Quantum Information Processing (2018) 17:188
https://doi.org/10.1007/s11128-018-1958-y

A quantum color image encryption scheme based on coupled hyper-chaotic Lorenz system with three impulse injections

Qiwen Ran[1] · Ling Wang[1] · Jing Ma[1] · Liying Tan[1] · Siyuan Yu[1]

Received: 2 November 2017 / Accepted: 12 June 2018 / Published online: 19 June 2018

Abstract
In this paper, a quantum color image encryption scheme based on coupled hyper-chaotic Lorenz system with three impulse injections is proposed. Firstly, in order to enhance the complexity of trajectory, three impulse signals values are injected into coupled hyper-chaotic Lorenz system during iterations. Then, six sequences generated from this system are used to encrypt red, green and blue components of the quantum color original image by XOR operations and right cyclic shift operations. Six initial values and three impulse signals values are used as keys, which could reduce the burden of keys transmission and make the cryptosystem own a key space large enough to resist exhaustive attack, even the attack from a quantum computer. Numerical simulations demonstrate that the proposed encryption scheme has a good feasibility and effectiveness for protecting quantum color images and is more secure in comparison with other encryption algorithms.

Keywords Quantum color image encryption · Quantum computation · Coupled hyper-chaotic Lorenz system · Impulse injection · Quantum color image representation

1 Introduction

With the development of multimedia information technology, information security issues are gradually put on the agenda. Image is one of the important tools of carrying information, and its security has been widely studied [1–3]. Especially because of

✉ Ling Wang
wangling199059@163.com

Qiwen Ran
qiwenran@hit.edu.cn

[1] State Key Laboratory of Tunable Laser Technology Research, Institute of Optic-Electronics, Harbin Institute of Technology, Harbin 150001, China

the unique characteristics of the chaotic system, such as high sensitivity, topological transitivity, and pseudorandomness, a series of image encryption schemes based on chaotic system have been proposed [4–7].

However, short-period behavior of chaotic system after too many times iteration can lead to degeneration of dynamics [8]. Fortunately, this problem can be solved by impulse injection during the iteration process [9], because chaotic system is extremely sensitive to the initial conditions and a tiny deviation in iterating can result in significantly different trajectory. The injection times can be determined by the size of original image, and the injection moments and injection values can be random numbers.

With the rapid development of network technology, multimedia communication based on Internet is of increasing importance. According to random classical computations, N data need N steps of loading operations for a single processor [10], which reduces the computational efficiency and results in the bottleneck of classical computers. Nowadays, quantum computation is becoming a potentially effective tool to meet the high real-time computational requirements [11,12]. In 1982, Feynman first presented a computation model named quantum computers based on the principles of quantum physics, which seems more powerful than classical ones [13]. Until the arrival of practical quantum computers, the first task in quantum image processing is the construction of a pattern for capturing and storing the images on quantum computers. A great number of research results concerning quantum image representation exist in the literature, i.e., qubit lattice [14], entangled image [15], RealKet [16], a flexible representation for quantum images (FRQI) [17], a multi-channel representation of quantum image (MCRQI) [18], a normal arbitrary quantum superposition state (NASS) [19], a quantum representation for log-polar images [20], a novel enhanced quantum representation (NEQR) [21] and a novel quantum representation of color digital images (NCQI) [22].

Consequently, some quantum image encryption algorithms were developed to secure quantum images [23–34]. In detail, in 2013, based on quantum image geometric transformations, Zhou et al. [23] proposed an encryption algorithm for quantum image. The same year, in order to solve the drawbacks of the optical encryption systems and combine the merits of quantum cryptography, Yang et al. [24] proposed a novel image encryption scheme based on QFT and DRPE. Immediately afterward, in 2014, Yang et al. put forward a quantum cryptographic algorithm for color images using quantum Fourier transform and double random-phase encoding, which can be realized by performing two secret random-phase encoding operations, respectively, in the input and the QFT planes [25]. By using image correlation decomposition, Hua et al. introduced a quantum image encryption algorithm in [26]. Besides, based on generalized affine transform, quantum image encryption schemes in [27,29,32] were presented. In the years of 2015 and 2016, based on quantum walks and one-dimensional quantum cellular automata, Yang et al. [28,30] proposed two kinds of encryption algorithms, respectively. Based on hyper-chaotic system and QFT, Tan et al. [33] proposed a quantum color image encryption algorithm. In 2017, Li and Zhao [34] proposed a simple encryption algorithm for quantum color image by using controlled rotation gates.

However, most of these schemes are proposed for quantum gray images. Out of the ordinary, schemes in [25,33,34] are proposed to encrypt quantum color images. Through our analysis, they are found to have some drawbacks. In [25,33], the color information of each pixel is encoded by three qubits $|r\rangle, |g\rangle, |b\rangle$ that represent the three primary colors of red, green and 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 [34], 24 qubits are employed to represent the pixel color values of each pixel, which makes the scheme free from the influence of quantum states collapse. However, for a $2^n \times 2^n$ quantum color original image, the secret key is a vector of length $2^n \times 2^n \times 24$, which is more likely to make the keys too large to distribute, store and memorize. In view of the above, we propose a novel quantum color image encryption scheme. In our scheme, we use the NCQI model, the same as the one used in [34], to represent the quantum color original image, in which 24 qubits are employed to represent the pixel color scale values of each pixel. Firstly, three impulse signals are injected into coupled hyper-chaotic Lorenz system during iterations to enhance the complexity of trajectory. Then, six sequences generated are used to encrypt the red, green and blue components by XOR operations and right cyclic shift operations. Six initial values and three impulse signals values are used as keys, which could reduce the burden of keys transmission and make the cryptosystem own a key space large enough to resist exhaustive attack, even the attack from a quantum computer. Numerical simulations demonstrate that the proposed encryption scheme has a good feasibility and effectiveness for protecting quantum color images and has better security in comparison with other encryption algorithms.

This paper is organized as follows: Sect. 2 introduces quantum color image representation and coupled hyper-chaotic Lorenz system and three impulse injections. Quantum color image right cycle shift operation is given in Sect. 3. In Sect. 4, the proposed quantum color image encryption and decryption scheme is described. Section 5 is devoted to the theoretical analyses and numerical simulations. Finally, a brief conclusion is drawn in Sect. 6.

2 Quantum color image representation and coupled hyper-chaotic Lorenz system

2.1 Quantum representation for color digital images

The novel quantum representation for color digital images (NCQI) has been proposed in [22]. The representative expression of a quantum color image sized $2^n \times 2^n$ is described as follows:

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

where $|C(y,x)\rangle$ denotes the color value of the corresponding pixel and it can be encoded by the binary sequence $R_{q-1} \cdots R_0 G_{q-1} \cdots G_0 B_{q-1} \cdots B_0$.

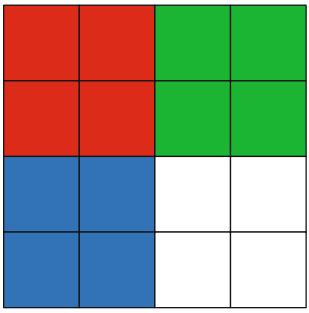

Fig. 1 A 4×4 color image (color figure online)

$$|C\,(y,x)\rangle = \left|\underbrace{R_{yx}^{q-1}\cdots R_{yx}^{0}}_{\text{Red}}\,\underbrace{G_{yx}^{q-1}\cdots G_{yx}^{0}}_{\text{Green}}\,\underbrace{B_{yx}^{q-1}\cdots B_{yx}^{0}}_{\text{Blue}}\right\rangle. \tag{2}$$

The values of every channel (R, G, B) range from 0 to $2^q - 1$. Equation (1) indicates the whole NCQI model is stored into a normalized quantum superposition state. There are three parts, i.e., the color information $|C\,(y,x)\rangle$, the vertical position $|y\rangle$ and the horizontal position $|x\rangle$ to represent one pixel. The tensor product of these three qubit sequences constitutes the basis state of NCQI. For a $2^n \times 2^n$ color image with every channel R, G, B in the range $\left[0, 2^q - 1\right]$, $2n + 3q$ qubits are employed to store image information into a NCQI state.

An example of a 4×4 color image with three channels R, G, B in the range $\left[0, 2^8 - 1\right]$, i.e., $n = 2, q = 8$, is shown in Fig. 1. The representation as shown in Eq. (3) depicts the whole NCQI is stored into a normalized quantum superposition state, in which each basis represents one pixel.

$$\begin{aligned}|I\rangle = \frac{1}{\sqrt{2^4}}\Bigg[&\left|\underbrace{11111111}_{R}\underbrace{00000000}_{G}\underbrace{00000000}_{B}\right\rangle \otimes (|0000\rangle + |0001\rangle + |0100\rangle + |0101\rangle)\\ &+ \left|\underbrace{00000000}_{R}\underbrace{11111111}_{G}\underbrace{00000000}_{B}\right\rangle \otimes (|0010\rangle + |0011\rangle + |0110\rangle + |0111\rangle)\\ &+ \left|\underbrace{00000000}_{R}\underbrace{00000000}_{G}\underbrace{11111111}_{B}\right\rangle \otimes (|1000\rangle + |1001\rangle + |1100\rangle + |1101\rangle)\\ &+ \left|\underbrace{11111111}_{R}\underbrace{11111111}_{G}\underbrace{11111111}_{B}\right\rangle \otimes (|1010\rangle + |1011\rangle + |1110\rangle + |1111\rangle)\Bigg].\end{aligned} \tag{3}$$

Notably, for a quantum color image sized $M \times N$ with every channel R, G, B in the range $\left[0, 2^q - 1\right]$, we can improve NCQI to store it. The improved model is called INCQI. An INCQI image representation can be written as follows:

$$|I\rangle = \frac{1}{\sqrt{2}^{m+n}} \sum_{y=0}^{N-1} \sum_{x=0}^{M-1} |C(y,x)\rangle \otimes |yx\rangle$$
$$= \frac{1}{\sqrt{2}^{m+n}} \sum_{y=0}^{N-1} \sum_{x=0}^{M-1} \left| R_{yx}^{q-1} \cdots R_{yx}^{0} G_{yx}^{q-1} \cdots G_{yx}^{0} B_{yx}^{q-1} \cdots B_{yx}^{0} \right\rangle \otimes |yx\rangle, \quad (4)$$

where

$$m = \begin{cases} \lceil \log_2 M \rceil, & M > 1 \\ 1, & M = 1 \end{cases} \quad (5)$$

$$n = \begin{cases} \lceil \log_2 N \rceil, & N > 1 \\ 1, & N = 1. \end{cases} \quad (6)$$

Of course, the encryption scheme put forward in Sect. 4 is also available for quantum color images of arbitrary size $M \times N$.

2.2 The coupled hyper-chaotic Lorenz system and three impulse injections

By coupling two identical Lorenz systems, the coupled hyper-chaotic Lorenz system was obtained by Grassi et al. [35], and the corresponding differential equation can be described as follows:

$$\begin{cases} \dot{x}_1 = a(y_1 - x_1) \\ \dot{y}_1 = bx_1 - y_1 - x_1 z_1 + k_1(x_2 - y_2) \\ \dot{z}_1 = x_1 y_1 - c z_1 \\ \dot{x}_2 = a(y_2 - x_2) \\ \dot{y}_2 = bx_2 - y_2 - x_2 z_2 + k_2(x_1 - y_1) \\ \dot{z}_2 = x_2 y_2 - c z_2, \end{cases} \quad (7)$$

where $X = [x_1, y_1, z_1, x_2, y_2, z_2]^{\mathrm{T}}$ is the state variable vector, a, b and c are control parameters, and $k_1, k_2 > 0$ are coupling parameters. The system exhibits hyper-chaotic behavior when $a = 10$, $b = 28$, $c = 8/3$, $k_1 = k_2 = 0.05$. Here, we set the initial values of $x_1(0) \neq x_2(0)$, $y_1(0) \neq y_2(0)$ and $z_1(0) \neq z_2(0)$, Fig. 2 shows the four-wing attractors.

When $a = 10$, $c = 8/3$ and $b \in [24, 51]$, the Lyapunov exponents are shown in Fig. 3. From Fig. 3, it is found that when $b \in [24, 51]$, the dynamics of system (7) is hyper-chaotic.

The problems of short period and degradation of dynamics seriously affect the practical applications of chaotic system. In order to solve these problems, one can try to randomly inject several impulse signal values into one of the variables during the iterating process to implement chaotic orbital transfer and remove the degradation of chaos dynamics. What is more, multiple injections can greatly enlarge the key space.

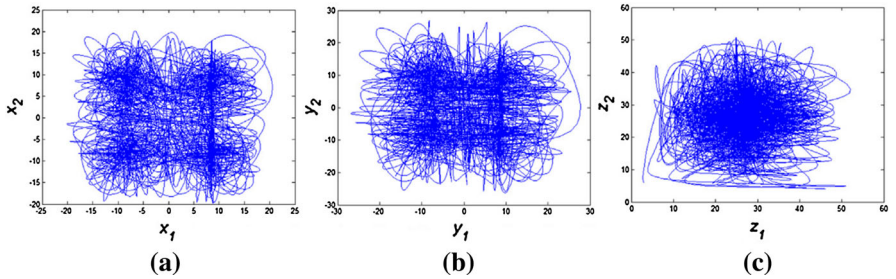

Fig. 2 Chaotic attractors of coupled hyper-chaotic Lorenz system

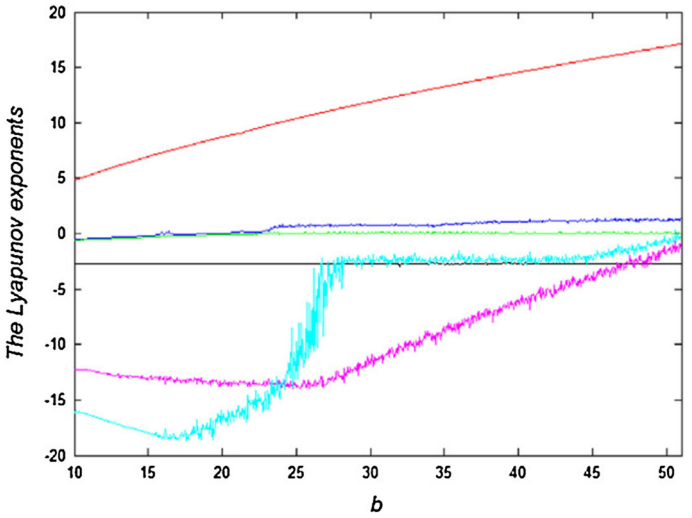

Fig. 3 Lyapunov exponent in the interval of parameter $b \in [24, 51]$

Because a tiny change in the initial value of chaotic system can result in completely different trajectory, assume that the total iterating time of system (7) is N and the injection time I can be designed to depend on the original image size. Here is the simplest example that we set $I = 2$ and then inject modified impulse signals of $\Delta x_{1(1)}, \Delta x_{1(2)} \in [0.1 \min(x_1), 0.1 \max(x_1)]$ into x_1, when $t = \lfloor N/3 \rfloor$, $t = \lfloor 2N/3 \rfloor$. The hyper-chaotic attractor after injection in three intervals of $[1, \lfloor N/3 \rfloor - 1]$, $[\lfloor N/3 \rfloor, \lfloor 2N/3 \rfloor - 1]$ and $[\lfloor 2N/3 \rfloor, N]$ is marked in different colors of red, green and blue, as shown in Fig. 4.

In the encryption scheme put forward in Sect. 4, we set $I = 3$, i.e., inject impulse signal values of $\Delta x_{1(1)}, \Delta x_{1(2)}, \Delta x_{1(3)} \in [0.1 \min(x_1), 0.1 \max(x_1)]$ into x_1, when $t = \lfloor N/4 \rfloor$, $t = \lfloor 2N/4 \rfloor$ and $t = \lfloor 3N/4 \rfloor$ in the process of iteration.

3 Quantum color image right cycle shift operations

The study [32] has proposed the cycle shift operations for quantum gray images. According to the study, the quantum color image right cycle shift operations are

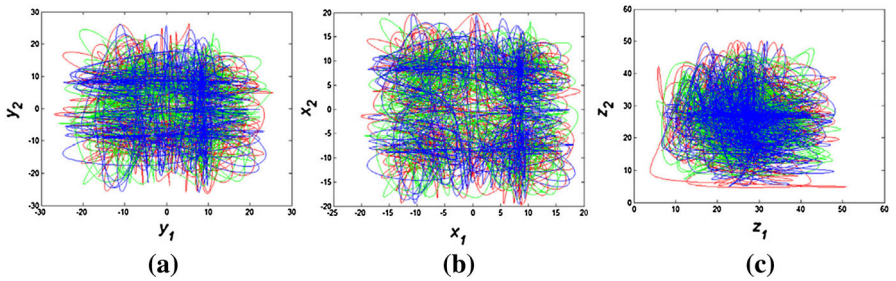

Fig. 4 Chaotic attractor of the coupled hyper-chaotic Lorenz system after impulse injection

defined in this section. The operations are executed on the pixel color values specially, and it will not be emphasized later.

For a quantum color image sized $2^n \times 2^n$ with values of every channel (R, G, B) in the range $[0, 2^q - 1]$, the quantum color image right cycle shift operations could be decomposed into 2^{2n} sub-operations and realized by quantum swap gates. The controlled swap gates U_{YX} controlled by a sequence $|H\rangle = \left\{\left|h_{0,0}\right\rangle, \left|h_{0,1}\right\rangle, \ldots, \left|h_{0,2^n-1}\right\rangle, \left|h_{1,0}\right\rangle, \ldots, \left|h_{2^n-1,2^n-1}\right\rangle\right\}$ are used to accomplish the sub-operations, where $|h_{YX}\rangle = \{|r_{YX}\rangle, |s_{YX}\rangle, |t_{YX}\rangle\}$, $Y = 0, 1, \ldots, 2^n - 1$, $X = 0, 1, \ldots, 2^n - 1$ are orderly. The color image right cycle shift operation is shown in Fig. 5. Correspondingly, Fig. 6 shows the three channels (R, G, B) of the color image right cycle shift operations for r, s, t times, respectively, where r, s, t are nonnegative integers and $0 \le r, s, t \le q - 1$.

If the times of three channels (R, G, B) right cycle shift operations are r, s, t, respectively, the controlled swap gate can be defined as:

$$\begin{aligned} U_{YX}\,|C\,(Y,X)\rangle &= U_{YX}\left|R_{YX}^{q-1}\cdots R_{YX}^{0}G_{YX}^{q-1}\cdots G_{YX}^{0}B_{YX}^{q-1}\cdots B_{YX}^{0}\right\rangle \\ &= \Big|\underbrace{R_{YX}^{r-1}\cdots R_{YX}^{0}R_{YX}^{q-1}\cdots R_{YX}^{r}}_{\text{Red}}\underbrace{G_{YX}^{s-1}\cdots G_{YX}^{0}G_{YX}^{q-1}\cdots G_{YX}^{s}}_{\text{Green}}\underbrace{B_{YX}^{t-1}\cdots B_{YX}^{0}B_{YX}^{q-1}\cdots B_{YX}^{t}}_{\text{Blue}}\Big\rangle. \end{aligned} \tag{8}$$

Then, the sub-operation S_{YX} constructed by the controlled swap gate U_{YX} can be defined as follows:

$$S_{YX} = \left(I \otimes \sum_{y=0}^{2^n-1}\sum_{\substack{x=0 \\ yx\neq YX}}^{2^n-1} |yx\rangle\langle yx|\right) + U_{YX} \otimes |YX\rangle\langle YX|. \tag{9}$$

The sub-operation S_{YX} is a unitary matrix, i.e., $S_{YX}S_{YX}^{\dagger} = I^{\otimes 2n+1}$, where $S_{YX}^{\dagger}$ is the Hermitian conjugation of matrix S_{YX}. The quantum color image right cycle shift operations could be implemented by the quantum sub-operation S_{YX}:

$$
\begin{aligned}
S_{YX}|I\rangle &= S_{YX}\left(\frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}\left|R_{yx}^{q-1}\cdots R_{yx}^{0}G_{yx}^{q-1}\cdots G_{yx}^{0}B_{yx}^{q-1}\cdots B_{yx}^{0}\right\rangle|yx\rangle\right)\\
&= \frac{1}{2^n}S_{YX}\left(\sum_{y=0}^{2^n-1}\sum_{\substack{x=0\\ yx\neq YX}}^{2^n-1}\left|R_{yx}^{q-1}\cdots R_{yx}^{0}G_{yx}^{q-1}\cdots G_{yx}^{0}B_{yx}^{q-1}\cdots B_{yx}^{0}\right\rangle|yx\rangle\right.\\
&\quad\left.+\left|R_{YX}^{q-1}\cdots R_{YX}^{0}G_{YX}^{q-1}\cdots G_{YX}^{0}B_{YX}^{q-1}\cdots B_{YX}^{0}\right\rangle|YX\rangle\right)\\
&= \frac{1}{2^n}\left(\sum_{y=0}^{2^n-1}\sum_{\substack{x=0\\ yx\neq YX}}^{2^n-1}\left|R_{yx}^{q-1}\cdots R_{yx}^{0}G_{yx}^{q-1}\cdots G_{yx}^{0}B_{yx}^{q-1}\cdots B_{yx}^{0}\right\rangle|yx\rangle\right.
\end{aligned}
$$

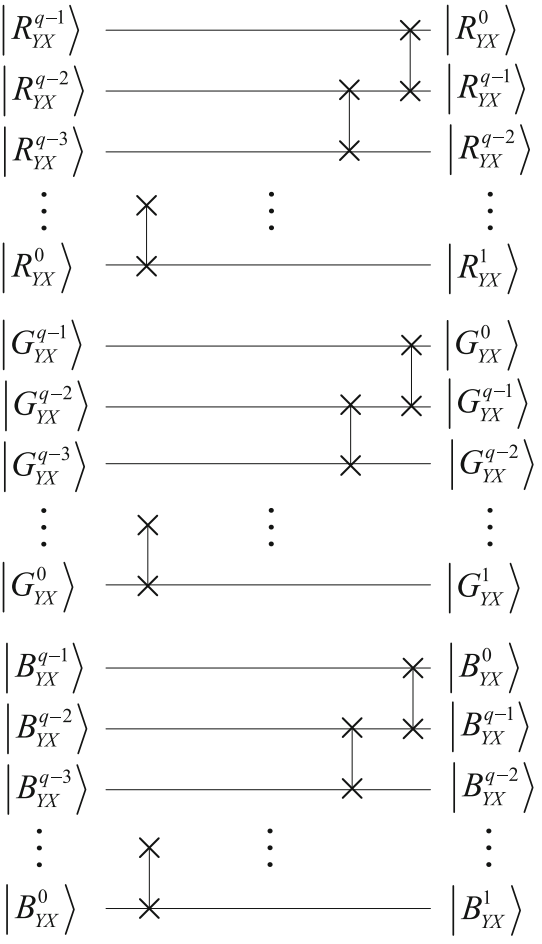

Fig. 5 Color image right cycle shift operation

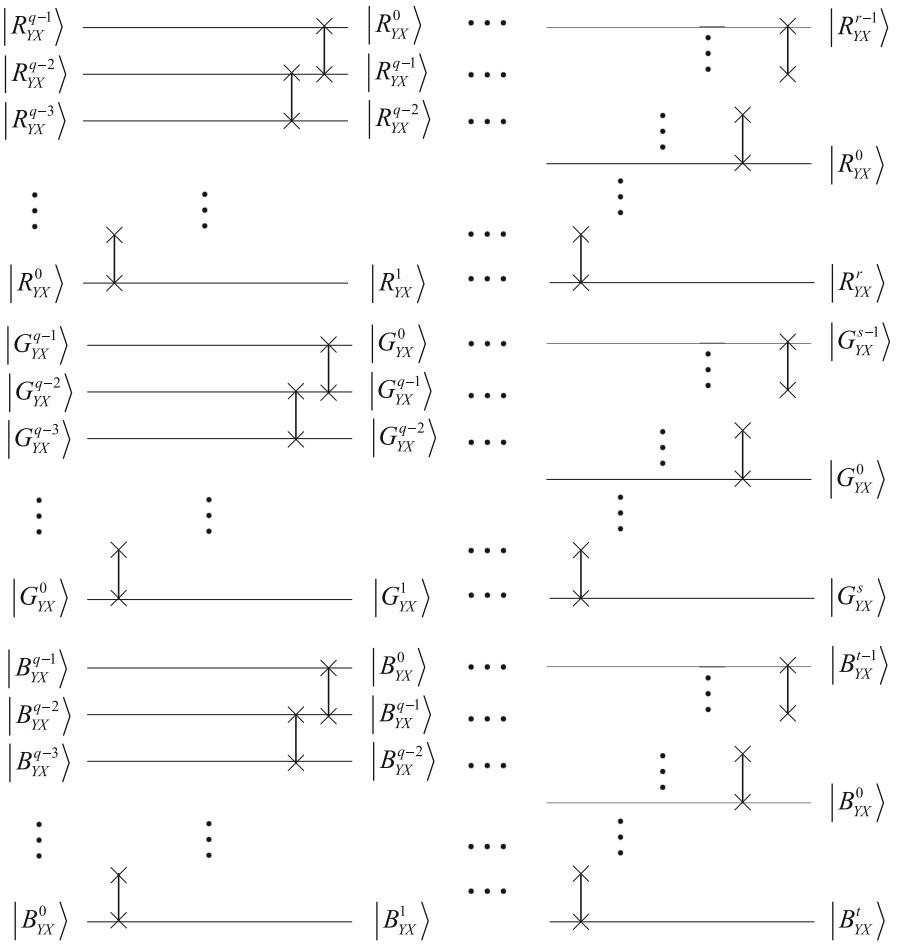

Fig. 6 Three channels of color image right cycle shift operations for r, s, t times, respectively

$$
\begin{aligned}
&+U_{YX}\left|R_{YX}^{q-1}\cdots R_{YX}^{0}G_{YX}^{q-1}\cdots G_{YX}^{0}B_{YX}^{q-1}\cdots B_{YX}^{0}\right\rangle|YX\rangle\Big)\\
&=\frac{1}{2^n}\left(\sum_{y=0}^{2^n-1}\sum_{\substack{x=0\\ yx\neq YX}}^{2^n-1}\left|R_{yx}^{q-1}\cdots R_{yx}^{0}G_{yx}^{q-1}\cdots G_{yx}^{0}B_{yx}^{q-1}\cdots B_{yx}^{0}\right\rangle|yx\rangle\right.\\
&+\left|R_{YX}^{r-1}\cdots R_{YX}^{0}R_{YX}^{q-1}\cdots R_{YX}^{r}G_{YX}^{s-1}\cdots G_{YX}^{0}G_{YX}^{q-1}\cdots G_{YX}^{s}B_{YX}^{t-1}\right.\\
&\left.\left.\cdots B_{YX}^{0}B_{YX}^{q-1}\cdots B_{YX}^{t}\right\rangle|YX\rangle\right)
\end{aligned}
\tag{10}
$$

$$
\begin{aligned}
&S_{Y'X'}S_{YX}\,|I\rangle\\
&=S_{Y'X'}\left(S_{YX}\frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}\left|R_{yx}^{q-1}\cdots R_{yx}^{0}G_{yx}^{q-1}\cdots G_{yx}^{0}B_{yx}^{q-1}\cdots B_{yx}^{0}\right\rangle|yx\rangle\right)
\end{aligned}
$$

$$
\begin{aligned}
&= S_{Y'X'} \frac{1}{2^n} \left(\sum_{y=0}^{2^n-1} \sum_{\substack{x=0 \\ yx \neq YX}}^{2^n-1} \left| R_{yx}^{q-1} \cdots R_{yx}^{0} G_{yx}^{q-1} \cdots G_{yx}^{0} B_{yx}^{q-1} \cdots B_{yx}^{0} \right\rangle |yx\rangle \right. \\
&\quad + \left| R_{YX}^{r-1} \cdots R_{YX}^{0} R_{YX}^{q-1} \cdots R_{YX}^{r} G_{YX}^{s-1} \cdots G_{YX}^{0} G_{YX}^{q-1} \cdots G_{YX}^{s} B_{YX}^{t-1} \right. \\
&\quad \left. \left. \cdots B_{YX}^{0} B_{YX}^{q-1} \cdots B_{YX}^{t} \right\rangle |YX\rangle \right) \\
&= \frac{1}{2^n} \left(\sum_{y=0}^{2^n-1} \sum_{\substack{x=0 \\ yx \neq YX, Y'X'}}^{2^n-1} \left| R_{yx}^{q-1} \cdots R_{yx}^{0} G_{yx}^{q-1} \cdots G_{yx}^{0} B_{yx}^{q-1} \cdots B_{yx}^{0} \right\rangle |yx\rangle \right. \\
&\quad + \left| R_{YX}^{r-1} \cdots R_{YX}^{0} R_{YX}^{q-1} \cdots R_{YX}^{r} G_{YX}^{s-1} \cdots G_{YX}^{0} G_{YX}^{q-1} \right. \\
&\quad \left. \cdots G_{YX}^{s} B_{YX}^{t-1} \cdots B_{YX}^{0} B_{YX}^{q-1} \cdots B_{YX}^{t} \right\rangle |YX\rangle \\
&\quad + \left| R_{Y'X'}^{r'-1} \cdots R_{Y'X'}^{0} R_{Y'X'}^{q-1} \cdots R_{Y'X'}^{r'} G_{Y'X'}^{s'-1} \cdots G_{Y'X'}^{0} G_{Y'X'}^{q-1} \right. \\
&\quad \left. \left. \cdots G_{Y'X'}^{s'} B_{Y'X'}^{t'-1} \cdots B_{Y'X'}^{0} B_{Y'X'}^{q-1} \cdots B_{Y'X'}^{t'} \right\rangle \left| Y'X' \right\rangle \right), \qquad (11)
\end{aligned}
$$

where r', s', t' are nonnegative integers and $0 \leq r', s', t' \leq q-1$. The sub-operations S_{YX} and $S_{Y'X'}$ are controlled by $\{|r\rangle, |s\rangle, |t\rangle\}$ and $\left\{\left|r'\right\rangle, \left|s'\right\rangle, \left|t'\right\rangle\right\}$, respectively.

Therefore, the quantum color image right cycle shift operations on its homologous pixels can be realized by 2^{2n} sub-operations S_{YX} as follows:

$$
S = \prod_{Y=0}^{2^n-1} \prod_{X=0}^{2^n-1} S_{YX}. \qquad (12)
$$

Corresponding to the quantum color image right cycle shift operations, the inverse sub-operation S_{YX}^{-1} could be built up by the three channels (R, G, B) of color image right cycle shift operations for $q-r, q-s, q-t$ times, respectively. So the details about S_{YX}^{-1} and S^{-1} are not needed to be addressed here.

4 Quantum color image encryption and decryption scheme

4.1 Quantum color image encryption scheme based on coupled hyper-chaotic Lorenz system with three impulse injections

Firstly, it is necessary to emphasize that the quantum color image encryption scheme proposed in this section is also available for quantum color images of arbitrary size $M \times N$. For simplicity, assume that the original quantum color image sized $2^n \times 2^n$ with values of every channel (R, G, B) in the range $\left[0, 2^8 - 1\right]$ to be encrypted is $|I\rangle$ and its NCQI representation can be written as:

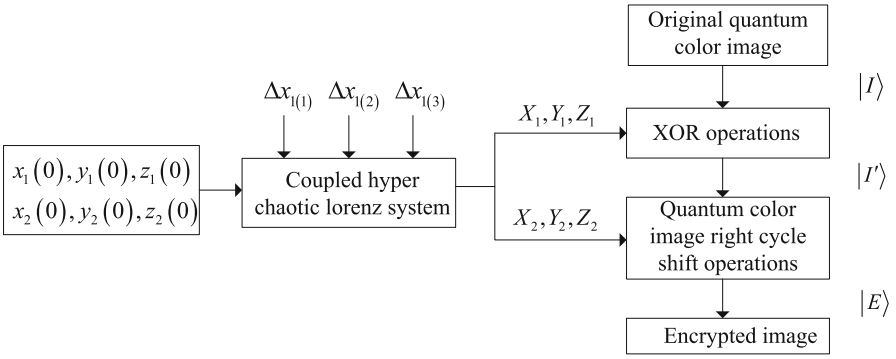

Fig. 7 Proposed quantum color image encryption scheme procedure

$$
\begin{aligned}
|I\rangle &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|C\,(y,x)\rangle \otimes |yx\rangle \\
&= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}\Big|\underbrace{R_{yx}^7\cdots R_{yx}^0}_{\text{Red}}\,\underbrace{G_{yx}^7\cdots G_{yx}^0}_{\text{Green}}\,\underbrace{B_{yx}^7\cdots B_{yx}^0}_{\text{Blue}}\Big\rangle \otimes |yx\rangle \\
&= \frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}|C\,(i)\rangle \otimes |i\rangle \\
&= \frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}\left|R_i^7\cdots R_i^0 G_i^7\cdots G_i^0 B_i^7\cdots B_i^0\right\rangle \otimes |i\rangle,
\end{aligned}
\tag{13}
$$

where $\left|R_i^k\right\rangle, \left|G_i^k\right\rangle, \left|B_i^k\right\rangle \in \{|0\rangle, |1\rangle\}$, $i = 0, 1, \ldots, 2^{2n}-1$, $k = 0, 1, \ldots, 7$. The proposed quantum color image encryption scheme consists of the following steps. The encryption procedure is shown in Fig. 7.

Input Original quantum color image $|I\rangle$.

Keys $x_1(0), y_1(0), z_1(0), x_2(0), y_2(0), z_2(0)$ and $\Delta x_{1(1)}, \Delta x_{1(2)}, \Delta x_{1(3)}$ represent keys which can be selected randomly.

Output The encrypted quantum color image $|E\rangle$ with the same size.

Step 1 Iterating system (7) with six initial values of $x_1(0), y_1(0), z_1(0), x_2(0), y_2(0), z_2(0)$ for $N = 2^n \times 2^n$ times. When the iterating times $t_1 = \lfloor N/4 \rfloor$, $t_2 = \lfloor 2N/4 \rfloor$ and $t_3 = \lfloor 3N/4 \rfloor$, inject $\Delta x_{1(1)}$, $\Delta x_{1(2)}$ and $\Delta x_{1(3)}$ into $x_1(t_1)$, $x_1(t_2)$ and $x_1(t_3)$, respectively, to produce six sequences of $X_1, Y_1, Z_1, X_2, Y_2, Z_2$.

$$
\begin{aligned}
X_1 &= \{x_1(0), x_1(1), \ldots, x_1(N-1)\} \\
Y_1 &= \{y_1(0), y_1(1), \ldots, y_1(N-1)\} \\
Z_1 &= \{z_1(0), z_1(1), \ldots, z_1(N-1)\}
\end{aligned}
$$

$$X_2 = \{x_2(0), x_2(1), \ldots, x_2(N-1)\}$$
$$Y_2 = \{y_2(0), y_2(1), \ldots, y_2(N-1)\}$$
$$Z_2 = \{z_2(0), z_2(1), \ldots, z_2(N-1)\}. \tag{14}$$

Step 2 Compute

$$T_i = \text{floor}\left(\text{mod}\left(x_1(i) \times 10^{14}, 256\right)\right)$$
$$V_i = \text{floor}\left(\text{mod}\left(y_1(i) \times 10^{14}, 256\right)\right)$$
$$W_i = \text{floor}\left(\text{mod}\left(z_1(i) \times 10^{14}, 256\right)\right)$$
$$J_i = \text{floor}\left(\text{mod}\left(x_2(i) \times 10^{14}, 8\right)\right)$$
$$K_i = \text{floor}\left(\text{mod}\left(y_2(i) \times 10^{14}, 8\right)\right)$$
$$L_i = \text{floor}\left(\text{mod}\left(z_2(i) \times 10^{14}, 8\right)\right), \tag{15}$$

where $i = 0, 1, \ldots, N-1$, and floor stands for the rounding operation.

Then transform $\{T_i\}$, $\{V_i\}$ and $\{W_i\}$ into binary qubit sequences:

$$|T_i\rangle = \bigotimes_{k=0}^{7} \left|T_i^k\right\rangle = \left|T_i^7\right\rangle \left|T_i^6\right\rangle \cdots \left|T_i^0\right\rangle$$
$$|V_i\rangle = \bigotimes_{k=0}^{7} \left|V_i^k\right\rangle = \left|V_i^7\right\rangle \left|V_i^6\right\rangle \cdots \left|V_i^0\right\rangle$$
$$|W_i\rangle = \bigotimes_{k=0}^{7} \left|W_i^k\right\rangle = \left|W_i^7\right\rangle \left|W_i^6\right\rangle \cdots \left|W_i^0\right\rangle, \tag{16}$$

where $\left|T_i^k\right\rangle, \left|V_i^k\right\rangle, \left|W_i^k\right\rangle \in \{|0\rangle, |1\rangle\}$, $i = 0, 1, \ldots, N-1$, $k = 0, 1, \ldots, 7$.

Step 3 Define the sub-operation P_t:

$$P_t = \left(I \otimes \sum_{i=0, i\neq t}^{N-1} |i\rangle\langle i| + D_t \otimes |t\rangle\langle t|\right), \tag{17}$$

where

$$\begin{aligned} D_t |C(t)\rangle &= D_t \left|R_t^7 \cdots R_t^0 G_t^7 \cdots G_t^0 B_t^7 \cdots B_t^0\right\rangle \\ &= D_t \left(\bigotimes_{k=0}^{7} \left|R_t^k\right\rangle \bigotimes_{k=0}^{7} \left|G_t^k\right\rangle \bigotimes_{k=0}^{7} \left|B_t^k\right\rangle\right) \\ &= \bigotimes_{k=0}^{7} \left|R_t^k \oplus T_t^k\right\rangle \bigotimes_{k=0}^{7} \left|G_t^k \oplus V_t^k\right\rangle \bigotimes_{k=0}^{7} \left|B_t^k \oplus W_t^k\right\rangle \end{aligned}$$

$$= \left| \left(R_t^7 \oplus T_t^7 \right) \cdots \left(R_t^0 \oplus T_t^0 \right) \left(G_t^7 \oplus V_t^7 \right) \cdots \left(G_t^0 \oplus V_t^0 \right) \left(B_t^7 \oplus W_t^7 \right) \cdots \left(B_t^0 \oplus W_t^0 \right) \right\rangle. \tag{18}$$

The color image color-information XOR operations could be implemented by the quantum sub-operation P_t:

$$\begin{aligned} P_t\left(|I\rangle\right) &= P_t\left(\frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} \left| R_i^7 \cdots R_i^0 G_i^7 \cdots G_i^0 B_i^7 \cdots B_i^0 \right\rangle \otimes |i\rangle\right) \\ &= \frac{1}{\sqrt{N}} P_t\left(\sum_{i=0, i\neq t}^{N-1} \left| R_i^7 \cdots R_i^0 G_i^7 \cdots G_i^0 B_i^7 \cdots B_i^0 \right\rangle \otimes |i\rangle \right. \\ &\quad \left. + \left| R_t^7 \cdots R_t^0 G_t^7 \cdots G_t^0 B_t^7 \cdots B_t^0 \right\rangle \otimes |t\rangle\right) \\ &= \frac{1}{\sqrt{N}} \left(\sum_{i=0, i\neq t}^{N-1} \left| R_i^7 \cdots R_i^0 G_i^7 \cdots G_i^0 B_i^7 \cdots B_i^0 \right\rangle \otimes |i\rangle \right. \\ &\quad \left. + D_t \left| R_t^7 \cdots R_t^0 G_t^7 \cdots G_t^0 B_t^7 \cdots B_t^0 \right\rangle \otimes |t\rangle\right) \\ &= \frac{1}{\sqrt{N}} \left(\sum_{i=0, i\neq t}^{N-1} \left| R_i^7 \cdots R_i^0 G_i^7 \cdots G_i^0 B_i^7 \cdots B_i^0 \right\rangle \otimes |i\rangle \right. \\ &\quad \left. + \left| \left(R_t^7 \oplus T_t^7 \right) \cdots \left(R_t^0 \oplus T_t^0 \right) \left(G_t^7 \oplus V_t^7 \right) \cdots \left(G_t^0 \oplus V_t^0 \right) \left(B_t^7 \oplus W_t^7 \right) \right. \right. \\ &\quad \left. \left. \cdots \left(B_t^0 \oplus W_t^0 \right) \right\rangle \otimes |t\rangle\right) \end{aligned} \tag{19}$$

$$\begin{aligned} P_s P_t\left(|I\rangle\right) &= P_s\left(P_t\left(\frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} \left| R_i^7 \cdots R_i^0 G_i^7 \cdots G_i^0 B_i^7 \cdots B_i^0 \right\rangle \otimes |i\rangle\right)\right) \\ &= P_s \frac{1}{\sqrt{N}} \left(\sum_{i=0, i\neq t}^{N-1} \left| R_i^7 \cdots R_i^0 G_i^7 \cdots G_i^0 B_i^7 \cdots B_i^0 \right\rangle \otimes |i\rangle \right. \\ &\quad \left. + \left| \left(R_t^7 \oplus T_t^7 \right) \cdots \left(R_t^0 \oplus T_t^0 \right) \left(G_t^7 \oplus V_t^7 \right) \cdots \left(G_t^0 \oplus V_t^0 \right) \left(B_t^7 \oplus W_t^7 \right) \right. \right. \\ &\quad \left. \left. \cdots \left(B_t^0 \oplus W_t^0 \right) \right\rangle \otimes |t\rangle\right) \\ &= \frac{1}{\sqrt{N}} \left(\sum_{i=0, i\neq t, s}^{N-1} \left| R_i^7 \cdots R_i^0 G_i^7 \cdots G_i^0 B_i^7 \cdots B_i^0 \right\rangle \otimes |i\rangle \right. \\ &\quad + \left| \left(R_t^7 \oplus T_t^7 \right) \cdots \left(R_t^0 \oplus T_t^0 \right) \left(G_t^7 \oplus V_t^7 \right) \cdots \left(G_t^0 \oplus V_t^0 \right) \left(B_t^7 \oplus W_t^7 \right) \right. \\ &\quad \left. \cdots \left(B_t^0 \oplus W_t^0 \right) \right\rangle \otimes |t\rangle \\ &\quad + \left| \left(R_s^7 \oplus T_s^7 \right) \cdots \left(R_s^0 \oplus T_s^0 \right) \left(G_s^7 \oplus V_s^7 \right) \cdots \left(G_s^0 \oplus V_s^0 \right) \left(B_s^7 \oplus W_s^7 \right) \right. \\ &\quad \left. \left. \cdots \left(B_s^0 \oplus W_s^0 \right) \right\rangle \otimes |s\rangle \right). \end{aligned} \tag{20}$$

From (19) and (20), it is distinct that the color image color-information XOR operations on its homologous pixels can be realized by quantum transform P:

$$P = \prod_{i=0}^{N-1} P_i. \tag{21}$$

By performing operation P on $|I\rangle$, one can obtain the image $\left|I'\right\rangle$:

$$\begin{aligned} P\left(|I\rangle\right) &= \prod_{i=0}^{N-1} P_i\left(|I\rangle\right) \\ &= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} D_i \left|R_i^7 \cdots R_i^0 G_i^7 \cdots G_i^0 B_i^7 \cdots B_i^0\right\rangle \otimes |i\rangle \\ &= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} \left|\left(R_i^7 \oplus T_i^7\right) \cdots \left(R_i^0 \oplus T_i^0\right) \left(G_i^7 \oplus V_i^7\right)\right. \\ &\quad \left. \cdots \left(G_i^0 \oplus V_i^0\right) \left(B_i^7 \oplus W_i^7\right) \cdots \left(B_i^0 \oplus W_i^0\right)\right\rangle \otimes |i\rangle \\ &= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} \left|R_i^{7'} \cdots R_i^{0'} G_i^{7'} \cdots G_i^{0'} B_i^{7'} \cdots B_i^{0'}\right\rangle \otimes |i\rangle \\ &= \left|I'\right\rangle. \end{aligned} \tag{22}$$

Step 4 The sequence

$$|H\rangle = \{|h_0\rangle, |h_1\rangle, \ldots, |h_{N-1}\rangle\} \tag{23}$$

should be generated before performing the quantum color image right cycle shift operations, where $|h_i\rangle = \{|J_i\rangle, |K_i\rangle, |L_i\rangle\}$, $i = 0, 1, \ldots, N-1$, are orderly. The controlled swap gate U_i is constructed by $|h_i\rangle$. Quantum color image right cycle shift operation is executed on $\left|I'\right\rangle$ by quantum transform S to acquire the quantum image $|E\rangle$, where $|E\rangle$ stands for the final encrypted image:

$$\begin{aligned} S\left|I'\right\rangle &= \prod_{i=0}^{N-1} S_i \left|I'\right\rangle \\ &= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} U_i \left|R_i^{7'} \cdots R_i^{0'} G_i^{7'} \cdots G_i^{0'} B_i^{7'} \cdots B_i^{0'}\right\rangle \otimes |i\rangle \\ &= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} \left|R_i^{(J_i-1)'} \cdots R_i^{0'} R_i^{7'} R_i^{J_i'} G_i^{(K_i-1)'} \cdots G_i^{0'} G_i^{7'} G_i^{K_i'} B_i^{(L_i-1)'}\right. \\ &\quad \left. \cdots B_i^{0'} B_i^{7'} B_i^{L_i'}\right\rangle \otimes |i\rangle \\ &= |E\rangle. \end{aligned} \tag{24}$$

4.2 Quantum color image decryption scheme

The image decryption scheme is as follows.

Step 1 The six sequences $\{T_i\}$, $\{V_i\}$, $\{W_i\}$, $\{J_i\}$, $\{K_i\}$ and $\{L_i\}$ should be generated with the six initial values $x_1(0)$, $y_1(0)$, $z_1(0)$, $x_2(0)$, $y_2(0)$, $z_2(0)$ and three impulse injections $\Delta x_{1(1)}$, $\Delta x_{1(2)}$, $\Delta x_{1(3)}$ according to Step 1 and Step 2 in the encryption scheme.

Step 2 The inverse color image right cycle shift operation S^{-1} controlled by sequence $|H\rangle = \{|h_0\rangle, |h_1\rangle, \ldots, |h_{N-1}\rangle\}$ is performed on $|E\rangle$ to obtain the quantum image $\left|I'\right\rangle$, where $|h_i\rangle = \{|J_i\rangle, |K_i\rangle, |L_i\rangle\}$, $i = 0, 1, \ldots, N-1$.

Step 3 The XOR operations controlled by sequences $\{|T_i\rangle\}$, $\{|V_i\rangle\}$ and $\{|W_i\rangle\}$, $i = 0, 1, \ldots, N-1$, are performed on quantum image $\left|I'\right\rangle$ to obtain the decrypted quantum color image $|I\rangle$.

5 Theoretical analyses and numerical simulations

Quantum communication and computation is based on the preparation and manipulation of qubit states. Qubit states are very fragile and easily destroyed by decoherence due to unwanted coupling with the environment. However, not all states are equally fragile when interacting with the environment. Indeed, if the qubit–environment interaction exhibits some symmetry, there are states which are immune to this interaction and can therefore be used to protect quantum information. These states are called decoherence-free (DF) states [36]. The amount of quantum information that a given DF subspace is able to protect depends on the number N of qubits [37]. For N even, the DF subspace spanned by states which are eigenstates of the whole Hamiltonian of the qubit-bath system and also eigenstates of the interaction Hamiltonian with eigenvalue zero has dimension:

$$d(N) = \frac{N!}{(N/2)!\,(N/2+1)!}. \tag{25}$$

The number of qubits encoded in DF states is $\log_2 d(N)$. For a large N,

$$\log_2 d(N) \simeq N - \frac{3}{2}\log_2 N. \tag{26}$$

Therefore, the encoding efficiency is asymptotically unity.

For N qubits to be processed by quantum computation (N is even and large), suppose the N-dimensional space is $\mathbb{S}$, due to the fact that the existence of DF subspace whose dimension is $\frac{2^N}{N^{3/2}}$, and we have

$$\mathbb{S} = \mathbb{S}_1 \oplus \mathbb{S}_2, \tag{27}$$

where $\mathbb{S}_2$ is the $\frac{2^N}{N^{3/2}}$-dimensional DF subspace. Because $\frac{2^N}{N^{3/2}} > \frac{N}{2}$, there exists a subspace $\mathbb{S}_1^* \subset \mathbb{S}_2$, satisfying that the projection of $\mathbb{S}_1$ on the $\mathbb{S}_2$ is $\mathbb{S}_1^*$, i.e., we can construct a unitary transformation σ, which makes $\sigma(\mathbb{S}_1) = \mathbb{S}_1^* \subset \mathbb{S}_2$.

As suggested above, for N qubits in quantum communication and computation, in order to suppress the effect of decoherence, the N qubits are separated into two parts to process. On the one hand, for the part projecting on the DF subspace $\mathbb{S}_2$, because the DF states are immune to the interaction with the environment, we can process it directly according to our requirement; on the other hand, for the part projecting on the subspace $\mathbb{S}_1$, we can first use a unitary transformation to project it on $\mathbb{S}_2$ and obtain $\mathbb{S}_1^*$, where $\mathbb{S}_1^* \subset \mathbb{S}_2$, and then the process is done as we need on the subspace $\mathbb{S}_1^*$. Finally, integrate the two parts of the processed qubits together and we can get the processed N qubits with lower cost of decoherence. Because unitary transformation is invertible, the processed N qubits are easily recovered to the original N qubits by the corresponding inverse processing and inverse unitary transformation.

Here, inspired by DF subspace, we only give a method for suppressing decoherence. In the future, if possible, we will study this method systematically and theoretically including the construction of orthogonal basis of DF subspace, the construction of unitary transformation and the concrete realization of this method on a quantum computer.

Furthermore, quantum Zeno effect, dynamical decoupling and quantum error correction are three important protection methods of quantum information, which also can suppress the decoherence effect and error. According to quantum Zeno effect, the decoherence effect of quantum computation process will be suppressed by making very frequent measurements of the system [38,39]; different from the measurement used in quantum Zeno effect, dynamical decoupling is used to suppress the decoherence process by imposing a time-dependent hamiltonian $H_c(t)$ on the target system [40,41]; last, for errors that occur at a certain probability in channel transmission, one can use quantum error correction to correct there random errors [42–44].

Due to the lack of quantum hardware, the simulations are executed with software MATLAB on a classical computer. The whole simulation is based on linear algebraic constructions. The quantum states are simulated by complex vectors, while the quantum operations are simulated by unitary matrices. So what needs to be emphasized is that, in the numerical simulations, we do not consider the effect of decoherence and errors.

In order to verify the performance of the proposed encryption scheme, three encryption schemes for color image in [25,33,34] are chosen as the comparison schemes. We select three groups of keys randomly for experimental simulations. The six initial values and three impulse injections are set as follows, respectively.

Keys 1: $x_1(0) = 4.175$, $y_1(0) = 8.203$, $z_1(0) = 1.376$, $x_2(0) = 14.362$,
$y_2(0) = 0.800$, $z_2(0) = 2.364$, $\Delta x_{1(1)} = 0.523$, $\Delta x_{1(2)} = 1.290$, $\Delta x_{1(3)} = 0.875$
Keys 2: $x_1(0) = 5.564$, $y_1(0) = 3.408$, $z_1(0) = 10.875$, $x_2(0) = 2.966$,
$y_2(0) = 8.862$, $z_2(0) = 1.640$, $\Delta x_{1(1)} = 0.624$, $\Delta x_{1(2)} = 2.875$, $\Delta x_{1(3)} = 4.558$
Keys 3: $x_1(0) = 15.778$, $y_1(0) = 6.521$, $z_1(0) = 0.643$, $x_2(0) = 2.390$,
$y_2(0) = 4.864$, $z_2(0) = 5.779$, $\Delta x_{1(1)} = 1.482$, $\Delta x_{1(2)} = 0.855$, $\Delta x_{1(3)} = 1.645$.

Six color images sized 512×512 are chosen as original images, shown in Fig. 8, and the corresponding encrypted images are shown in Fig. 9, where the six child figures

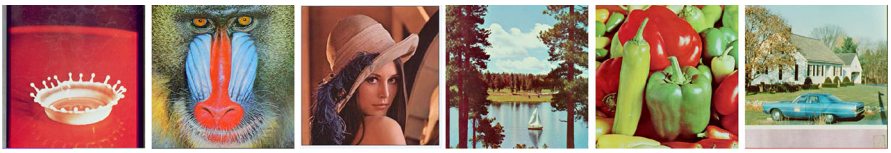

Fig. 8 Original images: **a** Splash, **b** Baboon, **c** Lena, **d** Sailboat, **e** Peppers and **f** House

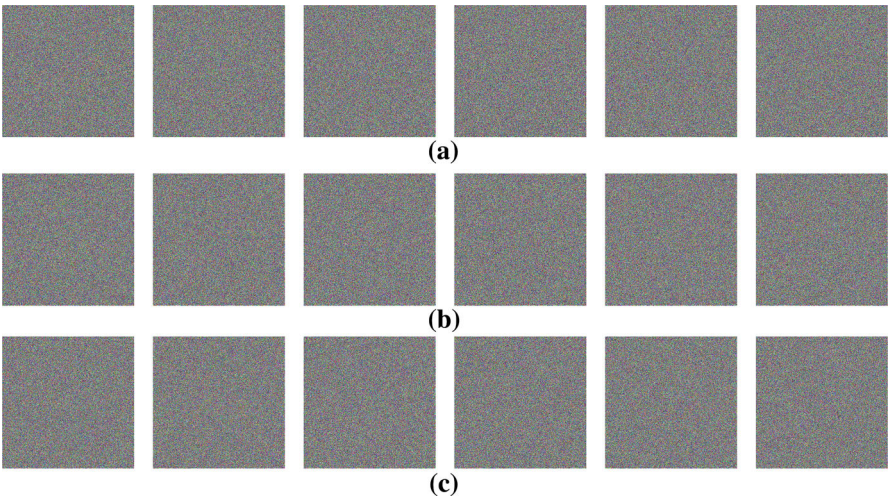

Fig. 9 Encrypted images: **a** using keys 1, **b** using keys 2 and **3** using keys 3

in Fig. 9a belong to encrypted images with keys 1, the six child figures in Fig. 9b belong to the encrypted images with keys 2, and the six child figures in Fig. 9c belong to encrypted images with keys 3. It is shown that one cannot obtain any information of the original images from the encrypted images. Therefore, the encryption scheme proposed in this paper is effective.

5.1 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 characterized by mean square error (MSE) defined as follows:

$$\mathrm{MSE}_R = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} \left(I_R(i, j) - E_R(i, j)\right)^2 \tag{28}$$

$$\mathrm{MSE}_G = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} \left(I_G(i, j) - E_G(i, j)\right)^2 \tag{29}$$

Table 1 MSE values of the encrypted images with three keys

Images	Keys	MSE_R	MSE_G	MSE_B
Splash	Keys 1	1.138E4	1.235E4	9.923E3
	Keys 2	1.142E4	1.232E4	9.924E3
	Keys 3	1.144E4	1.234E4	9.878E3
Baboon	Keys 1	8.633E3	7.754E3	9.452E3
	Keys 2	8.635E3	7.753E3	9.471E3
	Keys 3	8.629E3	7.750E3	9.476E3
Lena	Keys 1	9.115E3	9.772E3	1.066E4
	Keys 2	9.097E3	9.779E3	1.069E4
	Keys 3	9.114E3	9.784E3	1.066E4
Sailboat	Keys 1	7.282E3	1.148E4	1.155E4
	Keys 2	7.318E3	1.150E4	1.151E4
	Keys 3	7.317E3	1.150E4	1.148E4
Peppers	Keys 1	7.992E3	1.123E4	1.111E4
	Keys 2	8.012E3	1.126E4	1.117E4
	Keys 3	7.985E3	1.127E4	1.115E4
House	Keys 1	8.808E3	9.471E3	9.446E3
	Keys 2	8.786E3	9.489E3	9.483E3
	Keys 3	8.774E3	9.528E3	9.404E3

$$\mathrm{MSE}_B = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} \left(I_B(i, j) - E_B(i, j) \right)^2, \tag{30}$$

where $m \times n$ is the size of image. The parameters $I_R(i, j)$ and $E_R(i, j)$ are R values of pixel (i, j) in original and encrypted images, $I_G(i, j)$ and $E_G(i, j)$ are G values of pixel (i, j) in original and encrypted images, $I_B(i, j)$ and $E_B(i, j)$ are B values of pixel (i, j) in original and encrypted images, respectively. The larger the MSE value, the better the encryption security.

For the six original color images shown in Fig. 8, the MSE values with three groups of keys are calculated as shown in Table 1. The numerical values indicate the different keys chosen randomly have analogous effect to the encryption results.

For the six images encrypted by using our proposed scheme with keys 3, the MSE values are calculated as shown in Table 2. The MSE of the proposed encrypted image is more than the MSE of the scheme in [34], which shows that our scheme is more effective.

5.2 Statistical analysis

5.2.1 Correlation analysis of two adjacent pixels

Correlation reflects the degree of similarity of two variables. An efficient image cryptosystem should produce the encrypted image with sufficiently low correlation in

Table 2 Comparison of MSE of the encrypted images between the proposed scheme and the scheme in [34]

Images	Our scheme			Scheme in [34]		
	MSE_R	MSE_G	MSE_B	MSE_R	MSE_G	MSE_B
Splash	1.144E4	1.234E4	9.878E3	1.141E4	1.236E4	9.857E3
Baboon	8.629E3	7.750E3	9.476E3	8.618E3	7.749E3	9.531E3
Lena	9.114E3	9.784E3	1.066E4	1.062E4	9.046E3	7.111E3
Sailboat	7.317E3	1.150E4	1.148E4	7.289E3	1.147E4	1.151E4
Peppers	7.985E3	1.127E4	1.115E4	7.962E3	1.123E4	1.115E4
House	8.774E3	9.528E3	9.404E3	8.762E3	9.512E3	9.415E3

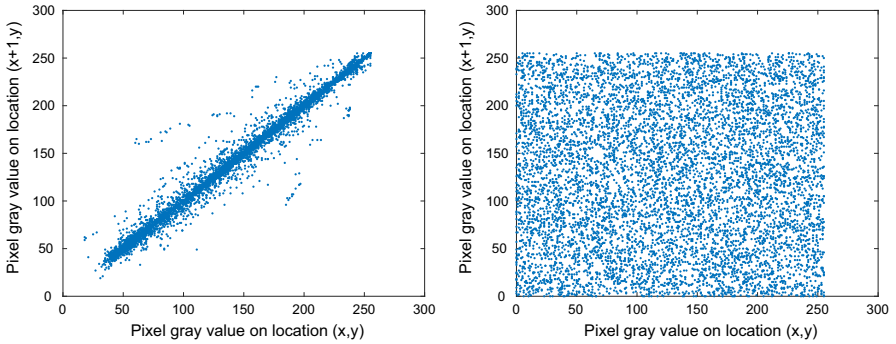

Fig. 10 Correlation distributions between two horizontal adjacent pixels in R channel: **a** image "Lena" and **b** encrypted image

horizontal, vertical and diagonal directions. In this subsection, we choose keys 1 as an example. In order to test the correlations of adjacent pixels in color images "Baboon," "Lena," "Peppers" and the corresponding encrypted images, for three channels (R, G, B), we randomly choose 8000 pairs of two adjacent pixels from horizontal, vertical and diagonal directions, respectively. Correlation coefficients can be calculated as:

$$C_{XY} = \frac{\sum_{i=1}^{N}\left(x_i - \frac{1}{N}\sum_{i=1}^{N} x_i\right)\left(y_i - \frac{1}{N}\sum_{i=1}^{N} y_i\right)}{\sqrt{\sum_{i=1}^{N}\left(x_i - \frac{1}{N}\sum_{i=1}^{N} x_i\right)^2 \sum_{i=1}^{N}\left(y_i - \frac{1}{N}\sum_{i=1}^{N} y_i\right)^2}}, \tag{31}$$

where x_i, y_i are gray-level values of two adjacent pixels in each primary color channel. Take R channel of "Lena" as an example; Figs. 10, 11 and 12 show the correlation distributions between two adjacent pixels in horizontal, vertical and diagonal directions. The correlation coefficients of color original images "Baboon," "Lena," "Peppers" and the corresponding encrypted images in horizontal, vertical and diagonal directions are listed in Tables 3, 4 and 5, respectively. It is clear from Table 3, 4 and 5 that the correla-

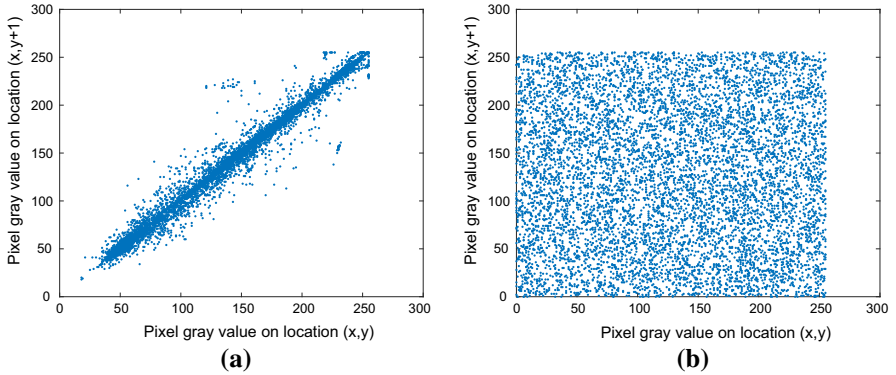

Fig. 11 Correlation distributions between two vertical adjacent pixels in *R* channel: **a** image "Lena" and **b** encrypted image

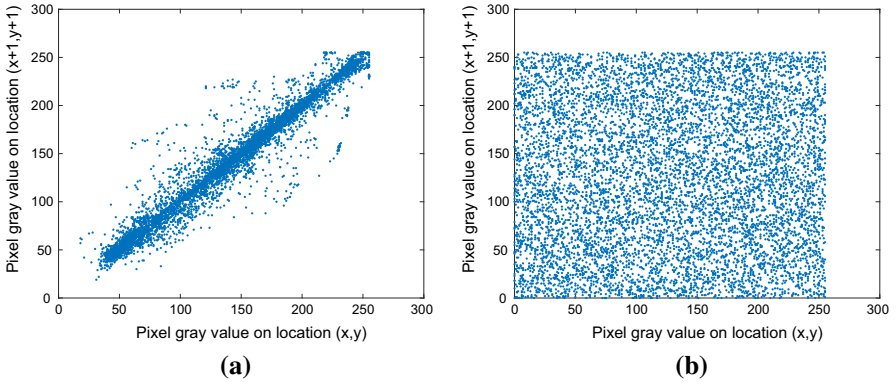

Fig. 12 Correlation distributions between two diagonal adjacent pixels in *R* channel: **a** image "Lena" and **b** encrypted image

tion between the adjacent pixels in the original image is very strong and adjacent pixels in the encrypted image is almost irrelevant, and in all three directions of horizontal, vertical and diagonal, the correlation of our scheme is weaker than that of [25,34]. This indicates that our scheme is more secure than the schemes in [25,34]. The proposed encryption scheme generally provides a satisfactory correlation performance to resist the attack based on statistical analysis.

5.2.2 Histogram analysis

Histogram reflects the pixel color value distribution of an image. If the histogram of an encrypted image is uniform, the encryption scheme is more robust against statistical attack and differential attack. The histograms of the pixel R, G, B values before and after encryption are shown in Fig. 13, where the three child figures in the first line belong to the original image "Lena," the three child figures in the second line belong to the encrypted image with keys 1, the three child figures in the third line belong to

Table 3 Results of correlation coefficients in horizontal direction

Correlation coefficient	Original image	Our scheme	Scheme in [25]	Scheme in [34]
Baboon (*R* channel)	0.8724	0.0033	− 0.0090	0.0085
Baboon (*G* channel)	0.7777	0.0026	− 0.0041	−0.0068
Baboon (*B* channel)	0.8896	− 0.0058	−0.0021	0.0126
Lena (*R* channel)	0.9897	− 0.0066	−0.0099	− 0.0166
Lena (*G* channel)	0.9871	0.0041	− 0.0082	−0.0104
Lena (*B* channel)	0.9842	− 0.0020	−0.108	− 0.0010
Peppers (*R* channel)	0.9647	− 0.0112	0.0043	0.0018
Peppers (*G* channel)	0.9805	− 0.0060	0.0092	− 0.0096
Peppers (*B* channel)	0.9696	0.0037	0.0128	0.0171

Table 4 Results of correlation coefficients in vertical direction

Correlation coefficient	Original image	Our scheme	Scheme in [25]	Scheme in [34]
Baboon (*R* channel)	0.9259	− 0.0013	0.0045	− 0.0116
Baboon (*G* channel)	0.8643	0.0038	0.0074	0.0087
Baboon (*B* channel)	0.9083	0.0014	0.0029	− 0.0086
Lena (*R* channel)	0.9865	0.0025	0.0088	− 0.0012
Lena (*G* channel)	0.9858	− 0.0017	0.0066	0.0048
Lena (*B* channel)	0.9831	− 0.0043	0.0067	0.0134
Peppers (*R* channel)	0.9626	− 0.0076	0.0298	0.0029
Peppers (*G* channel)	0.9802	− 0.0021	0.0290	0.0075
Peppers (*B* channel)	0.9697	0.0055	0.0050	0.0158

Table 5 Results of correlation coefficients in diagonal direction

Correlation coefficient	Original image	Our scheme	Scheme in [25]	Scheme in [34]
Baboon (*R* channel)	0.8599	− 0.0029	0.0133	0.0072
Baboon (*G* channel)	0.7371	− 0.0090	0.0066	− 0.0005
Baboon (*B* channel)	0.8462	− 0.0027	0.0017	− 0.0070
Lena (*R* channel)	0.9897	− 0.0066	0.0047	0.0070
Lena (*G* channel)	0.9765	0.0020	0.0023	− 0.0028
Lena (*B* channel)	0.9684	0.0032	0.0079	0.0112
Peppers (*R* channel)	0.9520	− 0.0028	0.0113	− 0.0078
Peppers (*G* channel)	0.9675	0.0018	0.0155	0.0081
Peppers (*B* channel)	0.9476	− 0.0027	−0.0058	− 0.0111

the encrypted image with keys 2, and the three child figures in the last line belong to the encrypted image with keys 3.

It can be seen that the encrypting operation can exhibit a uniform distribution of the histogram and does not provide any clue for eavesdroppers who perform statistical attack and differential attack on the encrypted image.

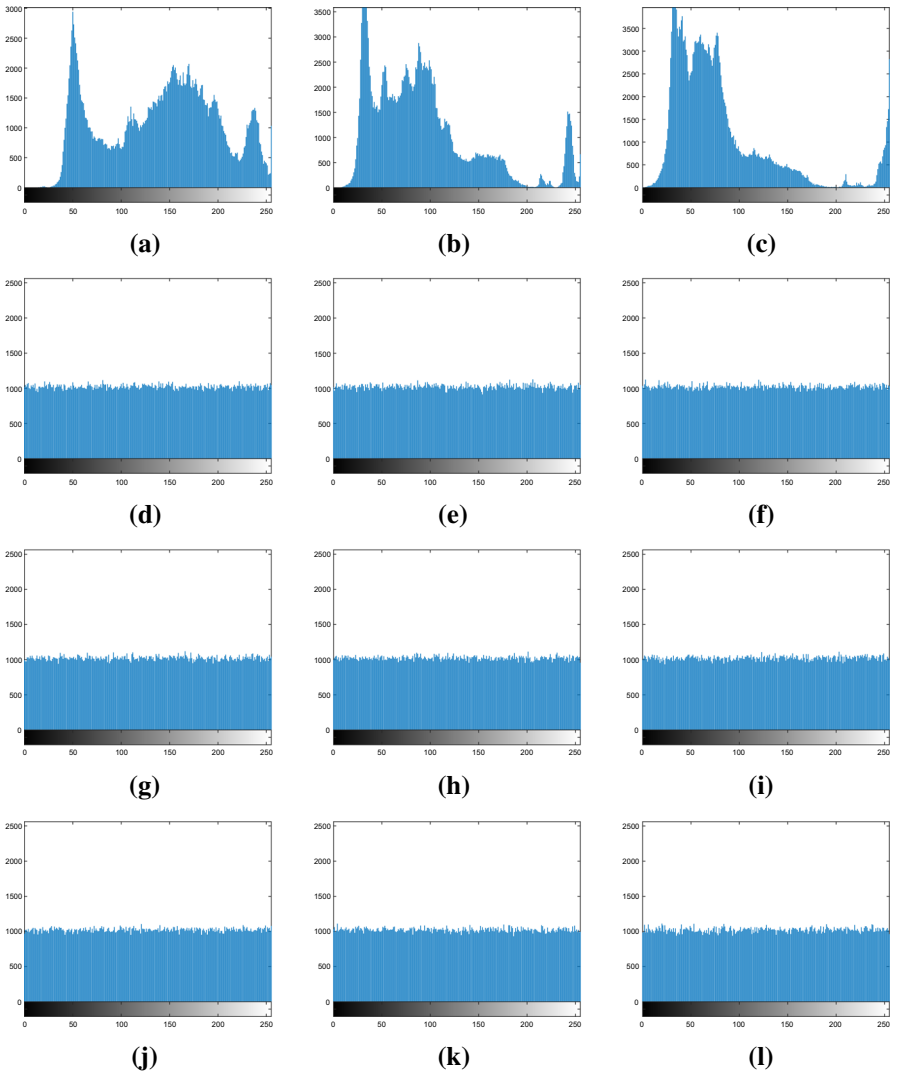

Fig. 13 Histogram distributions of the original and encrypted images

5.2.3 Information entropy

Information entropy is a statistical measure of uncertainty feature of the image. And the entropy $H(s)$ of a message source can be calculated as:

$$H(s) = -\sum_{i=0}^{2^N-1} p(s_i) \log_2 p(s_i), \tag{32}$$

where $p(s_i)$ represents the probability of the occurrence of symbol s_i and the ideal entropy value for an encrypted image should be 8 bits. A cryptosystem is reliable if

Table 6 Information entropy of the original and encrypted images (bit)

Channels	Original image	Our scheme			Scheme in [33]
		Keys 1	Keys 2	Keys 3	
Splash (R)	6.9481	7.9993	7.9992	7.9994	7.9959
Splash (G)	6.8845	7.9993	7.9993	7.9992	7.9951
Splash (B)	6.1265	7.9993	7.9993	7.9991	7.9957
Lena (R)	7.6503	7.9993	7.9993	7.9994	7.9950
Lena (G)	7.3053	7.9992	7.9994	7.9994	7.9953
Lena (B)	7.0746	7.9993	7.9993	7.9992	7.9955

and only if the entropy value of encrypted image is close to the ideal value to resist the entropy attacks. With the proposed image encryption scheme and the scheme in [33], counting times of each pixel in three primary colors (R, G, B) and calculating the corresponding probability, three color channels corresponding to the information entropy are listed in Table 6. From the results of statistics, the loss in the processing of information encryption is completely weak; thus, the proposed scheme is stable and secure against entropy attack. Compared with the scheme in [33], the entropy values of the encrypted images using our scheme are more close to the ideal value. Hence, our scheme is more secure against the entropy attack.

5.3 Key security analysis

5.3.1 Key space analysis

A desirable image encryption scheme should have a sufficiently large key space to resist brute-force attacks. It is recommended that the ideal key space should be larger than 2^{100} considering the current computer computation speed [45]. In our proposed encryption scheme, the total number of injection times is 3 and the key space is composed of: (1) six initial values selected randomly $x_1(0), y_1(0), z_1(0), x_2(0), y_2(0), z_2(0)$ and (2) three injected impulse signal values $\Delta x_{1(1)}, \Delta x_{1(2)}, \Delta x_{1(3)}$. Generally, the valid precision of state variables of nonlinear differential chaotic system is 10^{-14} [46], so the total key space reaches $S = 10^{14\times(6+3)} \gg 2^{100}$. Thus, the encryption scheme proposed in this paper has high security. It can resist brute-force attacks, even the attack from a quantum computer.

5.3.2 Key sensitivity analysis

Key sensitivity is an essential property for any good cryptosystem, which ensures that one cannot obtain any useful information from the decrypted image when a tiny change occurs to the keys. Here, for the original color image "Lena," keys 1 is taken as an example to simulate the key sensitivity of our proposed encryption scheme. Figure 14a shows the decrypted image "Lena" with correct keys. Figure 14b–j shows the decrypted images "Lena" with incorrect keys deviated 10^{-14}

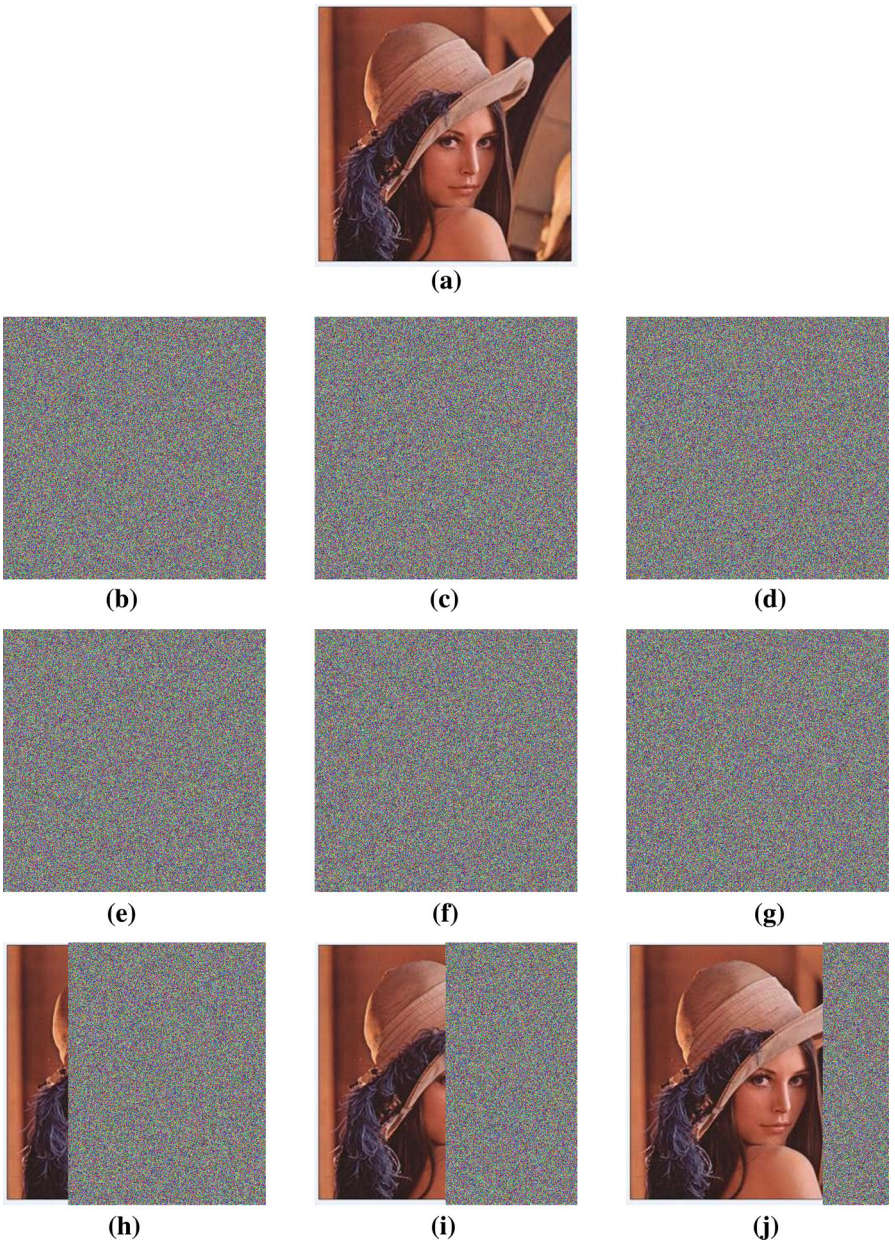

Fig. 14 Decrypted images with: **a** correct keys, **b** incorrect $x_1(0) + 10^{-14}$, **c** incorrect $y_1(0) + 10^{-14}$, **d** incorrect $z_1(0) + 10^{-14}$, **e** $x_2(0) + 10^{-14}$, **f** $y_2(0) + 10^{-14}$, **g** $z_2(0) + 10^{-14}$, **h** $\Delta x_1(1) + 10^{-14}$, **i** $\Delta y_1(1) + 10^{-14}$, **j** $\Delta z_1(1) + 10^{-14}$

from $x_1(0)$, $y_1(0)$, $z_1(0)$, $x_2(0)$, $y_2(0)$, $z_2(0)$, $\Delta x_{1(1)}$, $\Delta x_{1(2)}$ and $\Delta x_{1(3)}$, respectively, while the other keys are all right.

In order 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:

$$\mathrm{PSNR} = 20\log_{10}\left(\frac{255}{\sqrt{\frac{1}{3\times m\times n}\sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{k=1}^{3}\left[I'(i,j,k)-I(i,j,k)\right]^2}}\right), \tag{33}$$

where $m \times n$ is the size of image, and $I'(i, j)$ and $I(i, j)$ denote the restored image and the original image, respectively. After the comparison our restored images I' to the original images I, the RGB-PSNR values of six restored images are obtained as shown in Table 7.

From Fig. 14, when the decryption key deviated 10^{-14} from the correct key including $x_1(0), y_1(0), z_1(0), x_2(0), y_2(0), z_2(0)$, the decryption image has become an uniform white noise without any visual information. From Table 7, when the decryption key deviated 10^{-14} from the correct key including $x_1(0), y_1(0), z_1(0), x_2(0), y_2(0), z_2(0)$, there is almost no difference in the PSNR of the decrypted image and the corresponding encrypted image, and when the decryption key deviated 10^{-14} from the correct key including $\Delta x_{1(1)}, \Delta x_{1(2)}, \Delta x_{1(3)}$, a part of the visual information of the original image is decrypted and the PSNR of the decrypted image is only about 9, 11 or 14. It is proved that the correct image can be reconstructed only when the decryption key and the encryption key match accurately. Because the key space of the proposed encryption scheme is very big, unless someone has obtained in advance the correct secret key, it is almost impossible to accurately restore the original image.

5.4 The influence of noises in transmission

In the transmission process, the encrypted image is always interfered by noises. In order to test the impact of the noise interference on the proposed image encryption scheme, the noise is added into the encrypted image in the following method:

$$E' = E + k \cdot D, \tag{34}$$

where E and E' are encrypted image and noisy encrypted image, respectively, k is a coefficient indicating the noise strength, and D represents Gaussian random data with zero mean and standard deviation. In this subsection, for our proposed encrypted scheme, keys 1 is taken as an example to simulate the influence of noises in transmission. The decrypted images when k equals 0, 1, 3, 5, 7, 10 are shown in Fig. 15. It is found that the major information of the original color images can still be recognized

Table 7 RGB-PSNR values of six encrypted images and the restored images by the secret keys with a slight change

Decryption keys	Splash	Baboon	Lena	Sailboat	Peppers	House
Incorrect $x_1\ (0) + 10^{-14}$	7.6333	8.7789	8.1932	8.0854	8.0803	8.4726
Incorrect $y_1\ (0) + 10^{-14}$	7.6298	8.7670	8.1947	8.0851	8.0723	8.4682
Incorrect $z_1\ (0) + 10^{-14}$	7.6334	8.7768	8.1964	8.0838	8.0860	8.4735
Incorrect $x_2\ (0) + 10^{-14}$	7.6270	8.7790	8.1918	8.0812	8.0896	8.4629
Incorrect $y_2\ (0) + 10^{-14}$	7.6410	8.7790	8.1930	8.0866	8.0840	8.4694
Incorrect $z_2\ (0) + 10^{-14}$	7.6271	8.7776	8.1906	8.0881	8.0779	8.4664
Incorrect $\Delta x_1\ (1) + 10^{-14}$	8.8792	9.9623	9.5401	9.3621	9.3725	9.6749
Incorrect $\Delta y_1\ (1) + 10^{-14}$	10.5230	11.9781	11.3262	11.2553	11.1703	11.4412
Incorrect $\Delta z_1\ (1) + 10^{-14}$	13.2617	15.6914	14.1102	14.3447	14.0233	14.4674
Encrypted image	7.6324	8.7792	8.1975	8.0862	8.0837	8.4735

from the decrypted images, although the decrypted images turn blurrier with the noise intensity increasing. Thus, the encryption scheme proposed in this paper can resist noise interference to some degree.

5.5 Computational complexity

Assume the original color image to be encrypted is divided into three gray components and each component is represented by a channel. The channel can be viewed as a $2^n \times 2^n$ gray image. In our scheme, the computational complexity depends on XOR operations and right cycle shift operations. According to the parallel characteristics of quantum computation, the grayscale information for each pixel of the quantum image is performed by the quantum XOR operation, which is realized by using a $2n$-CNOT gate. It is understood that each n-CNOT gate can be decomposed into $4n - 8$ Toffoli gates, and the Toffoli gate can be realized by six controlled NOT gates [26]. Thus, the quantum image XOR operation needs $128 - 256$ basic gates. Consequently, the computational complexity of the quantum image XOR operation is $O\ (n)$. The complexity of the quantum color image right cycle shift operations could be evaluated via the complexity of the quantum sub-operation S_{YX}. The quantum sub-operation S_{YX} is implemented by operation U_{YX}. A color image right cycle shift operation involves $8 \times (r + s + t)$ swap gates, and each swap gate can be broken down into three CNOT gates. The number of unit gates included in the operations U_{YX} is $24 \times (r+s+t)$, where r, s, t represent the times of three channels of each pixel right cycle shift operations, respectively. Because $0 \leq r, s, t \leq 7$, the color image right cycle shift operation consists of 24×21 basic gates at most. Therefore, the total computational complexity of the proposed quantum color image encryption scheme is $O\ (n)$, while the total computational complexity in the corresponding classical case is $O\left(3 \times 2^{2n}\right)$. It is easily seen that the proposed quantum color image encryption scheme has a better performance than the classical counterparts in terms of the computational complexity.

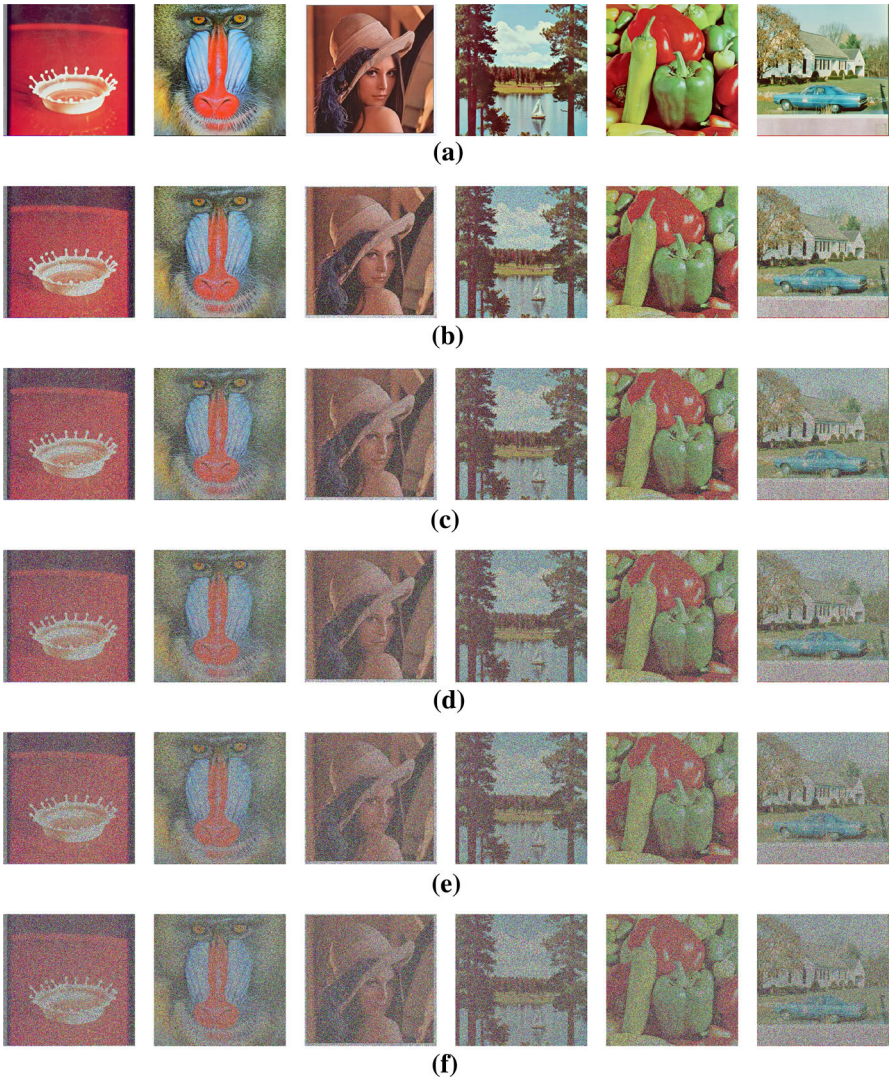

Fig. 15 Results of noise attack with different noise intensities: **a** $k = 0$, **b** $k = 1$, **c** $k = 3$, **d** $k = 5$, **e** $k = 7$ and **f** $k = 10$

6 Conclusion

In this paper, we have proposed a quantum color image encryption scheme based on coupled hyper-chaotic Lorenz system with three impulse injections. Firstly, since the short-period behavior of chaotic system after too many iterations can lead to degeneration of dynamics, three impulse signal values are injected into coupled hyper-chaotic Lorenz system during iterations to enhance the complexity of trajectory and make the encryption scheme whose key streams are generated from this system safer.

Then, in the encryption process, we use the NCQI model to represent the quantum color original image, in which 24 qubits are employed to represent the pixel color scale values of each pixel and six sequences generated from coupled hyper-chaotic Lorenz system are used to encrypt the red, green and blue components by XOR operations and right cyclic shift operations. Therefore, our scheme has three merits: (1) It is free from the influence of quantum states collapse and can obtain accurate pixel values in quantum measurement; (2) three impulse signal values are injected into coupled hyper-chaotic Lorenz system during iterations which can enhance the complexity of trajectory; (3) six initial values and three impulse signals values are used as keys, which could reduce the burden of keys transmission and make the cryptosystem own a key space large enough to resist exhaustive attack, even the attack from a quantum computer. Numerical simulations demonstrate that the proposed encryption scheme has a good feasibility and effectiveness for protecting quantum color images and is more secure in comparison with other encryption algorithms.

Acknowledgements The authors acknowledge the support from the National Natural Science Foundation of China (61671179) and the National Key Basic Research Program of China (2013CB329003).

References

1. Liu, Z., Li, S., Liu, W., et al.: Image encryption algorithm by using fractional Fourier transform and pixel scrambling operation based on double random phase encoding. Opt. Laser Eng. **51**(1), 8–14 (2013)
2. Zhao, T., Ran, Q., Yuan, L., et al.: Image encryption using fingerprint as key based on phase retrieval algorithm and public key cryptography. Opt. Laser Eng. **72**, 12–17 (2015)
3. Kumar, M., Iqbal, A., Kumar, P.: A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography. Signal Process. **125**, 187–202 (2016)
4. Zhou, Y., Bao, L., Chen, C.P.: A new 1D chaotic system for image encryption. Signal Process. **97**, 172–182 (2014)
5. Wang, X., Gu, S., Zhang, Y.: Novel image encryption algorithm based on cycle shift and chaotic system. Opt. Laser Eng. **68**, 126–134 (2015)
6. Zhou, Y., Bao, L., Chen, C.P.: Image encryption using a new parametric switching chaotic system. Signal Process. **93**(11), 3039–3052 (2013)
7. Zhang, Y., Xiao, D., Shu, Y., et al.: A novel image encryption scheme based on a linear hyperbolic chaotic system of partial differential equations. Signal Process. Image **28**(3), 292–300 (2013)
8. Zhang, X., Zhu, H., Yao, H.: Analysis of a new three-dimensional chaotic system. Nonlinear Dyn. **67**(1), 335–343 (2012)
9. Feng, G., Cao, J.: Master–slave synchronization of chaotic systems with a modified impulsive controller. Adv. Differ. Equs. **2013**(1), 1–12 (2013)
10. Löytynoja, T., Li, X., Jänkälä, K., et al.: Quantum mechanics capacitance molecular mechanics modeling of core-electron binding energies of methanol and methyl nitrite on Ag (111) surface. J. Chem. Phys. **145**(2), 024703 (2016)
11. Yan, F., Iliyasu, A.M., Venegas-Andraca, S.E.: A survey of quantum image representations. Quantum Inf. Process. **15**(1), 1–35 (2016)
12. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2010)
13. Feynman, R.P.: Simulating physics with computers. Int. J. Theor. Phys. **21**(6/7), 467–488 (1982)
14. Venegas-Andraca, S.E., Bose, S.: Storing, processing and retrieving an image using quantum mechanics. In: Proceedings of the SPIE Conference on Quantum Information and Computation, pp. 137–147 (2003)
15. Venegas-Andraca, S.E., Ball, J.L., Burnett, K., Bose, S.: Processing images in entangled quantum systems. Quantum Inf. Process. **9**(1), 1–11 (2010)

16. Latorre, J.I.: Image compression and entanglement. arXiv:quant-ph/0510031 (2005)
17. Le, P.Q., Dong, F., Hirota, K.: A flexible representation of quantum images for polynomial preparation, image compression and processing operations. Quantum Inf. Process. **10**(1), 63–84 (2010)
18. Sun, B., Iliyasu, A.M., Yan, F., Dong, F.Y., Hirota, K.: An RGB multi-channel representation for images on quantum computers. J. Adv. Comput. Intell. Intell. Inf. **17**(3), 404–417 (2013)
19. Li, H.S., Zhu, Q.X., Zhou, R.G., Li, M.C., et al.: Multidimensional color image storage, retrieval, and compression based on quantum amplitudes and phases. Inf. Sci. **273**, 212–232 (2014)
20. Zhang, Y., Lu, K., Gao, Y.H., Xu, K.: A novel quantum representation for log-polar images. Quantum Inf. Process. **12**(9), 3103–3126 (2013)
21. Zhang, Y., Lu, K., Gao, Y.H., Wang, M.: NEQR: a novel enhanced quantum representation of digital images. Quantum Inf. Process. **12**(12), 2833–2860 (2013)
22. Sang, J., Wang, S., Li, Q.: A novel quantum representation of color digital images. Quantum Inf. Process. **16**(2), 42 (2017)
23. Zhou, R., Wu, Q., Zhang, M., et al.: Quantum image encryption and decryption algorithms based on quantum image geometric transformations. Int. J. Theor. Phys. **52**(6), 1802–1817 (2013)
24. 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)
25. Yang, Y.G., Jia, X., Sun, S.J., et al.: Quantum cryptographic algorithm for color images using quantum Fourier transform and double random-phase encoding. Inf. Sci. **277**(2), 445–457 (2014)
26. 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)
27. Liang, H., Tao, X., Zhou, N.: Quantum image encryption based on generalized affine transform and logistic map. Quantum Inf. Process. **15**(7), 2701–2724 (2016)
28. Yang, Y.G., Pan, Q.X., Sun, S.J., Xu, P.: Novel image encryption based on quantum walks. Sci. Rep. UK **5**, 7784 (2015)
29. Zhou, N., Hua, T., Gong, L., et al.: Quantum image encryption based on generalized Arnold transform and double random-phase encoding. Quantum Inf. Process. **14**(4), 1193–1213 (2015)
30. Yang, Y.G., Tian, J., Lei, H., et al.: Novel quantum image encryption using one-dimensional quantum cellular automata. Inf. Sci. **345**, 257–270 (2016)
31. 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. **55**(7), 3234–3250 (2016)
32. Zhou, N., Hu, Y., Gong, L., et al.: Quantum image encryption scheme with iterative generalized Arnold transforms and quantum image cycle shift operations. Quantum Inf. Process. **16**(6), 1–23 (2017)
33. Tan, R.C., Lei, T., Zhao, Q.M., et al.: Quantum color image encryption algorithm based on a hyper-chaotic system and quantum Fourier transform. Int. J. Theor. Phys. **55**(12), 5368–5384 (2016)
34. Li, P., Zhao, Y.: A simple encryption algorithm for quantum color image. Int. J. Theor. Phys. **56**(6), 1961–1982 (2017)
35. Grassi, G., Severance, F.L., Miller, D.A.: Multi-wing hyperchaotic attractors from coupled lorenz systems. Chaos Solitons Fractals **41**(1), 284–291 (2009)
36. Kempe, J., Bacon, D., Lidar, D.A., et al.: Theory of decoherence-free fault-tolerant universal quantum computation. Phys. Rev. A **63**(4), 392–396 (2000)
37. Cabello, A.: Six-qubit permutation-based decoherence-free orthogonal basis. Phys. Rev. A **75**(2), 441–445 (2007)
38. Maniscalco, S., Francica, F., Zaffino, R.L., et al.: Protecting entanglement via the quantum Zeno effect. Phys. Rev. Lett. **100**(9), 090503 (2008)
39. Paz-Silva, G.A., Rezakhani, A.T., Dominy, J.M., et al.: Zeno effect for quantum computation and control. Phys. Rev. Lett. **108**(8), 080501 (2012)
40. Viola, L., Knill, E., Lloyd, S.: Dynamical decoupling of open quantum systems. Phys. Rev. Lett. **82**(12), 2417–2421 (1999)
41. Souza, A.M., lvarez, G.A., Suter, D.: Robust dynamical decoupling for quantum computing and quantum memory. Phys. Rev. Lett. **106**(24), 240501 (2011)
42. Calderbank, A.R., Shor, P.W.: Good quantum error-correcting codes exist. Phys. Rev. A **54**(2), 1098–1105 (1995)
43. Steane, A.: Multiple-particle interference and quantum error correction. Proc. R. Soc. Lond. A **452**(1954), 2551–2577 (1996)
44. Devitt, S.J., Munro, W.J., Nemoto, K.: Quantum error correction for beginners. Rep. Prog. Phys. **76**(7), 076001 (2013)

45. Yap, W.S., Phan, R.C.W., Goi, B.M., et al.: On the effective subkey space of some image encryption algorithms using external key. J. Vis. Commun. Image R **40**, 51–57 (2016)
46. Wang, L.Y., Song, H.J., Liu, P.: A novel hybrid color image encryption algorithm using two complex chaotic systems. Opt. Laser Eng. **77**, 118–125 (2016)