \otimes \sum_{y=0}^{2^n-1} \sum_{\substack{x=0 \\ yx \neq 0}}^{2^n-1} |yx\rangle \langle yx| + S_m \otimes |m\rangle \langle m| \tag{21}$$

The Pauli-z matrix D_m is a unitary matrix since $R_m R_m^{\dagger} = I^{\otimes 2n+1}$. If we apply $2n+1$ qubits unitary transform R on the quantum image $|Q_{i2}\rangle$, then $|f_{i2}\rangle$ will be achieved.

$$\begin{aligned} R\,|Q_{i2}\rangle &= \prod_{y=0}^{2^n-1}\prod_{x=0}^{2^n-1} R_m\,|Q_{i2}\rangle \\ &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}\left(\cos\theta_{yx}\,|1\rangle - \sin\theta_{yx}\,|0\rangle\right)|yx\rangle \\ &= |f_{i2}\rangle \end{aligned} \tag{22}$$

Phase shift gate K_t is performed on $|Q_{i3}\rangle$ and is controlled by a classical binary number l_t, where $l_t \in \{0,1\}$, $t = 0, 1, \ldots, 2^{2n}-1$. Binary sequence $L = l_1 l_2 \ldots l_{2^{2n}-1}$ is the key. Phase shift gate K_t is used to construct a $2n+1$ qubit-based unitary transform O_t.

$$O_t = (K_t)^{l_t} = \begin{cases} K_t, & l_t = 1; \\ I, & l_t = 0. \end{cases} \tag{23}$$

$$K_t = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\psi} \end{bmatrix} \tag{24}$$

where $t = 0, 1, \ldots, 2^{2n}-1$ and θ is a real number and distributed uniformly between 0 and 1. Unitary transform O_t is used to construct a $2n+1$ qubit-based unitary transform P_t.

$$P_t = I \otimes \sum_{y=0}^{2^n-1}\sum_{\substack{x=0 \\ yx\neq t}}^{2^n-1} |yx\rangle\langle yx| + O_t \otimes |t\rangle\langle t| \tag{25}$$

The controlled phase matrix P_t is a unitary matrix since $P_t P_t^{\dagger} = I^{\otimes 2n+1}$. By applying a $2n+1$ qubits unitary transform P on the quantum image $|Q_{i3}\rangle$, $|f_{i3}\rangle$ could be obtained.

$$\begin{aligned} P\,|Q_{i3}\rangle &= \prod_{y=0}^{2^n-1}\prod_{x=0}^{2^n-1} P_t\,|Q_{i3}\rangle \\ &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}\left(\cos\theta_{yx}\,|0\rangle + e^{j\psi}\sin\theta_{yx}\,|1\rangle\right)|yx\rangle \\ &= |f_{i3}\rangle \end{aligned} \tag{26}$$

Step 5. To obtain the quantum cipher-text image $|f\rangle$, one encrypts all of the images $|f_{i1}\rangle$, $|f_{i2}\rangle$ and $|f_{i3}\rangle$ into the superposition form.

$$|f\rangle = a_0\,|f_0\rangle + a_1\,|f_1\rangle + \cdots + a_{N-1}\,|f_{N-1}\rangle \tag{27}$$

where $a = (a_1, a_2, \ldots, a_{N-1})$ and $a_0^2 + a_1^2 + \cdots + a_{N-1}^2 = 1$. To obtain the orthonormal basis states $|M_i\rangle$, one applies Schmidt decomposition to cipher-text image $|f\rangle$.

$$|f\rangle = r_0\,|M_0\rangle + r_1\,|M_1\rangle + \cdots + r_{N-1}\,|M_{N-1}\rangle \tag{28}$$

where $r = (r_0, r_1, \ldots, r_{N-1})$ and $r_0^2 + r_1^2 + \cdots + r_{N-1}^2 = 1$.

4.2 Quantum multi-image Decryption Algorithm

In the multi-image encryption algorithm, the key involves iterative times i and the classical binary sequences $A = a_1 a_2 \ldots a_{2^{2n}-1}$, $E = e_1 e_2 \ldots e_{2^{2n}-1}$, $L = l_1 l_2 \ldots l_{2^{2n}-1}$. The decryption process is as follows.

Step 1. The cipher-text image $|f\rangle$ is obtained by making measurements on the received quantum image $|f_i\rangle$. With the projection operators $|M_i\rangle$, $i = 0, 1, \ldots, N-1$, the projection measurement can be executed.

$$J = \sum_{i=0}^{N-1} J_i \left|M_i\right\rangle \left\langle M_i\right| \tag{29}$$

$$J_i = \frac{t_i}{t - t_i} \tag{30}$$

where t represents the total number of the measurements and t_i is the number of the measurement result $|f_i\rangle$.

Step 2. According to the quantum image correlation decomposition, different inverse transforms are performed to obtain the sub-images $|Q_0\rangle$, $|Q_1\rangle$, $\ldots$, $|Q_{N-1}\rangle$. For $|f_{i1}\rangle$, the decryption operation B^{-1} is performed with the key A.

$$\begin{aligned} B^{-1}\left|f_{i1}\right\rangle &= \prod_{y=0}^{2^n-1}\prod_{x=0}^{2^n-1} B_j^{\dagger}\left|f_{i1}\right\rangle \\ &= \prod_{y=0}^{2^n-1}\prod_{x=0}^{2^n-1} B_j^{\dagger}\left(\frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}\left(\cos\theta_{yx}\left|1\right\rangle + \sin\theta_{yx}\left|0\right\rangle\right)\left|yx\right\rangle\right) \\ &= \left|Q_{i1}\right\rangle \end{aligned} \tag{31}$$

where $B_j^{\dagger}$ is the Hermitian conjugate of B_j. The decryption operation is performed on $|f_{i2}\rangle$ with the key E.

$$\begin{aligned} R^{-1}\left|f_{i2}\right\rangle &= \prod_{y=0}^{2^n-1}\prod_{x=0}^{2^n-1} R_m^{\dagger}\left|f_{i2}\right\rangle \\ &= \prod_{y=0}^{2^n-1}\prod_{x=0}^{2^n-1} R_m^{\dagger}\left(\frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}\left(\cos\theta_{yx}\left|1\right\rangle - \sin\theta_{yx}\left|0\right\rangle\right)\left|yx\right\rangle\right) \\ &= \left|Q_{i2}\right\rangle \end{aligned} \tag{32}$$

where $R_m^{\dagger}$ is the Hermitian conjugate of R_m. For $|h_{i3}\rangle$, the decryption operation P^{-1} should be executed to obtain image $|Q_{i3}\rangle$ with the key L.

$$\begin{aligned} P^{-1}|f_{i3}\rangle &= \prod_{y=0}^{2^n-1}\prod_{x=0}^{2^n-1} P_t^{\dagger}|f_{i3}\rangle \\ &= \prod_{y=0}^{2^n-1}\prod_{x=0}^{2^n-1} P_t^{\dagger}\left(\frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}(\cos\theta_{yx}|0\rangle + e^{j\psi}\sin\theta_{yx}|1\rangle)|yx\rangle\right) \\ &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|g(y,x)\rangle|yx\rangle \\ &= |Q_{i3}\rangle \end{aligned} \tag{33}$$

where P^{-1} is the inverse operator of P. Then the quantum image $|Q_i\rangle$ is rebuilt by these sub-images.

Step 3. One performs the inverse iteration Arnold transform with parameters A^{-i} on the quantum image $|Q_i\rangle$, where the quantum version of the inverse iteration Arnold transform A^{-i} with parameters is defined as:

$$\begin{aligned} |Q\rangle &= A^{-i}|Q_i\rangle \\ &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|g(y,x)\rangle A^{-i}\left|y'x'\right\rangle \\ &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|g(y,x)\rangle A^{-i}\left|y'\right\rangle A^{-i}|x\rangle \\ &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|g(y,x)\rangle|yx\rangle \end{aligned} \tag{34}$$

where

$$\begin{cases} |x\rangle = A^{-i}\left|x'\right\rangle = f_{2i+1}\left(x'-ku\right) - f_{2i}\left(y'-kv\right) \\ |y\rangle = A^{-i}\left|y'\right\rangle = -f_{2i}\left(x'-ku\right) + f_{2i-1}\left(y'-kv\right) \end{cases} \tag{35}$$

Step 4. LL_i $(i = 1, 2, 3, 4)$ could be obtained from the desirable image. Then the inverse discrete wavelet transform should be performed on these images.

$$I_i = \mathrm{DWT}^{-1}(LL_i) \tag{36}$$

where DWT^{-1} is the inverse transform of DWT. Finally, the corresponding plaintext images I_1, I_2, I_3 and I_4 are obtained.

5 Algorithm Analyses

Practical quantum computer is still not available due to the lack of the quantum hardware, thus the quantum multi-image encryption algorithm can not be simulated. The proposed

quantum multi-image encryption algorithm is limited to the theoretical analyses on key space, security and computational complexity.

5.1 Key Space

A good image encryption scheme should be as sensitive as possible to its keys, and the key space should be large enough to make brute-force attack infeasible or impossible. Assume that the key space for the iteration Arnold transform with parameters is K_1 and the key space for quantum image correlation decomposition is K_2, then the total key space of the proposed multi-image encryption algorithm is K_1K_2. Pauli-x gate, Pauli-z gate and phase shift gate build up the quantum image correlation decomposition. The keys of the iteration Arnold transform with parameters are composed of the parameters k, u, v and the iteration times i. The key space K_1 is very large. The key space of binary sequence A is 2^{2n}, so are E and L. The key space of K_2 is 2^{6n}. With so large total key space, it is very difficult to obtain the plaintext image if the attacker doesn't know the correct key.

5.2 Security

The performance of the proposed quantum multi-image encryption algorithm is better than that of the classical image encryption algorithm. The key space is larger and the computational complexity is lower than its classical counterparts. Hua TX et al.'s quantum image encryption scheme [19] used the corresponding parameters of the transform as the keys. If the attacker cracks the parameters, this part of the encryption scheme will fail and the information may be stolen by the attacker. The proposed multi-image encryption algorithm uses three binary sequences as the keys instead of the corresponding parameters. It increases the key space, and the key space of the proposed image encryption algorithm is larger than that of Hua TX et al.'s encryption algorithm. The image encryption algorithms based on classical Arnold transform have potential security threats due to its periodicity. If the attacker cracks the periodicity, the image will fail to be scrambled. The iteration Arnold transform with parameters in the multi-image encryption algorithm overcomes the shortcoming by the joined parameters k, u, v. The attacker cannot obtain the correct original image even if she decrypts the image with the right periodicity. Because the attacker doesn't know the joined parameters, it can greatly improve the security. The weakness of the algorithm is that it can not be simulated and that quantum image correlation on decomposition transform is limited to theoretical analyses.

5.3 Computational Complexity

Assume I_1, I_2, I_3 and I_4 are the original images of size $2^n \times 2^n$, then there are 2^{2n} pixels in each image. The computational complexity of the proposed multi-image encryption algorithm depends on the discrete wavelet transform, iteration Arnold transform with parameters and quantum image correlation decomposition. In the quantum image correlation decomposition, the computational complexity depends on Pauli-x gate, Pauli-z gate and phase shift gate, whose computational complexities are $O(n)$. The quantum image correlation decomposition needs to perform encryption operation on N sub-images at the same time. Therefore the computational complexity of quantum image correlation decomposition is $O(Nn)$. For the corresponding classical encryption algorithms, Pauli-x gate, Pauli-z gate and phase shift gate are performed on the image by using 2^{2n} multiplication operations, their computation complexities are $O\left(N2^{2n}\right)$. The elementary gates of ADDER-MOD2^n are $28n - 12$. The

iteration Arnold transform with parameters involves $2\left(f_{2i-1}+f_{2i}+k\right)(28n-12)$ basic gates. Then the total computational complexity of the proposed multi-image encryption algorithm is $O\left(\left[N+56\left(f_{2i-1}+f_{2i}+k\right)\right]n\right)$ [35]. The computational complexity of the classical iteration Arnold transform with parameters is $O\left(2^{2n}\right)$ and the total computational complexity is $O\left((N+1)\,2^{2n}\right)$. Therefore, the proposed multi-image encryption algorithm has lower computational complexity than its classical counterparts.

6 Conclusion

A quantum version of iteration Arnold transform with parameters is designed and its quantum circuit is suggested. By combining iteration Arnold transform with parameters with quantum image correlation decomposition technology, a quantum multi-image encryption algorithm is proposed. The encryption process can be realized by performing the discrete wavelet transform, the iteration Arnold transform with parameters and quantum image correlation decomposition technology on the different frequencies of images, position information and encoding color information of these sub-images, respectively. The independent parameters and three binary sequences are used as the keys, and the key space of the proposed multi-image encryption algorithm is very large. Detailed theoretical security and computational complexity analyses on the proposed multi-image encryption algorithm are given. Since the quantum image correlation decomposition technology cannot be simulated currently, the proposed multi-image encryption algorithm is in principle The quantum version of iteration Arnold transform with parameters can enlarge the key space and the scrambled image can be hardly decrypted by joined parameters. Even if the attacker knows the periodicity of the iteration Arnold transform with parameters, she also cannot obtain the correct image due to the joined parameters. The proposed multi-image encryption algorithm can encrypt multiple images at the same time, which has a higher efficiency. Moreover, the proposed multi-image encryption algorithm has lower computational complexity and larger key space than its classical counterparts.

Acknowledgements This work is supported by the National Natural Science Foundation of China (Grant No. 61462061 and 61561033), the China Scholarship Council (Grant No. 201606825042), the Department of Human Resources and Social security of Jiangxi Province, and the Major Academic Discipline and Technical Leader of Jiangxi Province (Grant No. 20162BCB22011).

References

1. Nielsen, M.A., Chuang, I.L.: Piazzesi M Handbook of Financial Econometrics Elsevier: Quantum computation and quantum information, vol. 10, p. 49. Cambridge University Press (2010)
2. Venegas-Andraca, S.E., Ball, J.L.: Processing images in entangled quantum systems. Quantum Inf. Process. **9**(1), 1–11 (2010)
3. Le, P.Q., Dong, F.Y., Hirota, K.: A flexible representation of quantum images for polynomial preparation, image compression, and processing operations. Quantum Inf. Process. **10**(1), 63–84 (2011)
4. Sun, B., Le, P.Q., Iliyasu, A.M., Yan, F., Garcia, J.A., Dong, F., Hirota, K.: A multi-channel representation for images on quantum computers using the RGBα color space. In: 2011 IEEE 7th International Symposium on Floriana, Intelligent Signal Processing (WISP), pp. 62–67 (2011)
5. Le, P.Q., Iliyasu, A.M., Garcia, J.A., Dong, F., Hirota, K.: Representing visual complexity of images using a 3d feature space based on structure, noise, and diversity. JACIII **16**(5), 631–640 (2012)
6. Zhang, Y., Lu, K., Gao, Y., Xu, K.: A novel quantum representation for log-polar images. Quantum Inf. Process. **12**(9), 3101–3126 (2013)

7. Yuan, S., Mao, X., Xue, Y., Chen, L., Xiong, Q., Compare, A.: SQR: A simple quantum representation of infrared images. Quantum Inf. Process. **13**(6), 1–27 (2014)
8. Le, P.Q., Iliyasu, A.M., Dong, F.Y., Hirota, K.: Fast geometric transformations on quantum images. IAENG Int. J. Appl. Math. **40**(3), 113–123 (2010)
9. Le, P.Q., Iliyasu, A.M., Dong, F.Y., Hirota, K.: Strategies for designing geometric transformations on quantum images. Theor. Comput. Sci. **412**(15), 1406–1418 (2011)
10. Iliyasu, A.M., Le, P.Q., Dong, F.Y., Hirota, K.: Watermarking and authentication of quantum images based on restricted geometric transformations. Inf. Sci. **186**(1), 126–149 (2012)
11. Zhang, Y., Lu, K., Gao, Y., Wang, M.: NEQR: A novel enhanced quantum representation of digital images. Quantum Inf. Process. **12**(8), 2833–2860 (2013)
12. Akhshani, A., Akhavan, A., Lim, S.C., Hassan, Z.: An image encryption scheme based on quantum logistic map. Commun. Nonlinear Sci. Numer. Simulat. **17**(12), 4653–4661 (2012)
13. Liao, X., Wen, Q., Song, T., Zhang, J.: Quantum steganography with high efficiency with noisy depolarizing channels. IEICE Trans. Fundam. **E96-A**(10), 2039–2044 (2013)
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. **52**(6), 1802–1817 (2013)
15. Abd El-Latif, A.A., Li, L., Wang, N., Han, Q., Niu, X.: A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces. Signal Process. **93**(11), 2986–3000 (2013)
16. Song, X., Wang, S., El-Latif, A.A.A., Niu, X.: Dynamic watermarking scheme for quantum images based on Hadamard transform. Multimedia Syst. **20**(4), 1–10 (2014)
17. Jiang, N., Wang, L., Wu, W.Y.: Quantum Hilbert Image Scrambling. Int. J. Theor. Phys. **53**(7), 2463–2484 (2014)
18. 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. **12**(11), 3477–3493 (2013)
19. Hua, T.X., Chen. J., Pei, D.J., Zhang, W.Q., Zhou, N.R.: Quantum image encryption algorithm based on image correlation decomposition. Int. J. Theor. Phys. **54**(2), 526–537 (2014)
20. Zhou, R.G., Chang, Z.B., Fan, P., Li, W., Huang, T.T.: Quantum image morphology processing based on quantum set operation. Int. J. Theor. Phys. **54**(6), 1974–1986 (2015)
21. Wang, J., Jiang, N., Wang, L.: Quantum image transform. Quantum Inf. Process. **14**(5), 1589–1604 (2015)
22. Jiang, N., Wu, W., Wang, L., Zhao, N.: Quantum image pseudocolor coding based on the density-stratified method. Quantum Inf. Process. **14**(5), 1735–1755 (2015)
23. Jiang, N., Wang, L.: Quantum image scaling using nearest neighbor interpolation. Quantum Inf. Process. **14**(5), 1559–1571 (2015)
24. Wang, S., Sang, J., Song, X., Niu, X.: Least significant qubit (LSQb) information hiding algorithm for quantum image. Measurement **73**, 352–359 (2015)
25. 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., 1–15 (2016)
26. Jiang, N., Wu, W.Y., Wang, L.: The quantum realization of Arnold and Fibonacci image scrambling. Quantum Inf. Process. **13**(5), 1223–1236 (2014)
27. Jiang, N., Wang, L.: Analysis and improvement of quantum Arnold and Fibonacci image scrambling. Quantum Inf. Process. **13**(7), 1545–1551 (2014)
28. 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. **14**(4), 1193–1213 (2015)
29. Liu, Z.J., Zhang, Y., Zhao, H.F., Ahmad, M.A., Liu, S.T.: Optical multi-image encryption based on frequency shift. Optik-International Journal for Light and Electron Optics **122**(11), 1010–1013 (2011)
30. Kong, D.Z., Shen, X.J.: Multi-image encryption based on optical wavelet transform and multichannel fractional Fourier transform. Opt. Laser Technol. **57**(4), 343–349 (2014)
31. Liao, X., Shu, C.: Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels. J. Vis. Commun. Image Represent. **28**(4), 21–27 (2015)
32. Pan, S.M., Wen, R.H., Zhou, Z.H., Zhou, N.R.: Optical multi-image encryption scheme based on discrete cosine transform and nonlinear fractional Mellin transform. Multimedia Tools and Applications **76**, 2933–2953 (2017)
33. Chen, T.H., Li, K.C.: Multi-image encryption by circular random grids. Inf. Sci. **189**(7), 255–265 (2012)
34. Arnold, V.I., Avez, A.: Ergodic problems of classical mechanics. Benjamin, New York (1968)
35. Vedral, V., Barenco, A., Ekert, A.: Quantum networks for elementary arithmetic operations. Phys. Rev. A **54**(1), 147–153 (1996)