Int J Theor Phys (2015) 54:526–537
DOI 10.1007/s10773-014-2245-z

Quantum Image Encryption Algorithm Based on Image Correlation Decomposition

Tianxiang Hua · Jiamin Chen · Dongju Pei · Wenquan Zhang · Nanrun Zhou

Received: 1 May 2014 / Accepted: 27 June 2014 / Published online: 9 August 2014

Abstract A novel quantum gray-level image encryption and decryption algorithm based on image correlation decomposition is proposed. 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 series of sub-images. These sub-images are stored into a complete binary tree array constructed previously and then randomly performed by one of the operations of quantum random-phase gate, quantum revolving gate and Hadamard transform. The encrypted image can be obtained by superimposing the resulting sub-images with the superposition principle of quantum states. For the encryption algorithm, the keys are the parameters of random phase gate, rotation angle, binary sequence and orthonormal basis states. The security and the computational complexity of the proposed algorithm are analyzed. The proposed encryption algorithm can resist brute force attack due to its very large key space and has lower computational complexity than its classical counterparts.

Keywords Image correlation decomposition · Quantum computation · Quantum image encryption · Information security

T. -X. Hua · W. -Q. Zhang · N. -R. Zhou (✉)
Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China
e-mail: znr21@163.com

J.-M. Chen
Department of Physics, Nanchang University, Nanchang 330031, China

D. -J. Pei
School of Computer and Information Engineering, Jiangxi Agricultural University, Nanchang 330045, China

N. -R. Zhou
Key Laboratory of Photoeletronics & Telecommunication of Jiangxi Province, Nanchang 330022, China

1 Introduction

Information security has become an important topic during the processing on information storage and transmission. Images are one of the most important information representation models and widely used in modern communications. Some random-phase operations and transforms have been introduced to design encryption algorithms, such as random phase encoding [1–3], Hadamard transform [4, 5], fractional Mellin transform [6] and ect. However, with the development of cryptanalysis and computer technology, ingenious methods for breaking the existing image encryption algorithms are presented successively [7–10], which threaten the existing traditional encryption systems.

Quantum computation has been applied in many fields of information sciences [11]. With the development of quantum computation, classical image processing is naturally extended to quantum scenario. Some methods for representing quantum images have been proposed [12–25]. The quantum image can be represented by color. i.e., a quantum state detected from monochromatic electromagnetic waves through special machines and position, and the storing unit was named Qubit Lattice [12, 13]. By mapping pixels into the real ket of Hilbert space, Latorre proposed a new method to complete image compression combined with pixel states [14]. The image color and position can be encoded into one quantum state by a flexible representation of quantum image (FRQI) [15], which keeps the classical properties of color and position. Then color transformation [16, 17], simple geometric transformation [18, 19], and image watermarking [20] were proposed based on FRQI. A 3D feature space was proposed by Le PQ et al to represent visual complexity of images based on structure, noise and diversity (SND) features extracted from the images [21]. Their method provided a rich understanding of the complexity of visual image, and has important applications to determine the capacity and the feasibility of image processing tasks. Ledesma S et al. proposed an optical analogy of quantum entanglement by means of classical image [22], which showed how to interpret some non-local features of the joint measurement by the bidimensional encoding of two-qubit states. A novel enhanced quantum image representation (NEQR) for digital images was invented, which uses the basis state of a qubit sequence to store the gray-scale value of each pixel in the image for the first time [23]. A quantum image representation for log-polar image (QUALPI) was proposed for the storage and processing of images sampled in the log-polar coordinates, which achieves high efficiency of the new quantum image registration algorithm [24]. Moreover, a method for quantum image processing on image storage, retrieval, compression and segmentation in a quantum system was proposed [25].

Consequently, some new quantum algorithms were developed as new theoretical tools for the security of quantum images. Since dissipative quantum maps can be characterized by sensitive dependence on initial conditions, an image encryption scheme based on quantum logistic map is proposed [26], which pointed out a clear direction for image security with quantum maps. In 2013, Zhou RG et al. proposed the quantum gray-scale image encryption and decryption algorithms based on quantum image geometric transformations, and it unfortunately involves repeated quantum image storages [27]. A robust watermark algorithm for quantum images was also proposed, where the watermark image is embedded into the Fourier coefficients of the quantum carrier image [28]. Akhshani A et al. proposed a new color image encryption scheme based on quantum chaotic systems [29]. Yang YG et al. proposed a novel gray image encryption/decryption scheme based on quantum Fourier transform and double random-phase encoding technique, which is enlightening for introducing more optical information processing techniques into quantum scenario [30]. In 2014, a novel dynamic watermarking scheme for

quantum images using Hadamard transform and FRQI was proposed [31]. The existing quantum image security algorithms provide references for follow-up study in different aspects.

In this paper, the image correlation decomposition is applied in the field of quantum image encryption. At the same time, quantum random-phase gate, quantum revolving gate and Hadamard transform are used to encode color information of quantum images. A detailed theoretical security analysis is given.

The rest of this paper is organized as follows. In Section 2, quantum gray-scale image representation, quantum image correlation decomposition, quantum revolving gate, Hadamard transform and quantum image superposition are introduced. The proposed quantum image encryption and decryption algorithm is given in Section 3. Section 4 is devoted to the theoretical security analysis and the computational complexity analysis. A brief conclusion is drawn in Section 5.

2 Quantum Image Representation and Transformation

2.1 Quantum Gray-Scale Image Representation

Classical image is represented by a matrix with the same size of the image, i.e. the number of pixels. In classical gray image, the pixel value of each point represents the gray-scale value and the position information. For a quantum image, the gray value and the position information of each pixel are stored into the corresponding quantum states, respectively. Therefore, the quantum image is a quantum system composed of quantum states. Figure 1 depicts the workflow of preparing a new quantum image model from the classical image representation.

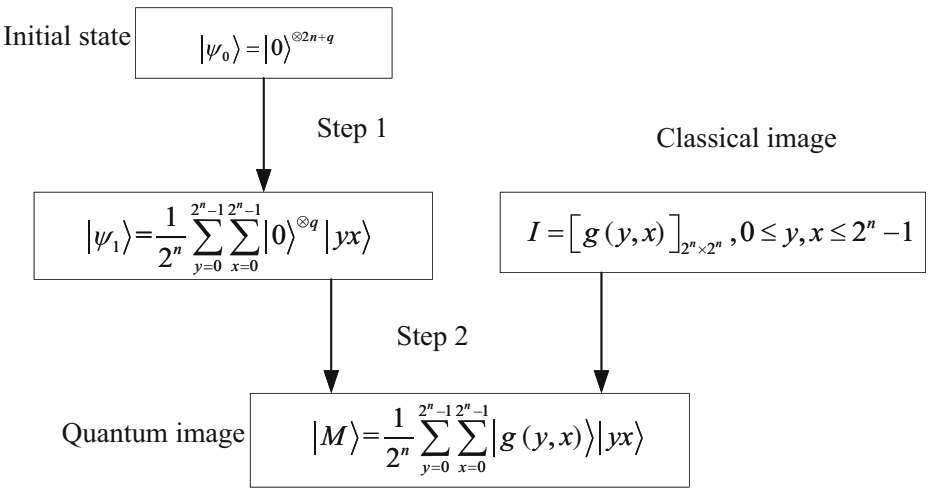

Fig. 1 Preparation of quantum image

Suppose M is a classical image of size $2^n \times 2^n$, $|M\rangle$ is the storage of the whole quantum states for a gray-scale image, the quantum image representation can be expressed as:

$$\begin{aligned} |M\rangle &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |g(y,x)\rangle |yx\rangle \\ |g(y,x)\rangle &= \cos\theta_i |0\rangle + \sin\theta_i |1\rangle, \theta_i \in \left[0, \tfrac{\pi}{2}\right], i = yx = 0, 1, ..., 2^{2n} - 1 \end{aligned} \tag{1}$$

where $\theta = \left(\theta_0, \theta_1, \cdots, \theta_{2^{2n}-1}\right)$ is the vector of angles encoding colors, $|g(y,x)\rangle$ encodes the color information of quantum image, $|i\rangle = |yx\rangle = |y\rangle |x\rangle = |y_{n-1} y_{n-2} \cdots y_0\rangle |x_{n-1} x_{n-2} \cdots x_0\rangle$ encodes the corresponding positions of the quantum images, $|y_{n-1} y_{n-2} \cdots y_0\rangle$ encodes the first n-qubit along the vertical location information while $|x_{n-1} x_{n-2} \cdots x_0\rangle$ encodes the second n-qubit along the horizontal location information, n is the number of quantum bits required for encoding. As a consequence, the unfolded representation for the 2×2 gray-scale image in Fig. 2 can be written as:

$$\begin{aligned} |M\rangle = \frac{1}{2} &[(\cos\theta_0 |0\rangle + \sin\theta_0 |1\rangle) |00\rangle + (\cos\theta_1 |0\rangle + \sin\theta_1 |1\rangle) |01\rangle \\ &+ (\cos\theta_2 |0\rangle + \sin\theta_2 |1\rangle) |10\rangle + (\cos\theta_3 |0\rangle + \sin\theta_3 |1\rangle) |11\rangle] \end{aligned} \tag{2}$$

2.2 Quantum Image Correlation Decomposition

According to the representation of quantum image in (1), we suppose that the locations of k pixels are in the states $|y\rangle |x+1\rangle, |y\rangle |x+2\rangle, \cdots, |y\rangle |x+k\rangle$, respectively. Thus, the gray values of k pixels are represented by $|g(y, x+1)\rangle, |g(y, x+2)\rangle, \cdots, |g(y, x+k)\rangle$, which can be simply rewritten as: $\left|g_{y,x+1}\right\rangle, \left|g_{y,x+2}\right\rangle, \cdots, \left|g_{y,x+k}\right\rangle$, respectively. The k-qubit system composed of k pixels of quantum image can be represented as:

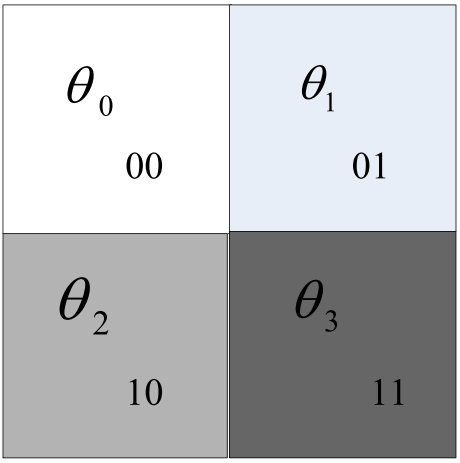

Fig. 2 Gray-scale image of 2×2

$$
\begin{aligned}
&\left|g_{y,x+1}g_{y,x+2^{\cdots}}g_{y,x+k}\right\rangle = \left|g_{y,x+1}\right\rangle \bigotimes \left|g_{y,x+2}\right\rangle \bigotimes^{\cdots} \bigotimes \left|g_{y,x+k}\right\rangle \\
&= \cos\theta_{y,x+1}\cos\theta_{y,x+2^{\cdots}}\cos\theta_{y,x+k-1}cos\theta_{y,x+k}\,|00^{\cdots}00\rangle \\
&+ \cos\theta_{y,x+1}\cos\theta_{y,x+2^{\cdots}}\cos\theta_{y,x+k-1}\sin\theta_{y,x+k}\,|00^{\cdots}01\rangle \\
&+ \cos\theta_{y,x+1}\cos\theta_{y,x+2^{\cdots}}\sin\theta_{y,x+k-1}\cos\theta_{y,x+k}\,|00^{\cdots}01\rangle \\
&\vdots \\
&+ \sin\theta_{y,x+1}\sin\theta_{y,x+2^{\cdots}}\sin\theta_{y,x+k-1}\sin\theta_{y,x+k}\,|11^{\cdots}11\rangle \\
&= \sum_{i=0}^{2^{k-1}} w_i\,|i\rangle = \sum_{i=0}^{N-1} w_i\,|i\rangle
\end{aligned}
\tag{3}
$$

where state vector $|b_{k-1^{\cdots}}b_1b_0\rangle$ is denoted by $|i\rangle$, i represents binary number $b_{k-1}\cdots b_1b_0$ corresponding to decimal number. w_i is the probability amplitude of $|i\rangle$ which satisfies the normalization condition $\sum_{i=0}^{N-1} w_i^2 = 1$. $\left|g_{y,x+1}g_{y,x+2^{\cdots}}g_{y,x+k}\right\rangle$ is called quantum image correlation decomposition. The above quantum system is an N-dimensional Hilbert space, and the probability amplitude of any one-dimensional state vector can be constructed by a sub-image of corresponding superposition state. According to (3), the probability amplitude w_i represents the cosine value of the angle θ_{yx} with the sub-image and the quantum image $|M\rangle$ is divided into N sub-images. Obviously, the original image can be restored by the color information of these sub-images.

2.3 Quantum Revolving Gate and Hadamard Transform

Quantum revolving gate is defined as

$$
R(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \tag{4}
$$

Suppose $|\phi\rangle = \begin{bmatrix} \cos\theta_0 \\ \sin\theta_0 \end{bmatrix}$, then $R(\theta)\,|\phi\rangle = \begin{bmatrix} \cos(\theta_0+\theta) \\ \sin(\theta_0+\theta) \end{bmatrix}$.

The single qubit Hadamard transformation H is a unitary transformation.

$$
H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{5}
$$

$$
H\,|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad H\,|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{6}
$$

Hadamard transformation applied on n qubits can be expressed as

$$
H^{\otimes n}\,|0\rangle = \frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^n-1}|i\rangle \tag{7}
$$

2.4 Superposition of Quantum Images

In quantum mechanics, the quantum state of microcosmic particles is described by using the wave function, which can be fully described by a unit vector in Hilbert space. If $|\psi_1\rangle$ and $|\psi_2\rangle$ are two vectors in a Hilbert space, then

$$
|\psi\rangle = c_1\,|\psi_1\rangle + c_2\,|\psi_2\rangle \tag{8}
$$

$|\psi\rangle$ is also a Hilbert space vector, where c_1, c_2 are two complex numbers which satisfy the condition $|c_1|^2 + |c_2|^2 = 1$. Assume that images M_A and M_B are stored in states $|M_A\rangle$ and $|M_B\rangle$, respectively. According to the principle of quantum states superposition, if $|M_A\rangle$ and $|M_A\rangle$ are two vectors in a Hilbert space, the definition of quantum image superposition is:

$$|M_c\rangle = \alpha\,|M_A\rangle + \beta\,|M_B\rangle \tag{9}$$

where $|M_c\rangle$ is a superposition image, α and β are the image superposing coefficients which should satisfy the normalization condition $|\alpha|^2 + |\beta|^2 = 1$.

3 Quantum Image Encryption and Decryption Algorithm

3.1 Encryption Algorithm

As the encrypting object is a quantum gray-scale image, the corresponding plain-text and cipher-text will also be quantum images. Assume that plaintext quantum image is

$$|M\rangle = \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|g(y,x)\rangle|yx\rangle\,,\ \text{where}\ |g(y,x)\rangle = \cos\theta_i|0\rangle + \sin\theta_i\,|1\rangle\,,\theta_i \in \left[0,\frac{\pi}{2}\right],$$

$i = yx = 0, 1, \ldots, 2^{2n} - 1$. The proposed image encryption algorithm consists of the following steps:

Step 1. $|M\rangle$ is divided into a series of characteristic sub-images $|M_0\rangle\,, |M_1\rangle\,, \cdots |M_{N-1}\rangle$ by utilizing quantum image correlation decomposition.

Step 2. The array of a complete binary tree is constructed by an integer sequence $0, 1, \cdots, N-1$, as shown in Fig. 3. After the array of the complete binary tree is performed preorder traversal, the sub-images are stored into the array of the complete binary tree. $|M_i\rangle$ corresponds to the ith node of the complete binary tree.

Step 3. To encode color information of quantum image, quantum random phase gate, quantum revolving gate and Hadamard transform are randomly performed on these sub-images. For the ith node of the complete binary tree, if $i \bmod 3 = 0$,

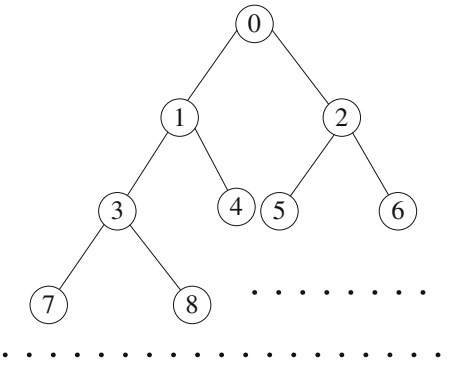

Fig. 3 Array of complete binary tree

perform random phase gate U_k on $|M_i\rangle$. Random phase gate is used to construct a $2n+1$ qubits-based unitary transform C_k.

$$C_k = \left(I \otimes \sum_{y=0}^{2^n-1} \sum_{\substack{x=0 \\ yx \neq k}}^{2^n-1} |yx\rangle \langle yx| \right) + U_k \otimes |k\rangle \langle k| \tag{10}$$

$$U_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{\mathrm{j}2\pi\varphi_k} \end{bmatrix} \tag{11}$$

where φ_k is a real number and distributed uniformly between 0 and 1. The controlled phase matrix C_k is a unitary matrix since $C_k C_k^{\dagger}=I^{\otimes 2n+1}$. Applying a $2n+1$ qubits unitary transform C on quantum image $|M_i\rangle$, one obtains :

$$\begin{aligned} & C\left(|M_i\rangle\right) = \prod_{y=0}^{2^n-1} \prod_{x=0}^{2^n-1} C_{yx} |M_i\rangle \\ & = \frac{1}{2^n} \sum_{y=0}^{2^{n-1}} \sum_{x=0}^{2^{n-1}} \left(\cos\theta_{yx} |0\rangle + e^{\mathrm{j}2\pi\varphi_k} \sin\theta_{yx} |1\rangle\right) |yx\rangle \\ & = |f_i\rangle \end{aligned} \tag{12}$$

If $i \bmod 3 = 1$, perform quantum revolving gate on $|M_i\rangle$. Quantum revolving gate $R\left(\phi_j\right)$ is used to construct a unitary transform R_j.

$$R_j = \left(I \otimes \sum_{y=0}^{2^n-1} \sum_{\substack{x=0 \\ yx \neq j}}^{2^n-1} |yx\rangle \langle yx| \right) + R\left(\phi_j\right) \otimes |j\rangle \langle j| \tag{13}$$

$$R\left(\phi_j\right) = \begin{bmatrix} \cos\phi_j & -\sin\phi_j \\ \sin\phi_j & \cos\phi_j \end{bmatrix} \tag{14}$$

where ϕ_j indicates the rotation angle, and ϕ_j is uniformly distributed from 0 to 2π. The controlled rotation matrix R_j is a unitary matrix since $R_j R_j^{\dagger} = I^{\otimes 2n+1}$. Applying a $2n+1$ qubits unitary transform R on quantum image $|M_i\rangle$, one obtains:

$$\begin{aligned} & R\left(|M_i\rangle\right) = \prod_{y=0}^{2^n-1} \prod_{x=0}^{2^n-1} R_{yx} |M_i\rangle \\ & = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} R(\phi_{yx}) |g(x,y)\rangle |yx\rangle \\ & = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{y=0}^{2^n-1} (\cos(\theta_{yx}+\phi_{yx}) |0\rangle + \sin(\theta_{yx}+\phi_{yx}) |1\rangle) |yx\rangle \\ & = |f_i\rangle \end{aligned} \tag{15}$$

If $i \bmod 3 = 2$, perform Hadamard transform operation on $|M_i\rangle$. Unitary transform T is controlled by a binary key K_1, where $K_1 = k_1 k_2 \cdots k_{2n+1}$, $k_1 = 1$, $k_i \in \{0, 1\}$, $i = 2, 3, \cdots, 2n+1$.

$$\begin{aligned} T|M_i\rangle &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} T(\cos\theta_{yx}|0\rangle + \sin\theta_{yx}|1\rangle)|yx\rangle \\ &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |d_{yx}\rangle|yx\rangle \\ &= |f_i\rangle \end{aligned} \tag{16}$$

where $T = H \overset{2n+1}{\underset{i=2}{\otimes}} H^{k_i}$, $H^{k_i} = \begin{cases} H, & k_i = 1 \\ I, & k_i = 0 \end{cases}$, $i = 2, 3, \cdots, 2n+1$, H is a Hadamard matrix and I is a 2-D identity matrix. The new images $|f_0\rangle, |f_1\rangle, \cdots, |f_{N-1}\rangle$ are obtained by implementing different transform operations in each node according to the residue of i divided by 3.

Step 4. To achieve the final quantum cipher-text image $|f\rangle$, one encrypts all of quantum images $|f_i\rangle$ into the superposition.

$$|f\rangle = \eta_0|f_0\rangle + \eta_1|f_1\rangle + \cdots + \eta_{N-1}|f_{N-1}\rangle \tag{17}$$

where $\eta = (\eta_0, \eta_1, \cdots, \eta_{N-1})$ and $\eta_0^2 + \eta_1^2 + \cdots + \eta_{N-1}^2 = 1$.

Step 5. To obtain the orthonormal basis states $|Q_i\rangle$, one applies Schmidt decomposition to cipher-text image $|f\rangle$.

$$|f\rangle = \sum_{i=0}^{N-1} \beta_i |Q_i\rangle \tag{18}$$

where β_i is a non-negative real number satisfying $\sum_{i=0}^{N-1} \beta_i^2 = 1$.

The quantum image encryption procedure is shown in Fig.4. The encryption algorithm is composed of quantum image correlation decomposition, three transforms and superposition operation.

3.2 Decryption Algorithm

In the encryption algorithm, random phase gate U_k, quantum revolving gate $R(\phi_j)$ and binary sequence K_1 are used to control quantum random-phase operation, quantum revolving operation and Hadamard transform, respectively. The keys involve the parameter φ_k of random phase gate, rotation angle ϕ_j, binary sequence $K_1 = k_1 k_2 \cdots k_{2n+1}$, and orthonormal basis states $K_2 = \{|Q_i\rangle, i = 0, 1 \cdots, N-1\}$. The decryption process is as follows.

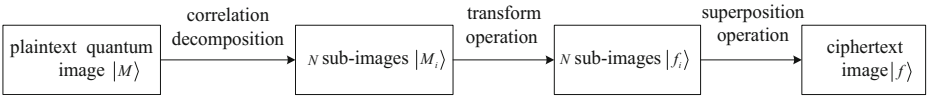

Fig. 4 Flow chart of quantum image encryption algorithm

Step 1. The cipher-text image $|f\rangle$ is obtained by making measurements on the received quantum images $|f_i\rangle$. Applying $K_2 = \{|Q_i\rangle, i = 0, 1, \cdots, N-1\}$ as the project operators to perform the projective measurements, i.e.,

$$P = \sum_{i=0}^{N-1} P_i |Q_i\rangle \langle Q_i| \tag{19}$$

$$p_i = \frac{t_i}{t - t_i} \tag{20}$$

where t represents the total number of the measurements, t_i is the number of the measurements coincided with the results of $|f_i\rangle$.

Step 2. According to the array of the complete binary tree, different inverse transforms are executed to get the sub-images $|M_0\rangle, |M_1\rangle, \cdots, |M_{N-1}\rangle$. For the node i of the complete binary tree, if $i \bmod 3 = 0$, the decryption operation is performed on $|f_i\rangle$ with the key φ_k.

$$\begin{aligned} &C^{-1}(|f_i\rangle) = \prod_{y=0}^{2^n-1}\prod_{x=0}^{2^n-1} C_{yx}^{\dagger}(|f_i\rangle) \\ &= \prod_{y=0}^{2^n-1}\prod_{x=0}^{2^n-1} C_{yx}^{\dagger}\left(\frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}(\cos\theta_{yx}|0\rangle + e^{\mathrm{i}2\pi\varphi_{yx}}\sin\theta_{yx}|1\rangle)|yx\rangle\right) \\ &= |M_i\rangle \end{aligned} \tag{21}$$

where $C_{yx}^{\dagger}$ is the Hermitian conjugate of C_{yx}. If $i \bmod 3 = 1$, perform the decryption operation on $|f_i\rangle$ with the key ϕ_j.

$$\begin{aligned} &R^{-1}(|f_i\rangle) = \prod_{y=0}^{2^n-1}\prod_{x=0}^{2^n-1} R_{yx}^{\dagger}(|f_i\rangle) \\ &= \prod_{y=0}^{2^n-1}\prod_{x=0}^{2^n-1} R_{yx}^{\dagger}\frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1} R(\phi_{yx})|g(x,y)\rangle|yx\rangle \\ &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|g(y,x)\rangle|yx\rangle \\ &= |M_i\rangle \end{aligned} \tag{22}$$

If $i \bmod 3 = 2$, execute the decryption operation on $|f_i\rangle$ with the key K_1, where T^{-1} is the inverse operator of T.

$$\begin{aligned} &T^{-1}|f_i\rangle = \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1} T^{-1}\left|d_{yx}\right\rangle|yx\rangle \\ &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1} T^{-1}\{T(\cos\theta_{yx}|0\rangle + \sin\theta_{yx}|1\rangle)\}|yx\rangle \\ &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}(\cos\theta_{yx}|0\rangle + \sin\theta_{yx}|1\rangle)|yx\rangle \\ &= |M_i\rangle \end{aligned} \tag{23}$$

Step 3. According to the nature of quantum image correlation decomposition, the color information of the original image is rebuilt by these sub-images.

4 Algorithm Analyses

Since a practical and useful quantum computer is unavailable, there is lack of quantum hardware to simulate the quantum image encryption algorithm. Thus the proposed algorithm is limited to the theoretical analyses on key space, security and computational complexity.

4.1 Key Space

The key space of a good image encryption algorithm should be large enough to make brute-force attack infeasible. It is recommended in Ref.[32] that the ideal key space should be larger than 2^{100} while considering the current computation speed of a general computer. In the proposed algorithm, random phase gate U_k, quantum revolving gate $R\left(\phi_j\right)$ and binary sequence K_1 are used to control quantum random-phase operation, quantum revolving operation and Hadamard transform, respectively. The keys are composed of the parameter φ_k of random phase gate, rotation angle ϕ_j, binary sequence K_1, and orthonormal basis states K_2. Here, φ_k is a real number and distributed uniformly between 0 and 1, ϕ_j is uniformly distributed from 0 to 2π, $k_i \in \{0, 1\}$, $i = 2, 3, \cdots, 2n + 1$. φ_k, ϕ_j imply a very large key space, and the key space of K_1 is 2^{2n}. The total key space is a very huge number, thus the proposed algorithm can resist brute-force attack.

4.2 Security

The encrypted image is stored and transmitted in the form of quantum states. Since the quantum no-cloning theorem and quantum uncertainty principle, the process of exactly replicating any unknown quantum state can not be realized in quantum mechanics. If the attacker wants to obtain the information about the quantum state, he has to measure it, which will make the quantum state collapse randomly into an eigenstate of the measurement operators irreversibly. Therefore, the legitimate users can detect whether the quantum information has suffered from attacks or not. So the proposed quantum encryption algorithm has provable security and will immune from the interception with unlimited computing power of eavesdroppers due to the principles of quantum mechanics. Zhou RG et al.'s scheme realized quantum image encryption by utilizing quantum image geometric transformations. Unfortunately, it involves repeated quantum image storage and the adversary can get plaintext image as long as he decrypts a quantum image from the full-binary-tree array. However, the proposed encryption algorithm successfully solved these drawbacks. In the proposed algorithm, the whole quantum image is divided into a series of sub-images, and these sub-images are encrypted by utilizing quantum random-phase gate, quantum revolving gate and Hadamard transform. The receiver has to decrypt all quantum images from the array of the complete binary tree to obtain the sub-images, and then recover the plaintext image under quantum information theory. The proposed quantum image encryption algorithm increased the decryption difficulty. Moreover, the quantum state measurements are the most essential decryption operations. Therefore, the proposed algorithm can greatly improve the security of image encryption and decryption.

4.3 Computational Complexity

Assume that M is a $2^n \times 2^n$ original image. There are 2^{2n} pixels in the original image. For quantum image encryption algorithm, due to the properties of quantum parallel computation, the use of quantum transforms speeds up the image encryption and decryption.

The computational complexity of the proposed encryption algorithm depends on quantum random-phase operation, quantum revolving operation and Hadamard transform. The complexity of quantum random-phase operation for a quantum image is $O(n)$. Since the computational complexity is the same as quantum random-phase operation, revolving operation and Hadamard transform, and the encryption algorithm needs to perform encryption operation on N sub-images at the same time. So the total computational complexity is $O(Nn)$. By analyzing the corresponding classical image encryption algorithm, random-phase operation is performed on the image by using 2^{2n} multiplication operations, so the computational complexity is $O\left(2^{2n}\right)$. The computational complexity is the same as random-phase operation, revolving operation and Hadamard transform. Thus, the total computational complexity is $O\left(N2^{2n}\right)$. Therefore, the computational complexity of the proposed encryption algorithm is lower than its classical counterparts.

5 Conclusion

We utilized the superposition and measurement principle of quantum states to establish the correlation among image pixels and proposed a novel quantum image encryption and decryption algorithm based on image correlation decomposition. The encryption algorithm is realized by combining quantum image correlation decomposition, three transforms with superposition operation. Quantum random-phase operation, quantum revolving operation and Hadamard transform are used to encode color information of these sub-images, which increases the decryption difficulty. The encrypted image can be obtained by superimposing the resulting sub-images. A detailed theoretical security and computational complexity analysis of the encryption algorithm is given. The proposed encryption algorithm can resist brute-force attack due to its very large key space. Moreover, the proposed algorithm has lower computational complexity than its classical counterparts. It implements quantum image encryption by combining quantum information theory with classical image encryption technology, which introduces a new theoretical tool for image encryption.

Acknowledgments This work is supported by the National Natural Science Foundation of China (grant no. 61262084), the Natural Science Foundation of Jiangxi Province, China (grant no. 20122BAB201031), the Foundation for Young Scientists of Jiangxi Province (Jinggang Star) (grant no. 20122BCB23002), the Research Foundation of the Education Department of Jiangxi Province (grant nos. GJJ14138 and GJJ13057), the Open Project of Key Laboratory of Photoeletronics & Telecommunication of Jiangxi Province (grant no. 2013003), and the Innovation Project of Jiangxi Graduate Education (grant no. YC2012-S009).

References

1. Javidi, B., Zhang, G., Li, J.: Opt. Eng. **35**, 2506 (1996)
2. Peng, X., Zhang, P., Wei, H., Yu, B.: Opt. Lett. **31**, 1044 (2006)
3. Tao, R., Xin, Y., Wang, Y.: Opt. Express **15**, 16067 (2007)
4. Maity, S.P., Kundu, M.K.: Inform. Sci. **181**, 450 (2011)
5. Aung, A., Ng, B.P., Rahardja, S.: J. Signal Process. Sys. **64**, 319 (2011)
6. Zhou, N.R., Wang, Y.X., Gong, L.H.: Opt. Commun. **284**, 3234 (2011)
7. Solak, E., Rhouma, R., Belghith, S.: Opt. Commun. **283**, 232 (2010)
8. Rhouma, R., Solak, E., Belghith, S.: Commun. Nonlinear Sci. Numer. Simulat. **15**, 1887 (2010)
9. Zhang, Y., Xiao, D.: Nonlinear Dynam. **72**, 751 (2013)
10. Li, C., Liu, Y., Zhang, L.Y., Chen, M.Z.: Int. J. Bifurcat. Chaos **23**, 1350075 (2013)
11. Nielsen, M.A., Chuang, I.L.: Cambridge University Press (2010)

12. Venegas-Andraca, S.E., Bose, S.: Conference on Quantum Information and Computation, Orlando. Fl. **5105**, 137 (2003)
13. Venegas-Andraca, S.E., Ball, J.L.: Quantum Inf. Process. **9**, 1 (2010)
14. Latorre, J.I.: Quantum Phys. 0510031 (2005)
15. Le, P.Q., Dong, F.Y., Hirota, K.: Quantum Inf. Process. **10**, 63 (2011)
16. Le, P.Q., Iliyasu, A.M., Dong, F.Y., Hirota, K.I.: JACIII **15**, 698 (2011)
17. Sun, B., Le, P.Q., Iliyasu, A.M., Yan, F., Garcia, J.A., Dong, F., Hirota, K.: Intelligent Signal Processing (WISP), 2011 IEEE 7th International Symposium on. Floriana **1** (2011)
18. Le, P.Q., Iliyasu, A.M., Dong, F.Y., Hirota, K.: IAENG Int. J. Apl. Math. **40**, 113 (2010)
19. Le, P.Q., Iliyasu, A.M., Dong, F.Y., Hirota, K.: Theor. Comput. Sci. **412**, 1406 (2011)
20. Iliyasu, A.M., Le, P.Q., Dong, F.Y., Hirota, K.: Inform. Sci. **186**, 126 (2012)
21. Le, P.Q., Iliyasu, A.M., Garcia, J.A., Dong, F., Hirota, K.: JACIII **16**, 631 (2012)
22. Goldin, M.A., Francisco, D., Ledesma, S.: Opt. Commun. **284**, 2089 (2011)
23. Zhang, Y., Lu, K., Gao, Y.H., Wang, M.: Quantum Inf. Process. **12**, 2833 (2013)
24. Zhang, Y., Lu, K., Gao, Y.H., Xu, K.: Quantum Inf. Process. **12**, 3101 (2013)
25. Li, H.S., Zhu, Q.X., Song, L., Shen, C.Y., Zhou, R.G., Mo, J.: Quantum Inf. Process. **12**, 2269 (2013)
26. Akhshani, A., Akhavan, A., Lim, S.C., Hassan, Z.: Commun. Nonlinear Sci. Numer. Simulat. **17**, 4653 (2012)
27. Zhou, R.G., Wu, Q., Zhang, M.Q., Shen, C.Y.: Int. J. Theor. Phys. **52**, 1802 (2013)
28. Zhang, W.W., Gao, F., Liu, B., Wen, Q.Y., Chen, H.: Quantum Inf. Process. **12**, 793 (2013)
29. Abd El-Latif, A.A., Li, L., Wang, N., Han, Q., Niu, X.M.: Sig. Process **.93**, 2986 (2013)
30. Yang, Y.G., Xia, J., Jia, X., Zhang, H.: Quantum Inf. Process. **12**, 3477 (2013)
31. Song, X.H., Wang, S., Abd El-Latif, A.A., Niu, X.M.: Multimedia Syst. **20**, 379 (2014)
32. Alvarez, G., Li, S.J.: Int. J. Bifurcat. Chaos **16**, 2129 (2006)