Int J Theor Phys (2017) 56:1961–1982
DOI 10.1007/s10773-017-3341-7

A Simple Encryption Algorithm for Quantum Color Image

Panchi Li[1] · **Ya Zhao**[1]

Received: 13 September 2016 / Accepted: 13 March 2017 / Published online: 22 March 2017

Abstract In this paper, a simple encryption scheme for quantum color image is proposed. Firstly, a color image is transformed into a quantum superposition state by employing NEQR (novel enhanced quantum representation), where the R,G,B values of every pixel in a 24-bit RGB true color image are represented by 24 single-qubit basic states, and each value has 8 qubits. Then, these 24 qubits are respectively transformed from a basic state into a balanced superposition state by employed the controlled rotation gates. At this time, the gray-scale values of R, G, B of every pixel are in a balanced superposition of 2^{24} multi-qubits basic states. After measuring, the whole image is an uniform white noise, which does not provide any information. Decryption is the reverse process of encryption. The experimental results on the classical computer show that the proposed encryption scheme has better security.

Keywords Image processing · Quantum image representing · Quantum image processing · Quantum image encrypting

1 Introduction

With the development of multimedia information technology, information security issues are gradually put on the agenda. The image is one of the important tools of carrying information, it has been widely studied. The classic image processing is a relatively mature discipline. The study of quantum image processing begins with the establishment of the form of quantum image representation. For the classic image processing, the relevant technologies (e.g., image encryption, image geometric transformation, image enhancement,

✉ Panchi Li
lipanchi@vip.sina.com

[1] School of Computer & Information Technology, Northeast Petroleum University, Daqing 163318, China

image compression) have developed quite mature [1–14]. Many classic image processing problems, such as image transformation, image security, are built on the basis of the representation of an image. Similarly, quantum image processing also needs to select a reasonable representation and storage method. At present, there is no uniform or universally accepted definition about the representation of quantum image. Existing representation basically draws on the classic image description method. That is, how to encode the pixel's gray (color) and position, and describe it into a quantum superposition state.

In terms of quantum image representation, Yan et al. [29] has made a detailed analysis of the existing methods. At present, the main quantum image representation are as follows: (1) Quantum image representation based on Qubit Lattice [15–17]. In this method, according to the different wavelength of the electromagnetic wave, the monochromatic electromagnetic wave is geometrically mapped and stored in the quantum state. (2) Quantum image representation based on quantum entanglement [18]. This method makes the corresponding pixels in the image by quantum entanglement. However, this method can only store and process the binary image, which limits the application of this method. (3) Flexible Representation of Quantum Images (FRQI) [19–22]. In this method, the gray level and the position of the pixels are expressed as a normalized quantum superposition state, and a method for making such a quantum state is given. However, this method can only describe the monochrome gray level image. When describing a color image, need to use three qubits stored three color gray-scale information. (4) NEQR (novel enhanced quantum representation) [23]. By using this method, some classical image processing algorithms can be easily extended to quantum images. For these models, only in NEQR, the pixel color values are represented as basic state of qubits, rather than the probability amplitude of basic state, which eliminates the influence of measurement process and is currently the most ideal quantum image representing method. In addition, the video signal is another type of digital signal different from the digital image, and Yan et al. [30] gives the coding method of the video signal, which further enriches the emerging research field of quantum information processing.

Quantum image encryption is one of the important branches of quantum image processing. In an encryption scheme, the data are encrypted and transmitted by the sender in public environment, and it only can be decrypted by the designated receiver with the decryption key. Although the secret information can be detected by the attacker, he/she has no way to get it. As the quantum counterpart of classical encryption schemes, quantum image encryption has been developed rapidly in recent years. However, so far, the literatures in this direction are still relatively scarce. Based on quantum image geometric transformations, Zhou et al. [24] presented a quantum image encryption scheme. However, this encryption method does not follow the principle of quantum mechanics. In [25, 26], Yang et al. deeply studies the problem of quantum image encryption, and proposed an encryption scheme that can be run on future quantum computer. In Yang's approach, the color information of each pixel is encoded by three qubits $|r\rangle$, $|g\rangle$, $|b\rangle$ that represent three primary colors of red, green, blue, respectively. However, the color values of the pixels are encoded with probability amplitude of qubits. By the influence of quantum states collapse, during the measurement, this method is difficult to obtain accurate pixel values. In view of this, we propose an novel color image encryption method. In our scheme, we use the NEQR model to represent the color image, in which 24 qubits are employed to represent the pixel gray scale values of each pixel. The encryption process is achieved by employing the controlled rotation gates. In the encrypted image, the color value of each pixel is a balanced superposition of 2^{24} basic states. After measuring, the whole image is an uniform white noise, which does not provide any information. Although the encryption process is very simple, but the encryption effect is ideal.

The rest of this paper is organized as follows. The next section introduces the NEQR model, and then the represent and encryption method of color image are given in Section 2. In Section 3, we simply introduce the measurement of quantum image. In Section 4, we present the simulation results on the classical computer. Finally, a short conclusion is given in Section 5.

2 Novel Enhanced Quantum Representation (NEQR)

The NEQR have been proposed in [23]. While the FRQI encodes a gray-scale value of 8 bits in 1 qubit, the NEQR represents it in a binary string of 8 qubits. In the NEQR representation, the gray-scale image $f(Y, X)$ with $n \times n$ pixels is expressed by the following equation.

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

where $f(Y, X) = C_{YX}^0 C_{YX}^1 \cdots C_{YX}^{q-1}$, $C_{YX}^k \in \{0, 1\}$, $f(Y, X) \in \{0, 1, \cdots, 2^{q-1}\}$.

In order to explain this scheme in detail, we use a small image with 2×2 pixels in Fig. 1 as an example image, and the following equation shows its NEQR representation, where the range of gray scale is from 0 to 255.

$$\begin{aligned} |I\rangle &= 0.5(|(0)_{\text{dec}}\rangle|00\rangle + |(100)_{\text{dec}}\rangle|01\rangle + |(200)_{\text{dec}}\rangle|10\rangle + |(255)_{\text{dec}}\rangle|11\rangle) \\ &= 0.5|(00000000)_{\text{bin}}\rangle|00\rangle + 0.5|(01100100)_{\text{bin}}\rangle|01\rangle \\ &+ 0.5|(11001000)_{\text{bin}}\rangle|10\rangle + 0.5|(11111111)_{\text{bin}}\rangle|11\rangle. \end{aligned} \tag{2}$$

3 Quantum Encryption Scheme for Color Image

As mentioned earlier, for a $2^n \times 2^n$ image of the gray range of $0 \sim 2^q - 1$, the $q + 2n$ qubits are needed to represent it by NEQR. For a color image of gray scale range $0 \sim 2^8 - 1$, each primary color (R or G or B) needs 8 qubits. Therefore, for a $2^n \times 2^n$ color image of gray scale range $0 \sim 2^8 - 1$, $24 + 2n$ qubits are need to represent it by NEQR. The specific implementation scheme of quantum encryption algorithm for color image is described as follows.

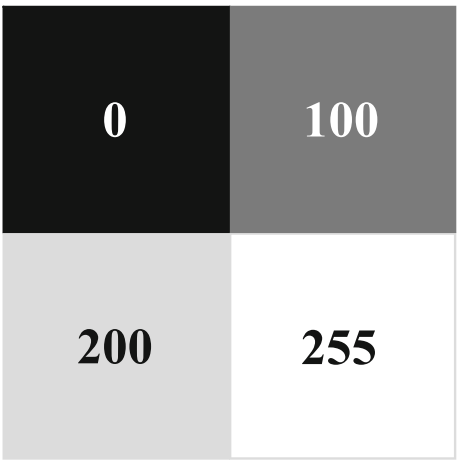

Fig. 1 2×2, 256-level image and its NEQR representation

3.1 Preparation of NEQR-Based Quantum Image

First, we need to prepare $24 + 2n$ qubits in the state of $|0\rangle$. The tensor product of these 24 qubits is written as $|0\rangle^{\otimes(24+2n)}$. Suppose that the binary number of the R,G,B values of pixel $P(Y, X)$ is written as

$$\begin{aligned} f(Y,X) &= C_{YX}^{R0}\cdots C_{YX}^{R7}C_{YX}^{G0}\cdots C_{YX}^{G7}C_{YX}^{B0}\cdots C_{YX}^{B7} \\ &= C_{YX}^{0}\cdots C_{YX}^{7}C_{YX}^{8}\cdots C_{YX}^{15}C_{YX}^{16}\cdots C_{YX}^{23}, \end{aligned} \tag{3}$$

where $C_{YX}^{i} \in \{0, 1\}, i = 0, 1, \cdots, 23$.

In NEQR, an important operator is U_{YX}, and the main work of U_{YX} is Ω_{YX}. This operator converts the R,G,B values of pixel $P(Y, X)$ to quantum state $|f(Y, X)\rangle$ as shown in following equation, and its corresponding quantum circuit is shown in Fig. 2.

$$\Omega_{YX}|0\rangle^{\otimes 24} = \otimes_{i=0}^{23}(\Omega_{YX}^{i}|0\rangle) = \otimes_{i=0}^{23}|0 \oplus C_{YX}^{i}\rangle = \otimes_{i=0}^{23}|C_{YX}^{i}\rangle = |f(Y, X)\rangle. \tag{4}$$

According to NEQR representation, a $2^n \times 2^n$ color image can be described as follows.

$$|\Psi_0\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|f(Y, X)\rangle|YX\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\otimes_{i=0}^{23}|C_{YX}^{i}\rangle|YX\rangle. \tag{5}$$

Next, taking a 2×2 color image in Fig. 3 as an example, we introduce the specific implementation methods of NEQR image. In Fig. 3, the R,G,B values of the 4 pixels are: $f(00)$=[0, 128, 128], $f(01)$=[128, 0, 128], $f(10)$=[128, 128, 0], $f(11)$=[128, 128, 128]. To facilitate the description of the physical implementation of quantum image, we first introduce the concept of the quantum NOT gate and the controlled-NOT gate.

Quantum NOT gate is a single qubit gate, it can be describe by the matrix $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. This gate's role in a single qubit is to flip the state of the qubit, namely, $X|0\rangle = |1\rangle, X|1\rangle = |0\rangle$. The controlled-NOT gate is a multi-qubits gate, the corresponding quantum circuits is shown in Fig. 4.

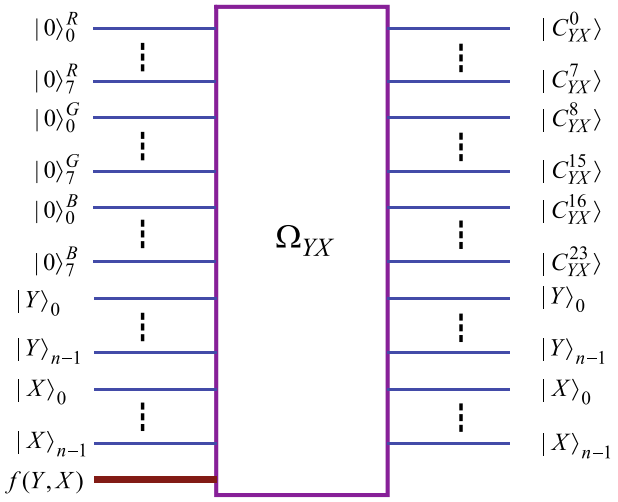

Fig. 2 The black-box circuit of quantum operation Ω_{YX}, which transforms color value $f(Y, X)$ into the quantum state $|f(Y, X)\rangle$ as in (4)

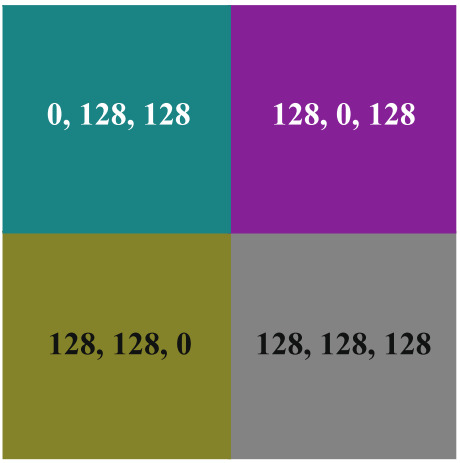

Fig. 3 A color image of size of 2×2

In Fig. 4, the first n qubits of $|x_1\rangle, |x_2\rangle, \cdots, |x_n\rangle$ are the control qubits, and the last one $|\varphi\rangle$ is the target qubit. The notation "$\oplus$" on the $|\varphi\rangle$ denotes the quantum NOT gate. The notation "$\bullet$" on the control qubits indicates that the target qubit $|\varphi\rangle$ is controlled by this control qubit only when it lives in state $|1\rangle$. Similar, the notation "$\circ$" on the control qubits indicates that the target qubit $|\varphi\rangle$ is controlled by this control qubit only when it lives in state $|0\rangle$. When and only when all control bits are satisfied with the control condition, the target qubit $|\varphi\rangle$ is flipped by quantum NOT gate [27].

As a matter of fact, the NEQR representation provides the interface of the color image from the classical domain to the quantum domain. Next, in order to explain the concrete realization method of a NEQR-based color image, taking the 2×2 color image in Fig. 3 as an example, the quantum circuit of transforming a classical image into a NEQR-based quantum image is given in Fig. 5.

In Fig. 5, $|\Psi_0\rangle = |0\rangle^{\otimes 26}$, the $|\Psi_1\rangle$ and the $|\Psi_2\rangle$ are written as

$$|\Psi_1\rangle = \frac{1}{2}\left(\sum_{Y=0}^{1}\sum_{X=0}^{1}|0\rangle^{24} \otimes |YX\rangle\right), \tag{6}$$

$$\begin{aligned}|\Psi_2\rangle = \tfrac{1}{2}(&|00000000, 10000000, 10000000\rangle|00\rangle + \\ &|10000000, 00000000, 10000000\rangle|01\rangle + \\ &|10000000, 10000000, 00000000\rangle|10\rangle + \\ &|10000000, 10000000, 10000000\rangle|11\rangle).\end{aligned} \tag{7}$$

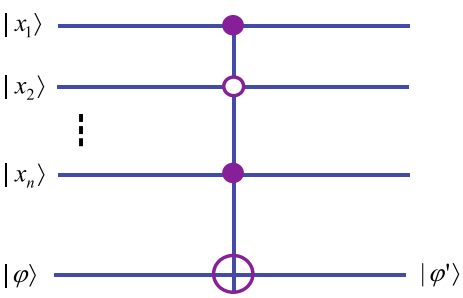

Fig. 4 Quantum circuit of controlled-NOT gate

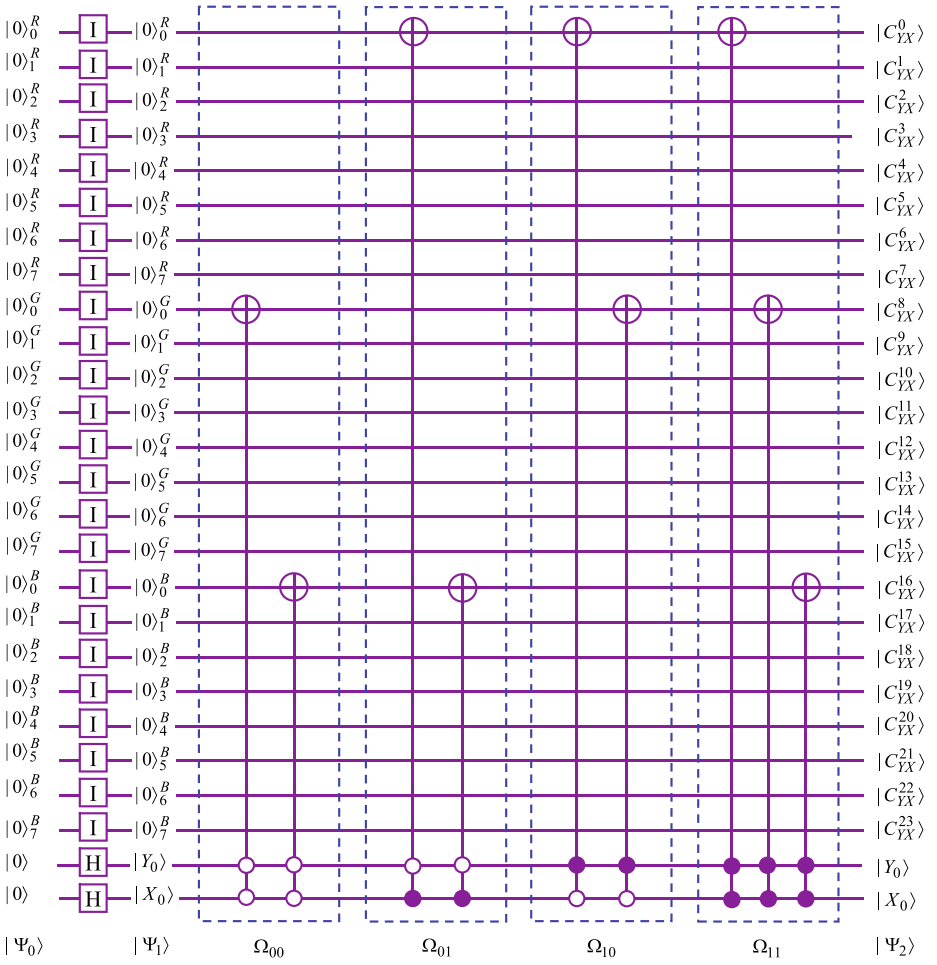

Fig. 5 Quantum circuit of transforming the classical image into the corresponding quantum version

The $|\Psi_2\rangle$ in (7) is a NEQR-based quantum image corresponding to the 2×2 classical image in Fig. 3.

3.2 Encrypt Scheme of Quantum Color Image

According to NEQR, the R,G,B values of pixel $P(Y, X)$ are stored in the basic state consisting of 24 qubits $|C_{YX}^0\rangle, |C_{YX}^1\rangle, \cdots, |C_{YX}^{23}\rangle$, rather than storing in the probability amplitude of the basic state. This basic state is a deterministic state without any randomness. The binary numbers of this basic state are the R,G,B values of the corresponding pixel, which is the advantage of NEQR. For example, the basic state $|10000000, 00000000, 10000000\rangle$ denote that the R,G,B values of $R = 128$, $G = 0$, $B = 128$.

In the encryption method proposed in this paper, all 24 qubits $|C_{YX}^0\rangle, |C_{YX}^1\rangle, \cdots, |C_{YX}^{23}\rangle$ are randomly rotated $\pi/4$ or $-\pi/4$. As a result, the color value of each pixel is no longer in a determined basic state, but in a balanced superposition state of containing 2^{24} basic states. In

this case, the color image is an uniform white noise which does not contain any information of the original image after it is measured. Next, we introduce the specific rotation method.

For a $2^n \times 2^n$ color image, first, generate a random sequence of length 24×2^{2n} and values from the $\{-1, 1\}$.

$$S = 2 * round(rand(2^n, 2^n, 24)) - 1, \tag{8}$$

where the $rand(n, m, p)$ is a MATLAB function which generates $n \times m \times p$ random numbers uniformly distributed in the interval $(0, 1)$, and the $round$ is a rounding function. In subsequent experiments, the specific version of MATLAB is 2014a.

It is worth noting that, the rand() function returns a pseudo-random number, not the true random number. This may lead to an inaccuracy of simulation process. Due to the lack of hardware devices that can generate truly random numbers, therefore, limited by the hardware environment, at present, we can only use the rand() function to simulate the performance of the proposed scheme, which is also the most commonly used method of other similar literatures.

A single qubit rotation gate is defined as

$$R(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}. \tag{9}$$

Let $R^i_{YX} = R(S(Y, X, i) \times \pi/4)$, $\tilde{R}_{YX} = \otimes^{23}_{i=0} R^i_{YX}$, then

$$\tilde{R}_{YX}(\otimes^{23}_{i=0}|C^i_{YX}\rangle) = \otimes^{23}_{i=0}(R^i_{YX}|C^i_{YX}\rangle) = \otimes^{23}_{i=0}|\hat{C}^i_{YX}\rangle. \tag{10}$$

According to the principle of quantum computation, the controlled random rotation operator of color qubits of the pixel (Y, X) in the color image can be defined as follows.

$$R_{YX} = \left(I^{\otimes 24} \otimes \sum_{j=0}^{2^n-1} \sum_{i=0, ji \neq YX}^{2^n-1} |ji\rangle\langle ji| \right) + \tilde{R}_{YX} \otimes |YX\rangle\langle YX|. \tag{11}$$

The rotation operator of the whole color image can be composed of 2^{2n} sub operator R_{YX} as follows.

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

Taking the 2×2 color image in Fig. 3 as an example, the quantum circuit of performing random rotation is shown in Fig. 6.

3.3 Security of Encrypted Image

In our quantum encryption scheme, the security of the encrypted image is guaranteed by following two points.

(1) For the color image after encryption, the color value of all pixels is no longer in the determined basic state, but in a balanced superposition state of 2^{24} basic states.

Taking the first pixel in Fig. 3 as an example, the color value of this pixel is $f(0, 0) = [0, 128, 128]$, the corresponding qubits' basic state is $|C_{00}\rangle = |00000000, 10000000,$

10000000⟩. The rotation of these qubits is only 4 cases, namely, rotating $|C_{00}^{i}\rangle = |0\rangle$ through $\pm\pi/4$, and rotating $|C_{00}^{i}\rangle = |1\rangle$ through $\pm\pi/4$. The specific rotation is as follows.

$$|C_{00}^{i_1}\rangle = \begin{bmatrix} \cos(\frac{\pi}{4}) & -\sin(\frac{\pi}{4}) \\ \sin(\frac{\pi}{4}) & \cos(\frac{\pi}{4}) \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = |+\rangle, \tag{13}$$

$$|C_{00}^{i_2}\rangle = \begin{bmatrix} \cos(-\frac{\pi}{4}) & -\sin(-\frac{\pi}{4}) \\ \sin(-\frac{\pi}{4}) & \cos(-\frac{\pi}{4}) \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle, \tag{14}$$

$$|C_{00}^{i_3}\rangle = \begin{bmatrix} \cos(\frac{\pi}{4}) & -\sin(\frac{\pi}{4}) \\ \sin(\frac{\pi}{4}) & \cos(\frac{\pi}{4}) \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{-|0\rangle + |1\rangle}{\sqrt{2}} = -|-\rangle, \tag{15}$$

$$|C_{00}^{i_4}\rangle = \begin{bmatrix} \cos(-\frac{\pi}{4}) & -\sin(-\frac{\pi}{4}) \\ \sin(-\frac{\pi}{4}) & \cos(-\frac{\pi}{4}) \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = |+\rangle. \tag{16}$$

It can be known that, regardless of the situation, after the rotation, the $|C_{00}^{i}\rangle$ is in a balanced (equal probability distribution) superposition state of $|0\rangle$ and $|1\rangle$. Therefore, after the rotation, the tensor product of 24 qubits is in an equilibrium (equal probability distribution) superposition of 2^{24} basic states.

It is worth noting that, when the basic states $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$ are used as measurement operators, the state represent the color value of a pixel is a determined basic state for the color encryption image. However, the proposed scheme is still secure. From (13–16), after the encryption, the basic state $|0\rangle$ is transformed into $|+\rangle$ and $|-\rangle$ with equal probability, and the basic state $|1\rangle$ is also performed by the same transformation. In this case, each qubit has an error measurement probability of 50%. Therefore, the results are similar to those measured using basic states $|0\rangle$ and $|1\rangle$. Thus, the security of the encrypt scheme is only rely on class random function rand(n, m, p).

(2) The key space is large enough.

In our quantum encryption scheme, the *Key* is a random arrangement of $2^n \times 2^n \times 24 = 3 \times 2^{2n+3}$ 1 and -1. It can be seen, the size of the key space is $2^{3\times 2^{2n}+3}$. Therefore, the encrypted image has a large key space, enough to resist brute force attacks of illegal users.

3.4 Decryption of Encrypted Image

Since the encryption strategy proposed in this paper is designed based on quantum computer, so all the operators are reversible and unitary, the inverse operator is its own conjugate transpose, and the decryption procedure is just the inverse of the encryption procedure. According to the reversibility of quantum computing, the decryption process can be achieved by employing the conjugate transpose of encryption operators. In this phase, the key is needed to decrypt the encrypted image. Our decryption procedure is briefly summarized as follows.

First of all, legitimate receiver gets the secret key S in (8) through sharing it with sender, and then he/she constructs the following rotation matrix

$$\tilde{R}_{YX} = \bigotimes_{i=0}^{23} \begin{bmatrix} \cos(S(Y, X, i) \times \pi/4) & -\sin(S(Y, X, i) \times \pi/4) \\ \sin(S(Y, X, i) \times \pi/4) & \cos(S(Y, X, i) \times \pi/4) \end{bmatrix}, \tag{17}$$

$$R_{YX} = \left(I^{\otimes 24} \otimes \sum_{j=0}^{2^n-1} \sum_{i=0, ji\neq YX}^{2^n-1} |ji\rangle\langle ji| \right) + \tilde{R}_{YX} \otimes |YX\rangle\langle YX|. \tag{18}$$

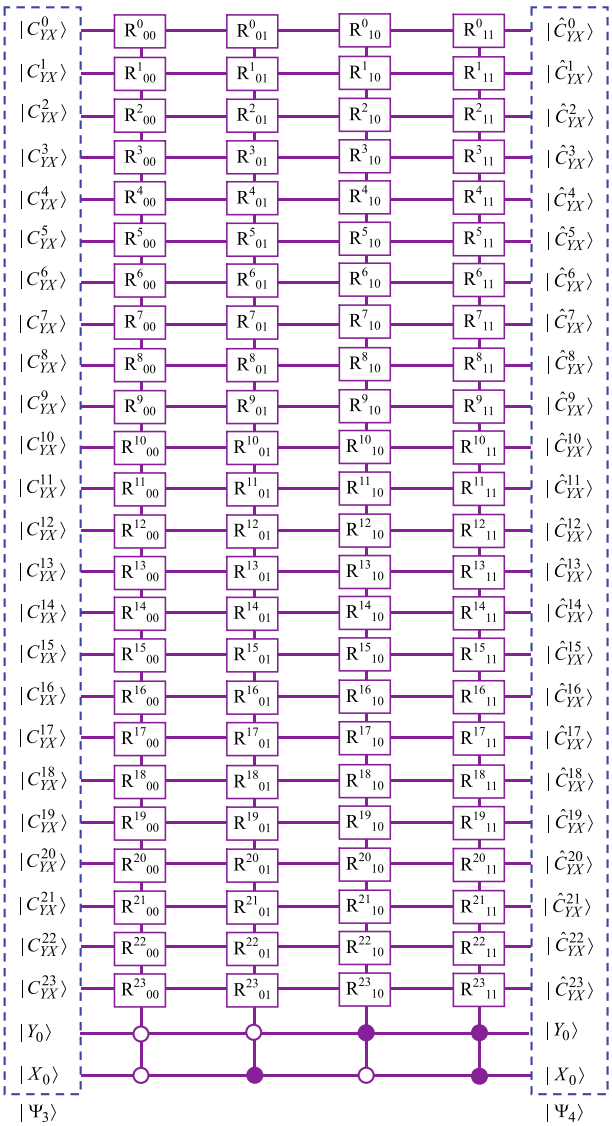

Fig. 6 Quantum circuit of performing random rotation of qubit $C^i_{YX}, i = 0, 1, \cdots, 23$

The decryption operation of encrypted image can be achieved by following unitary operator

$$R = \left(\prod_{Y=0}^{2^n-1} \prod_{X=0}^{2^n-1} R_{YX} \right)^{\dagger}, \tag{19}$$

where $R^{\dagger}$ denotes the conjugate transpose R. Specifically, the decryption process can be described as $|I\rangle_{decryption} = R|I\rangle_{encryption}$.

3.5 Quantum Image Measurement

3.5.1 Measurement of Quantum Image after Decryption

According to the NEQR scheme, for the decrypted image, only the R,G,B values of every pixel are stored in the determined basic state of multi-qubits, and the position of the pixel is still stored in the superposition state with randomness. Therefore, each measurement will lead to the collapse of a quantum system, which makes the quantum superposition system collapse to a certain basic state. Thus, for each measurement, we can only get the information of one pixel corresponding to the collapsed basic state. Although the position of this pixel is random, the color value is accurate. This is the essence of NEQR is superior to FRQI. Hence, through the preparation of a large number of the same quantum superposition state, and then the measurement is carried out on the superposition states, as long as the number of prepared superposition states is enough, we can get the color value information of all pixels. Thus, we can realize the transformation of the quantum image to the classical image.

3.5.2 Measurement of Encrypted Image

For the encrypted image, the pixel position and its color value are all in an uniform quantum superposition state. Similar to the measurement of the decrypted image, for each measurement, we also can only get the information of one pixel corresponding to the collapsed basic state, However, the pixel position and its color value obtained at this time are random. In terms of the R,G,B values of every pixel, the probability of taking each value in the $(0, 0, 0) \sim (255, 255, 255)$ is equal to 2^{-24}. Hence, the encrypted image becomes an uniform white noise after it is measured.

4 Simulation on Classical Computer

Herein, the simulations of the original image's encryption and decryption are performed on a classical computer due to the condition that the physical quantum computer is not in our grasp right now. The simulations are demonstrated with a classical computer with Intel(R) Core(TM) i5-3470 CPU @ 3.20GHz 4.00GB RAM and 32-bit operating system. The simulations are based on linear algebra with complex vectors as quantum states and unitary matrices as unitary transforms using Matlab 7.8.0(R2009a).

In order to verify the performance of the proposed scheme, a more convincing scheme must be chosen as a comparison target. In this paper, the double encryption scheme in the time domain and frequency in [28] is chosen as the comparison scheme. The reason this scheme is chosen as a comparison target is that it has some outstanding advantages as follows. For encrypted image, the distribution of histogram is uniform, the chi-square value is considerably low, the mean square error of encrypted image is big enough, the correlation coefficients in all three directions are sufficiently small, and the total key length is large enough to resist any brute-force attack, et. al.

The first 8 color images used in the experiment are from following website: http://sipi.usc.edu/database/database.php, and the last 4 color images are from the Peking University

and the Tsinghua University campus. For the first 8 images, each row and column contains 512 pixels. The sizes of the last 4 color images are 1024×759, 770×460, 1024×683, and 998×598, respectively.

4.1 Encryption Effect

The original images are shown in Fig. 7, and the corresponding encrypted images are shown in Fig. 8. The Decrypted images and the original images are exactly the same, so the display will not be repeated.

In Fig. 8, the encrypted images are presented as random white noise, which suggests that, at least from a visual point of view alone, the encryption strategy proposed in this paper is effective.

4.2 Key Sensitivity Analysis

A desirable encryption scheme requires high sensitivity to the encryption keys. In order to test the sensitivity of the secret key, a method of randomly changing some element in encryption key is employed. Specifically, we randomly select respectively 10%, 20%, 30%, 40% of the secret key elements, and put these elements to their opposite number. Then the modified secret key is used to decrypt the encrypted images. The decrypted images are shown in Fig. 9.

To evaluate the quality of the color images restored from the encrypted images with the modified secret key, the RGB Peak Signal-to-Noise Ratio (RGB-PSNR) is used as defined below.

$$PSNR = 20 \log_{10} \left(\frac{255}{\sqrt{\frac{1}{3mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \sum_{k=0}^{3} [I'(i, j, k) - I(i, j, k)]^2}} \right), \tag{20}$$

where $I'(i, j)$ and $I(i, j)$ denote the restored image and the original image, respectively, m and n are the number of pixels per row and column in an image.

After the comparison of our restored images I' with the original images I, the RGB-PSNR values of 12 restored images are obtained as presented in Table 1.

From Fig. 9, when the random components of secret key reaches 40%, the decryption image has become an uniform white noise without any visual information. From Table 1, when the random components of secret key reaches 40%, there is almost no difference in the peak signal to noise ratio of the decrypted image and the corresponding encrypted image, and when the random components of secret key reaches 10%, the peak signal to noise ratio of the decrypted image is only about 12. Through the test, it is proved that the correct image can be reconstructed only when the decryption key and the encryption key match accurately. Due to the key space of proposed method is very big, unless someone has obtained in advance the correct secret key, it is almost impossible to accurately restore the original image.

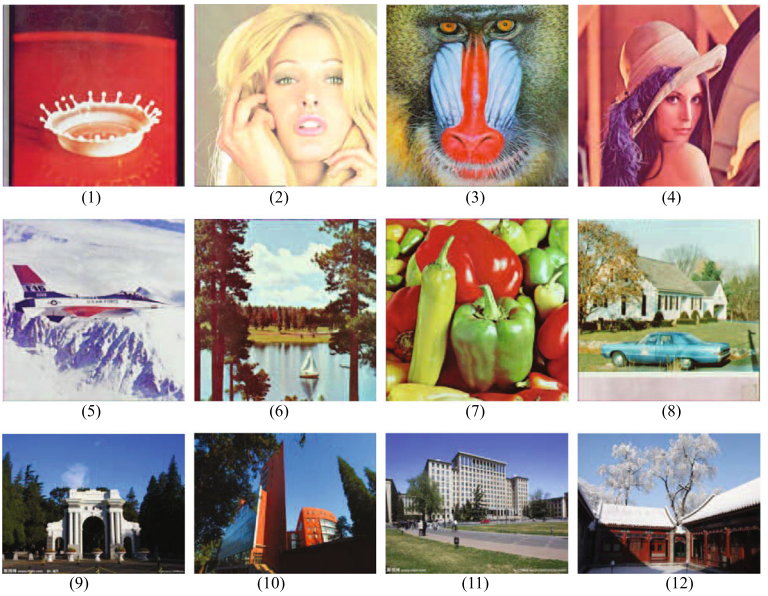

Fig. 7 The original images

4.3 Correlation Analysis of Adjacent Pixels

In ordinary image having definite visual content, each pixel is highly correlated with its adjacent pixels. The good encryption approach should produce the cipher image with no

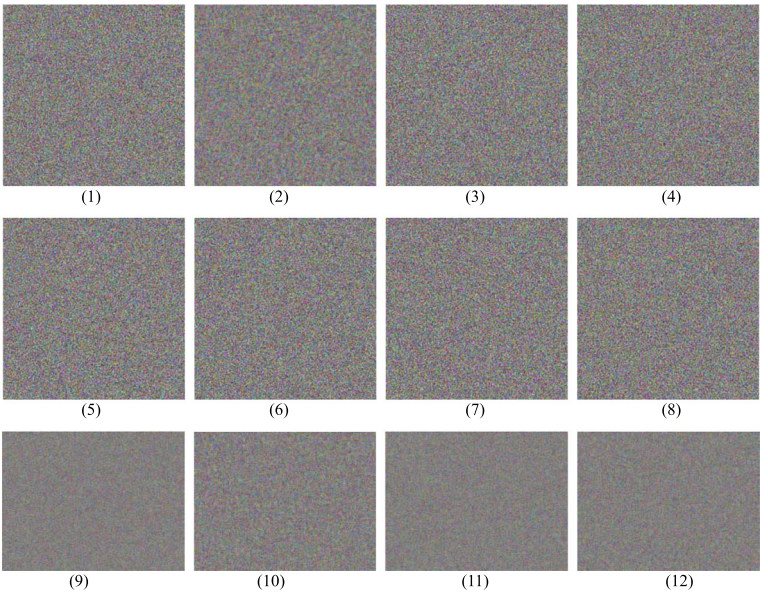

Fig. 8 The encrypted images

Fig. 9 The secret key sensitivity test, where the first column is the decrypted images by the secret key with 10% random components, the remainder analogy

such correlation in the adjacent pixels (correlation coefficient$\approx$ 0). To quantify and compare the correlations of adjacent pixels in the original image and its encrypted version, we also

Table 1 The RGB-PSNR values of 12 encrypted images and the restored images by the secret key with some random components

No.	Encrypted image	Random_key 10%	Random_key 20%	Random_key 30%	Random_key 40%
1	7.6332	11.6899	9.88850	8.6351	7.6299
2	7.0625	11.4513	9.54160	8.1550	7.0694
3	8.7692	12.1131	10.5502	9.5217	8.7724
4	8.6237	12.0695	10.4762	9.3972	8.6196
5	7.9774	11.8164	10.1026	8.8913	7.9738
6	8.0899	11.8584	10.1693	8.9856	8.0804
7	8.0796	11.8578	10.1606	8.9729	8.0773
8	8.4789	12.0099	10.3735	9.2823	8.4725
9	7.1244	11.4734	9.58580	8.2120	7.1225
10	7.0173	11.4210	9.51120	8.1250	7.0174
11	8.4324	11.9889	10.3609	9.2647	8.4323
12	7.5217	11.6301	9.82490	8.5313	7.5137

calculated the correlation coefficient R_{xy} of adjacent pixels of the original image and its encrypted version by the following equation.

$$R_R(x_R, y_R) = \frac{E(x_R - E(x_R))E(y_R - E(y_R))}{\sqrt{D(x_R)D(y_R)}}, \tag{21}$$

$$R_G(x_G, y_G) = \frac{E(x_G - E(x_G))E(y_G - E(y_G))}{\sqrt{D(x_G)D(y_G)}}, \tag{22}$$

$$R_B(x_B, y_B) = \frac{E(x_B - E(x_B))E(y_B - E(y_B))}{\sqrt{D(x_B)D(y_B)}}, \tag{23}$$

where $E(x_R)$, $E(x_G)$, $E(x_B)$ and $D(x_R)$, $D(x_G)$, $D(x_B)$ denote the expectation and variance of the gray-level value of three primary colors of red, green, blue, respectively.

To investigate the diffusion effect of our scheme, the correlation is tested between two horizontally, vertically, and diagonally adjacent pixels in the 12 original images and the corresponding encrypted images, respectively. Specifically, by randomly selecting 10,000 pairs of adjacent pixels in each direction from the original image and its encrypted version, the correlation between pixels can be obtained. Suppose that the I_{Ori} and I_{Enc} denote the original image and the encrypted image, respectively, and that the $I_{[28]}$ denotes the encrypted image by using the scheme in [28]. The results of correlation coefficients for horizontal, vertical and diagonal adjacent pixels for 12 original images and their corresponding encrypted images are given in Table 2.

It is clear from Table 2 that the correlation between the adjacent pixels in the original image I_{Ori} is very strong, and the adjacent pixels in the encrypted image I_{Enc} is almost irrelevant, and in all three directions of horizontal, vertical and diagonal, the correlation of our method are weaker than that of [28]. This indicates that our method is more secure than scheme in [28].

The visual testing of the correlation of adjacent pixels can be done by plotting the distribution of the adjacent pixels in the plain image and its corresponding cipher image.

Table 2 The correlation coefficients for horizontal, vertical and diagonal adjacent pixels for the original images and their corresponding encrypted images

No.	Image	Horizontal correlation			Vertical correlation			Diagonal correlation			Absolute average
		R_R	R_G	R_B	R_R	R_G	R_B	R_R	R_G	R_B	
	I_{Ori}	0.9984	0.9896	0.9864	0.9960	0.9814	0.9862	0.9952	0.9730	0.9750	0.9868
1	I_{Enc}	−0.0024	0.0094	−0.0294	−0.0017	0.0044	−0.0004	0.0024	0.0101	−0.0115	0.0080
	$I_{[28]}$	0.0124	0.0160	−0.0021	−0.0083	−0.0024	−0.0122	0.0156	0.0058	0.0190	0.0104
	I_{Ori}	0.9794	0.9583	0.9573	0.9666	0.9267	0.9195	0.9545	0.9098	0.9016	0.9415
2	I_{Enc}	−0.0035	0.0019	−0.0163	−0.0010	−0.0048	0.0036	−0.0053	0.0055	0.0223	0.0071
	$I_{[28]}$	0.0245	0.0015	0.0142	0.0107	0.0105	−0.0041	−0.0204	0.0038	−0.0171	0.0119
	I_{Ori}	0.8954	0.7882	0.8871	0.9364	0.8724	0.9127	0.8861	0.7591	0.8502	0.8653
3	I_{Enc}	0.0085	−0.0068	0.0126	−0.0116	0.0087	−0.0086	0.0072	−0.0005	−0.0070	0.0079
	$I_{[28]}$	−0.0217	−0.0075	0.0115	−0.0185	0.0170	0.0070	−0.0102	−0.0100	−0.0089	0.0125
	I_{Ori}	0.9890	0.9823	0.9555	0.9802	0.9702	0.9344	0.9697	0.9565	0.9171	0.9617
4	I_{Enc}	−0.0166	−0.0104	−0.0010	−0.0012	0.0048	0.0134	0.0070	−0.0028	0.0112	0.0076
	$I_{[28]}$	0.0133	−0.0138	−0.0079	−0.0122	0.0181	0.0311	0.0161	−0.0094	−0.0170	0.0154
	I_{Ori}	0.9725	0.9719	0.9620	0.9701	0.9684	0.9634	0.9478	0.9484	0.9410	0.9606
5	I_{Enc}	−0.0042	−0.0031	−0.0005	−0.0072	0.0021	0.0011	−0.0146	0.0073	−0.0067	0.0052
	$I_{[28]}$	−0.0122	0.0041	−0.0134	−0.0092	−0.0100	−0.0148	−0.0243	0.0032	0.0073	0.0109
	I_{Ori}	0.9470	0.9527	0.9669	0.9620	0.9757	0.9745	0.9383	0.9434	0.9543	0.9572
6	I_{Enc}	0.0028	−0.0081	0.0098	0.0009	−0.0119	0.0088	0.0102	−0.0036	−0.0019	0.0064
	$I_{[28]}$	0.0115	−0.0113	−0.0040	−0.0160	−0.0197	0.0182	0.0235	−0.0048	0.0139	0.0137
	I_{Ori}	0.9705	0.9865	0.9725	0.9696	0.9843	0.9689	0.9641	0.9755	0.9576	0.9722
7	I_{Enc}	0.0018	−0.0096	0.0171	0.0029	0.0075	0.0158	−0.0078	0.0081	−0.0111	0.0091
	$I_{[28]}$	0.0318	−0.0027	−0.0243	0.0137	0.0081	−0.0083	0.0176	−0.0154	−0.0038	0.0140
	I_{Ori}	0.9448	0.9579	0.9791	0.9464	0.9521	0.9775	0.9168	0.9201	0.9606	0.9506
8	I_{Enc}	−0.0000	−0.0013	0.0028	0.0075	0.0011	0.0129	0.0061	0.0037	−0.0022	0.0042

Table 2 (continued)

No.	Image	Horizontal correlation			Vertical correlation			Diagonal correlation			Absolute average
		R_R	R_G	R_B	R_R	R_G	R_B	R_R	R_G	R_B	
	$I_{[28]}$	−0.0186	0.0074	0.0109	−0.0151	−0.0028	0.0055	−0.0075	0.0003	−0.0122	0.0089
	I_{Ori}	0.9628	0.9674	0.9849	0.9685	0.9717	0.9876	0.9422	0.9489	0.9767	0.9679
9	I_{Enc}	−0.0078	0.0010	0.0078	−0.0277	−0.0017	0.0177	−0.0006	0.0005	0.0078	0.0081
	$I_{[28]}$	−0.0094	−0.0024	0.0151	0.0121	0.0113	0.0196	−0.0117	−0.0125	0.0143	0.0120
	I_{Ori}	0.9624	0.9631	0.9775	0.9527	0.9601	0.9784	0.9354	0.9393	0.9637	0.9592
10	I_{Enc}	−0.0045	−0.0032	−0.0012	0.0005	0.0091	−0.0040	−0.0136	−0.0132	0.0095	0.0065
	$I_{[28]}$	0.0037	−0.0104	0.0095	−0.0039	−0.0104	0.0075	0.0031	−0.0167	−0.0125	0.0086
	I_{Ori}	0.8982	0.8773	0.9501	0.9165	0.9009	0.9627	0.8548	0.8284	0.9326	0.9024
11	I_{Enc}	0.0002	0.0053	−0.0024	−0.0036	−0.0014	0.0055	0.0009	0.0181	0.0081	0.0051
	$I_{[28]}$	0.0112	0.0108	−0.0145	−0.0048	0.0193	0.0018	0.0121	−0.0131	−0.0036	0.0101
	I_{Ori}	0.9112	0.9264	0.9387	0.9184	0.9322	0.9431	0.8903	0.9091	0.9238	0.9215
12	I_{Enc}	0.0208	−0.0075	0.0085	−0.0176	−0.0031	0.0070	0.0094	0.0048	0.0120	0.0101
	$I_{[28]}$	−0.0178	0.0335	0.0069	−0.0122	−0.0081	0.0119	0.0056	0.0250	0.0042	0.0139

To illustrate the diffusion effect of our scheme, taking the fourth image as an example, the distribution of the adjacent pixels in the original image and its encrypted image are respectively plotted in Figs. 10, 11 and 12. In each of the figure, the three child figures at the top belong to the original image, and the three child figures at the bottom belong to the encrypted image.

The experimental results show that the proposed encryption strategy generally provides a satisfactory correlation performance.

4.4 Histogram Test

Histogram can reflect the distribution of pixel color value in the image, it is clear that the uniform distribution of the histogram can effectively resist various brute force attacks. Taking the twelfth image as an example, the histogram of the pixel R,G,B values before and after encryption is shown in Fig. 13, where the three child figures at the top belong to the original image, and the three child figures at the bottom belong to the encrypted image.

It can be seen from the Fig. 13, the encrypting operation can exhibit a uniform distribution of the histogram, and do not provide any clue to employ any statistical attack on the proposed image encryption algorithm.

The uniformity of a histogram is justified using the χ^2 test [28], in the following equation

$$\chi^2 = \sum_{k=1}^{256} \frac{(O_k - E_k)^2}{E_k}, \tag{24}$$

where k denotes the number of gray levels (256), O_k denotes the observed occurrence frequencies of each gray level (0-255), and E_k denotes the expected occurrence frequencies of

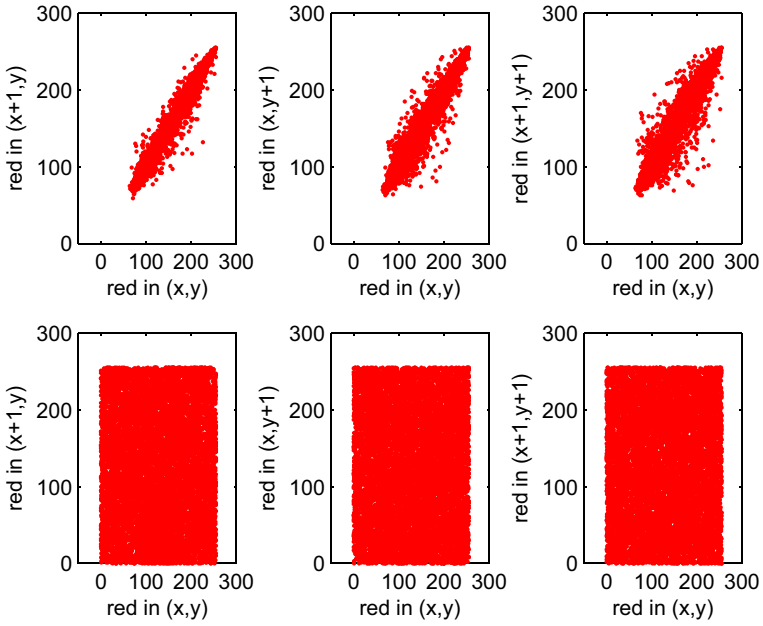

Fig. 10 Correlations between two adjacent pixels in the *red color*

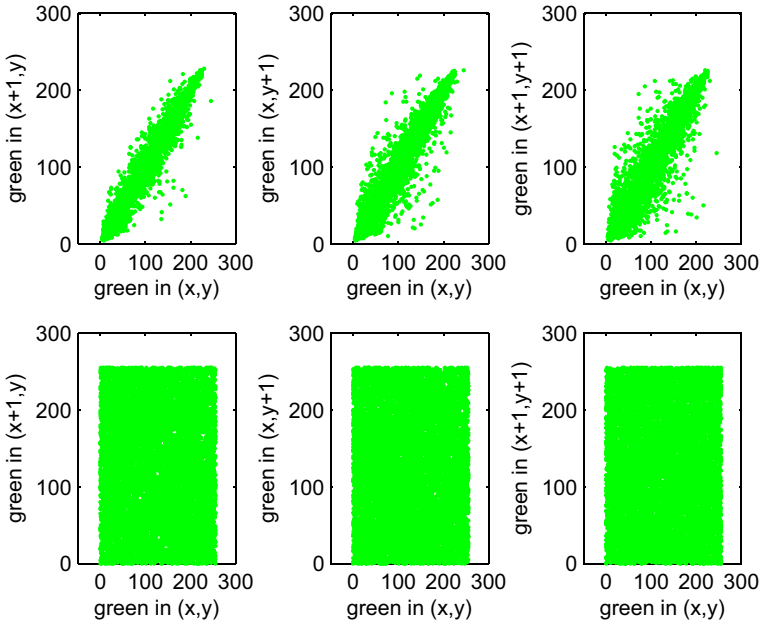

Fig. 11 Correlations between two adjacent pixels in the *green color*

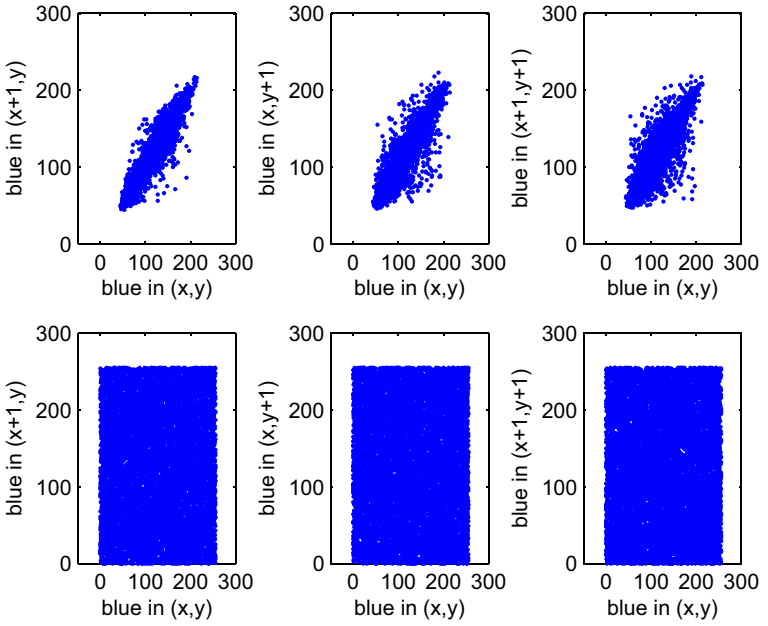

Fig. 12 Correlations between two adjacent pixels in the *blue color*

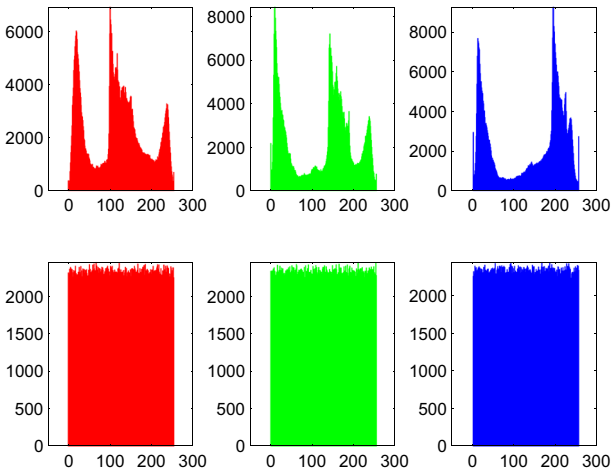

Fig. 13 The histogram distributions of the original image and the encrypted one

each level. For example, E_k is equal to 64 for image size of 128×128. Obviously, the less the χ^2 value, the better the uniformity. The χ^2 values are presented for all twelve encrypted images as shown in Table 3. In order to compare with other algorithms, the results obtained by using the scheme in [28] are also given in this table.

From Table 3, the χ^2 value for encrypted images of our proposed method is about is considerably lower than this value of encryption scheme in [28].

Table 3 Comparison of χ^2 test of the encrypted images between the proposed scheme and the scheme in [28]

	Original image			Encrypted image with our scheme			Encrypted image with scheme in [28]		
No.	χ^2_R	χ^2_G	χ^2_B	χ^2_R	χ^2_G	χ^2_B	χ^2_R	χ^2_G	χ^2_B
1	6.05E5	7.71E5	1.47E6	2.31E3	2.26E3	2.16E3	3.42E3	3.91E3	3.54E3
2	1.54E7	7.50E5	7.64E5	2.24E3	2.36E3	2.28E3	3.82E3	3.91E3	3.84E3
3	8.28E4	1.42E5	7.99E4	2.25E3	2.33E3	2.45E3	3.48E3	3.74E3	3.77E3
4	2.54E5	1.13E5	3.44E5	2.28E3	2.45E3	2.17E3	3.47E3	3.93E3	3.63E3
5	6.78E5	6.82E5	1.10E6	2.34E3	2.19E3	2.32E3	3.61E3	4.01E3	3.80E3
6	1.96E5	1.30E5	3.44E5	2.15E3	2.36E3	2.29E3	3.70E3	3.56E3	3.49E3
7	2.13E5	3.18E5	4.91E5	2.40E3	2.19E3	2.39E3	3.70E3	3.52E3	3.92E3
8	1.92E5	3.32E5	2.48E5	2.28E3	2.29E3	2.29E3	3.79E3	3.73E3	3.92E3
9	1.67E6	6.89E5	1.18E6	6.44E3	6.06E3	6.30E3	1.02E4	9.88E3	9.75E3
10	1.09E6	1.42E6	1.56E6	2.96E3	2.90E3	3.06E3	4.73E3	4.54E3	5.07E3
11	4.82E5	5.67E5	1.73E6	5.55E3	5.69E3	5.82E3	9.48E3	9.38E3	9.49E3
12	2.44E5	3.55E5	4.41E5	4.86E3	5.01E3	5.05E3	8.00E3	8.38E3	7.86E3

4.5 Mean Square Error

An ideal encrypted image should be significantly different from the original one. The difference between encrypted images and original ones can be characterize by mean square error (MSE) defined in the following equation.

$$\mathrm{MSE_R} = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} (I_{Ori}(i, j, 2) - I_{Enc}(i, j, 1))^2, \tag{25}$$

$$\mathrm{MSE_G} = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} (I_{Ori}(i, j, 3) - I_{Enc}(i, j, 2))^2, \tag{26}$$

$$\mathrm{MSE_B} = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} (I_{Ori}(i, j, 3) - I_{Enc}(i, j, 3))^2, \tag{27}$$

where $m \times n$ is the size of image. The parameters $I_{Ori}(i, j, k)$ and $I_{Enc}(i, j, k), k = 1, 2, 3$, are R,G,B values of pixel (i, j) in original and encrypted images, respectively, where $k = 1$ denotes R, $k = 2$ denotes G, and $k = 3$ denotes B. The larger the MSE value, the better the encryption security.

For all twelve encrypted images by our proposed scheme and scheme in [28], the MSE values are calculated as shown in Table 4.

The MSE of the proposed encrypted image is more than MSE of the scheme in [28], which shows that our method is more effective.

4.6 Probability Deviation

In the encrypted image, the color value of each pixel is no longer in a determined basic state, but in a balanced superposition state, and the probability of which is in state 0 or 1 state is

Table 4 Comparison of mean square error of the encrypted images between the proposed scheme and the scheme in [28]

	Our scheme				Scheme in [28]			
No.	$\mathrm{MSE_R}$	$\mathrm{MSE_G}$	$\mathrm{MSE_B}$	Average	$\mathrm{MSE_R}$	$\mathrm{MSE_G}$	$\mathrm{MSE_B}$	Average
1	1.141E4	1.236E4	9.857E3	1.121E4	1.116E4	1.256E4	9.879E4	1.120E4
2	1.781E4	1.316E4	7.386E3	1.278E4	1.725E4	1.273E4	7.133E3	1.237E4
3	8.618E3	7.749E3	9.531E3	8.633E3	8.518E3	7.625E3	9.439E3	8.527E3
4	1.062E4	9.046E3	7.111E3	8.927E3	1.032E4	9.115E3	7.056E3	8.832E3
5	9.978E3	1.066E4	1.043E4	1.036E4	9.651E3	1.040E4	1.009E4	1.004E4
6	7.289E3	1.147E4	1.151E4	1.009E4	7.203E3	1.142E4	1.145E4	1.002E4
7	7.962E3	1.123E4	1.115E4	1.011E4	7.828E3	1.107E4	1.124E4	1.005E4
8	8.762E3	9.512E3	9.415E3	9.229E3	8.587E3	9.239E3	9.323E3	9.050E3
9	1.295E4	1.062E4	1.424E4	1.260E4	1.307E4	1.055E4	1.407E4	1.256E4
10	1.275E4	1.111E4	1.489E4	1.292E4	1.273E4	1.112E4	1.483E4	1.289E4
11	8.348E3	7.534E3	1.210E4	9.329E3	8.296E3	7.455E3	1.192E4	9.225E3
12	1.041E4	1.146E4	1.264E4	1.150E4	1.040E4	1.138E4	1.255E4	1.145E4

Table 5 Probability deviation contrasts between the original images and the encrypted images

	Original image			Encrypted image		
No.	ΔP_R	ΔP_G	ΔP_B	ΔP_R	ΔP_G	ΔP_B
1	1048576	1048576	1048576	5.170E-26	5.170E-16	5.170E-26
2	1048576	1048576	1048576	5.170E-26	5.170E-26	5.170E-26
3	1048576	1048576	1048576	5.170E-26	5.170E-26	5.170E-26
4	1048576	1048576	1048576	5.170E-26	5.170E-26	5.170E-26
5	1048576	1048576	1048576	5.170E-26	5.170E-26	5.170E-26
6	1048576	1048576	1048576	5.170E-26	5.170E-26	5.170E-26
7	1048576	1048576	1048576	5.170E-26	5.170E-26	5.170E-26
8	1048576	1048576	1048576	5.170E-26	5.170E-26	5.170E-26
9	3108864	3108864	3108864	1.533E-25	1.533E-25	1.533E-25
10	1416800	1416800	1416800	6.985E-26	6.985E-26	6.985E-26
11	2797568	2797568	2797568	1.379E-25	1.379E-25	1.379E-25
12	2387216	2387216	2387216	1.177E-25	1.177E-25	1.177E-25

0.5. Suppose that the k–th qubit of pixel $P(Y, X)$ is $|C^k_{YX}\rangle = \cos\theta^k_{YX}|0\rangle + \sin\theta^k_{YX}|1\rangle$. The specific definition of probability deviation is as follows.

$$\Delta P_R = \sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\sum_{k=0}^{7}\frac{(\cos^2\theta^k_{YX}-0.5)^2}{0.5}, \tag{28}$$

$$\Delta P_G = \sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\sum_{k=8}^{15}\frac{(\cos^2\theta^k_{YX}-0.5)^2}{0.5}, \tag{29}$$

$$\Delta P_B = \sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\sum_{k=16}^{23}\frac{(\cos^2\theta^k_{YX}-0.5)^2}{0.5}. \tag{30}$$

We calculated the probability deviation of 12 original images and the corresponding encrypted images, and the results are shown in Table 5.

From Table 5, the probability deviation of all the encrypted images is almost zero, which indicates that the qubits in encrypted image are accurately in the equilibrium quantum superposition state, namely, the probability that they are in state $|0\rangle$ or state $|1\rangle$ is equal. Therefore, only an uniform white noise can be obtained that all pixels take random values when the encrypted image is measured, which can effectively resist brute force attacks of illegal users.

5 Conclusions

In quantum digital images encryption, although, most of the encryption algorithms are designed in the spatial domain and the frequency domain, the quantum digital image could be encrypted only in the spatial domain as well. we proposed a simple algorithm to encrypt an quantum images only in spatial domain. In proposed method, the images are represented based on NEQR model. The pixel's gray level information is described by 24 quantum bits which is in $|0\rangle$ or $|1\rangle$. The encryption scheme is to make these qubits be in an equilibrium quantum superposition state. For a $2^n \times 2^n$ color image, the secret key is a vector of

length $2^n \times 2^n \times 24$, and each component of the vector is randomly taken 1 or -1. The advantage of this method is that it can be implemented on the future quantum computer and has a large secret key space. The simulation results on a classical computer verify that the proposed quantum image encryption scheme is more secure in comparison with other encryption algorithms.

Acknowledgments We thank the anonymous reviewers for their constructive suggestions. This work was supported by the National Natural Science Foundation of China (Grant No. 61170132), the Natural Science Foundation of Heilongjiang Province of China (Grant No. F2015021), and by the Scientific Technology Research Project of the Education Department of Heilongjiang Province, China (Grant No. 12541059).

References

1. Akhshani, A., Akhavan, A., Lim, S.C.: Commu. Non. Sci. Num. Sim. **17**(12), 4653–4661 (2012)
2. Chen, L.F., Zhao, D.M., Ge, F.: Opt. Commun. **291**(3), 98–103 (2013)
3. Chen, T.H., Wu, C.S.: Inf. Sci. **180**(9), 1690–1701 (2010)
4. Chen, T.H., Li, K.C.: Inf. Sci. **189**(15), 255–265 (2012)
5. Lu, D.J., He, W.Q., Peng, X.: J. Opt. **15**(10), 105405 (2013)
6. Mandal, M.K.B., Gourab, D., Chattopadhyay, D.: IETE Tech. Rev. **29**(5), 395–404 (2012)
7. Ozkaynak, F., Ozer, A.B., Yavuz, S.: Opt. Comm. **285**(24), 4946–4948 (2012)
8. Shi, Y.S., Li, T., Wang, Y.L.: Opt. Lett. **38**(9), 1425–1427 (2013)
9. Sun, M.J., Shi, J.H., Li, H.: Opt. Express. **21**(16), 19395–19400 (2013)
10. Wang, X.G., Zhao, D.M.: Appl. Opt. **52**(25), 21–29 (2013)
11. Wang, X.Y., Liu, L.T.: Non. Dyn. **73**(1–2), 795–800 (2013)
12. Ye, G.D., Wong, K.W.: Non. Dyn. **69**(4), 2079–2087 (2012)
13. Zang, J.L., Xie, Z.W., Zhang, Y.: Opt. Lett. **38**(8), 1289–1291 (2013)
14. Zhu, Z.L., Zhang, W., Wong, K.W.: Inf. Sci. **181**(6), 1171–1186 (2011)
15. Salvador, E., Venegas, A., Sougato, B.: In: Proc. SPIE 5105, Quantum Information and Computation, vol. 137 (2003)
16. Li, H.S., Zhang, Q.X., Lan, S.: Quant. Inf. Process. **12**(6), 2269–2290 (2013)
17. Yuan, S., Mao, X., Xue, Y., et al.: Quant. Inf. Process. **13**(6), 1353–1379 (2014)
18. Venegas, S.E., Ball, J.L.: Quant. Inf. Process. **9**(1), 1–11 (2010)
19. Le, P.Q., Dong, F., Hirota, K.: A flexible representation of quantum images for polynomial preparation, image compression, and processing operations. Quant. Inf. Process. **10**(1), 63–84 (2011)
20. Sun, B., Itiyasua, M., Yan, F., et al.: J. Adv. Comput. Intell. Intell. Inform. **17**(3), 404–417 (2013)
21. Li, H.S., Zhu, Q., Zhou, R.G., et al.: Multi-dimensional color image storage and retrieval for a normal arbitrary quantum superposition state. Quant. Inf. Process. **13**(4), 991–1011 (2013)
22. Song, X.H., Wang, S., Niu, X.M.: J. Inf. Hid. Multimed. Signal Process. **5**(4), 574–585 (2014)
23. Zhang, Y., Lu, K., Gao, Y., et al.: Quant. Inf. process. **12**(8), 2833–2860 (2013)
24. Zhou, R.G., Wu, Q., Zhang, M.Q., Shen, C.Y.: Int. J. Theor. Phys. **52**(6), 1802–1817 (2013)
25. Yang, Y.G., Xia, J., Sun, S.J., Pan, Q.X.: Inf. Sci. **277**(9), 445–457 (2014)
26. Yang, Y.G., Xia, J., Jia, X., et al.: Quant. Inf. Process. **12**(11), 3477–3493 (2013)
27. GGiuliano, B., Giulio, C., Giuliano, S.: Principles of Quantum Computation and Information (Volume I: Basic Concepts). World Scientific, Singapore (2004)
28. Shahram, E.B., Mohammad, E.: Telecommun. Syst. **52**(2), 525–537 (2013)
29. Yan, F., Abdullah, M.I., Salvador, E.V.: Quantum Inf. Process. **15**(1), 1–35 (2016)
30. Yan, F., Abdullah, M.I., Salvador, E.V., et al.: Int. J. Theor. Phys. **54**(8), 2893–2904 (2015)