Multimedia Tools and Applications (2020) 79:6661–6687
https://doi.org/10.1007/s11042-019-08514-z

Double quantum color images encryption scheme based on DQRCI

Ling Wang[1] · **Qiwen Ran**[1] · **Jing Ma**[1]

Received: 14 March 2019 / Revised: 6 October 2019 / Accepted: 26 November 2019 /
Published online: 17 December 2019

Abstract
In this paper, a double quantum color images representation model (DQRCI) which can store two color digital images simultaneously into a quantum superposition state is investigated. Based on DQRCI, some simple image processing operations are discussed and the corresponding quantum circuits are designed. The circuits indicate that these operations have very low computational complexity. Moreover, to ensure the security of DQRCI quantum state image, an encryption scheme is proposed and the validity verification of image encryption system in quantum field is given for the first time. Numerical simulation and performance comparison demonstrate that the proposed double quantum color images encryption scheme outperforms the previous pertinent work in terms of security and computational complexity. This work will help the researchers to further investigate more efficient quantum image representation model and corresponding encryption algorithm.

Keywords DQRCI · Double quantum images encryption · Quantum computation · Validity verification

1 Introduction

In recent years, due to the outstanding properties of quantum computation, such as entanglement, superposition and parallelism, it has been widely applied into many fields of information sciences [1, 2, 5, 18]. Combining quantum mechanics with classical information theory has developed into an important and effective approach to improve information processing speed and enhance communication security [14]. As one of these applications and a young emerging cross-discipline of quantum mechanics and image processing, quantum image processing (QImP) which is devoted to making use of quantum computing technologies to capture, manipulate, and recover classical images for various purposes has become a hot research topic since it has huge storage capacity and parallel processing ability [27, 28].

✉ Ling Wang
wangling199059@163.com

[1] National Key Laboratory of Tunable Laser Technology, Harbin Institute of Technology, Harbin 150001, China

The first step of QImP is how to store classical images into quantum computers by utilizing qubits. Many quantum image representation models are gradually put forward, such as Qubit Lattice [23], Entangled Image [22], Real Ket [8], FRQI [9], MCQI [20], QUALPI [35], NEQR [34], GQIR [7], NCQI [17], FQRCI [30], IFRQI [16], OCQR [12] and QRCI [26]. The existing representation models mainly focus on single quantum gray or color image, while the investigation on double quantum color images representation is still scarce.

Where there is information, where there will be dissemination. Undoubtedly, when the image information is transmitted through a public channel, attackers may intercept it and do some illegal operations such as duplication, modification and forgery. So it is very necessary to have some useful techniques to prevent the illegal invasions. One of the simplest and most efficient methods for protecting image data is image encryption which ensures that unauthorized persons could not obtain the original image without correct keys even if the encrypted image information is divulged. Quantum image encryption is defined as the approach of transforming a meaningful original quantum state image into a disordered one by performing quantum operations on a quantum image representation. Many algorithms for quantum image encryption have been suggested [3, 6, 10, 11, 15, 21, 29, 31, 32, 36, 37, 39]. Several examples can be considered; in 2013, Zhou et al. put forward a quantum image encryption and decryption algorithm by employing quantum image geometric transformations [36]. Following that, in 2015, Yang et al. presented an image encryption algorithm based on quantum walks [31]. Afterward, they investigated another quantum image encryption algorithm by using one-dimensional quantum cellular automata [32]. Subsequently, Gong et al. designed a quantum image encryption algorithm based on quantum image XOR operations [3]. And more recently, Ran et al. raised a quantum color image encryption scheme based on coupled hyper-chaotic Lorenz system with three impulse injections [15]. Zhou et al. investigated a bit-level quantum color image encryption scheme with cross-exchange operation and hyper-chaotic system, in which the gray values of three channels (RGB) were swapped to enhance the scrambling effect [39]. However, all the encryption schemes introduced above are devised for single quantum image.

Uniquely, in order to encrypt two images simultaneously in quantum computers, Liu et al. designed a double quantum image encryption algorithm based on quantum Arnold transform (QAT) and random qubit rotation, in which QAT was used to scramble the pixel's position information and the corresponding gray information was altered by using random qubit rotation [13]. The theoretical analyses and numerical simulations had shown that it has superior performance in computational complexity and security. But, through our analysis, it is found that this encryption algorithm has some disadvantages as follows: (1) It is designed to deal with quantum gray images, while it is not applicable to quantum color images; (2) It directly adopts FRQI model to represent two original gray images, but it not devises an effective quantum representation model to store two images simultaneously, which leads to the storage resource (i.e., the number of qubits) required is not reduced; (3) FRQI model utilizes probability amplitudes of quantum states to store the gray information, so it is difficult to retrieve the classical image from a FRQI quantum state accurately. Despite aforementioned shortcomings, this article is the first paper to implement double quantum image encryption which can achieve the aim of improving the quantum image encryption efficiency. To conquer above problems, in this contribution, firstly, a double quantum color images representation model, i.e., DQRCI, together with its corresponding quantum circuit are investigated, by which two color digital images could be stored simultaneously into a quantum superposition state. Moreover, some simple DQRCI-based image processing operations are discussed and the corresponding quantum circuits are designed.

Through analyses, it has been proved that DQRCI representation model has the following advantages:

1. DQRCI can save more storage space since it only employs $2n + 9$ qubits to store two color images of size $2^n \times 2^n$, while $(2n + 24) \times 2$ qubits are needed to encode the same images' information in NCQI.
2. Different from FQRCI in which color information is stored as the probability amplitudes of three single qubits, the classical color images can be accurately retrieved from DQRCI quantum state due to the color information is encoded by the basis state of qubit sequence.
3. The complex and elaborate color transformations could be performed on DQRCI conveniently and some simple DQRCI-based image processing operations have very low computational complexity.

Furthermore, to ensure the security of DQRCI quantum state image, an encryption scheme is proposed. The validity verification of encryption system in quantum field is given for the first time. Numerical simulation and performance comparison demonstrate that the proposed double quantum color images encryption scheme shows better performance in histogram, correlation, information entropy and computational complexity.

The rest of this paper is organized as follows. Section 2 investigates DQRCI quantum image representation model, preparation and retrieving. Section 3 discusses some simple DQRCI-based image processing operations and designs the corresponding quantum circuits. The proposed double quantum color images encryption/decryption scheme and validity verification are described in Section 4. Section 5 gives numerical simulation and performance comparison. Finally, the conclusion work is drawn in Section 6.

2 DQRCI quantum image representation model, preparation and retrieving

2.1 DQRCI quantum image representation model and preparation

In ref. [26], QRCI representation model is proposed to store a color digital image of size $2^n \times 2^n$ with every channel ranged $[0, 255]$ in quantum computers. It uses three entangled qubit sequences to encode the image information, where the color information of three channels (R,G,B) is encoded into the first qubit sequence, while the corresponding bit-plane information and position information are encoded into the second and third qubit sequence, respectively. Its modularized preparation circuit is shown in Fig. 1 and the corresponding quantum representation can be written as

$$\begin{aligned} |I\rangle &= \frac{1}{\sqrt{2^{2n+3}}} \sum_{L=0}^{2^3-1} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} |C_L(Y,X)\rangle \otimes |L\rangle \otimes |YX\rangle \\ &= \frac{1}{\sqrt{2^{2n+3}}} \sum_{L=0}^{2^3-1} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} |R_{LYX} G_{LYX} B_{LYX}\rangle \otimes |L\rangle \otimes |YX\rangle \end{aligned} \tag{1}$$

$$|L\rangle = |L_2 L_1 L_0\rangle \tag{2}$$

$$|YX\rangle = |Y\rangle |X\rangle = |Y_{n-1} Y_{n-2} \ldots Y_0\rangle |X_{n-1} X_{n-2} \ldots X_0\rangle \tag{3}$$

where $|L\rangle$ and $|YX\rangle$ denote the bit-plane information and position information, respectively; $|C_L(Y, X)\rangle$ represents the corresponding color information of pixel (Y, X) in bit-plane L; $R_{LYX}, G_{LYX}, B_{LYX} \in \{0, 1\}$, $L = 0, 1, \ldots, 7$, $Y, X = 0, 1, \ldots, 2^n - 1$.

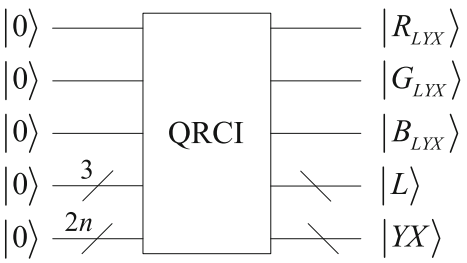


Fig. 1 Modularized preparation circuit of QRCI

Inspired by QRCI, by taking full advantage of quantum superposition and quantum entanglement, we investigate DQRCI representation model to store two color images of size $2^n \times 2^n$ with every channel ranged [0, 255] simultaneously as follows

$$\begin{aligned}|D\rangle &= \frac{1}{\sqrt{2^{2n+3}}}\sum_{L=0}^{2^3-1}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|C(L,Y,X)\rangle\otimes|L\rangle\otimes|YX\rangle \\ &= \frac{1}{\sqrt{2^{2n+3}}}\sum_{L=0}^{2^3-1}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\left|C_L^1(Y,X)\,C_L^2(Y,X)\right\rangle\otimes|L\rangle\otimes|YX\rangle \\ &= \frac{1}{\sqrt{2^{2n+3}}}\sum_{L=0}^{2^3-1}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\left|R_{LYX}^1G_{LYX}^1B_{LYX}^1R_{LYX}^2G_{LYX}^2B_{LYX}^2\right\rangle\otimes|L\rangle\otimes|YX\rangle\end{aligned} \tag{4}$$

where $\left|C_L^1(Y,X)\right\rangle = \left|R_{LYX}^1G_{LYX}^1B_{LYX}^1\right\rangle$ and $\left|C_L^2(Y,X)\right\rangle = \left|R_{LYX}^2G_{LYX}^2B_{LYX}^2\right\rangle$ represent the color information of pixel $|YX\rangle$ in bit-plane $|L\rangle$ in two images, respectively.

According to ref. [17], $(2n+24)\times 2$ qubits are needed to encode two color digital images of size $2^n \times 2^n$ with every channel ranged [0, 255] in NCQI. However, DQRCI only employs $2n+9$ qubits to store the same image information. The quantum circuit of encoding image information in DQRCI representation model is designed in Fig. 2.

Figure 3 shows the modularized preparation circuit of DQRCI.

Taking two color images with size 2×2 shown in Fig. 4 as examples, the DQRCI expression is as

$$\begin{aligned}|D\rangle = \frac{1}{\sqrt{2^5}}[&|100000\rangle\otimes|000\rangle\otimes|00\rangle + |000001\rangle\otimes|000\rangle\otimes|01\rangle + |001000\rangle\otimes|000\rangle\otimes|10\rangle \\ &+|110000\rangle\otimes|000\rangle\otimes|11\rangle + |100000\rangle\otimes|001\rangle\otimes|00\rangle + |000101\rangle\otimes|001\rangle\otimes|01\rangle \\ &+|101000\rangle\otimes|001\rangle\otimes|10\rangle + |110000\rangle\otimes|001\rangle\otimes|11\rangle + |110010\rangle\otimes|010\rangle\otimes|00\rangle \\ &+|100101\rangle\otimes|010\rangle\otimes|01\rangle + |011000\rangle\otimes|010\rangle\otimes|10\rangle + |110111\rangle\otimes|010\rangle\otimes|11\rangle \\ &+|100000\rangle\otimes|011\rangle\otimes|00\rangle + |010001\rangle\otimes|011\rangle\otimes|01\rangle + |001110\rangle\otimes|011\rangle\otimes|10\rangle \\ &+|110000\rangle\otimes|011\rangle\otimes|11\rangle + |100000\rangle\otimes|100\rangle\otimes|00\rangle + |000101\rangle\otimes|100\rangle\otimes|01\rangle \\ &+|101000\rangle\otimes|100\rangle\otimes|10\rangle + |110000\rangle\otimes|100\rangle\otimes|11\rangle + |110010\rangle\otimes|101\rangle\otimes|00\rangle \\ &+|100001\rangle\otimes|101\rangle\otimes|01\rangle + |111000\rangle\otimes|101\rangle\otimes|10\rangle + |110111\rangle\otimes|101\rangle\otimes|11\rangle \\ &+|110010\rangle\otimes|110\rangle\otimes|00\rangle + |110001\rangle\otimes|110\rangle\otimes|01\rangle + |011110\rangle\otimes|110\rangle\otimes|10\rangle \\ &+|110111\rangle\otimes|110\rangle\otimes|11\rangle + |100000\rangle\otimes|111\rangle\otimes|00\rangle + |010101\rangle\otimes|111\rangle\otimes|01\rangle \\ &+|001110\rangle\otimes|111\rangle\otimes|10\rangle + |110000\rangle\otimes|111\rangle\otimes|11\rangle]\end{aligned} \tag{5}$$

2.2 Image retrieving

Because quantum state image cannot be recognized by human eyes, it is an important processing operation to retrieve classical image from quantum system accurately. Quantum measurement is a unique way to retrieve classical image from quantum state. During

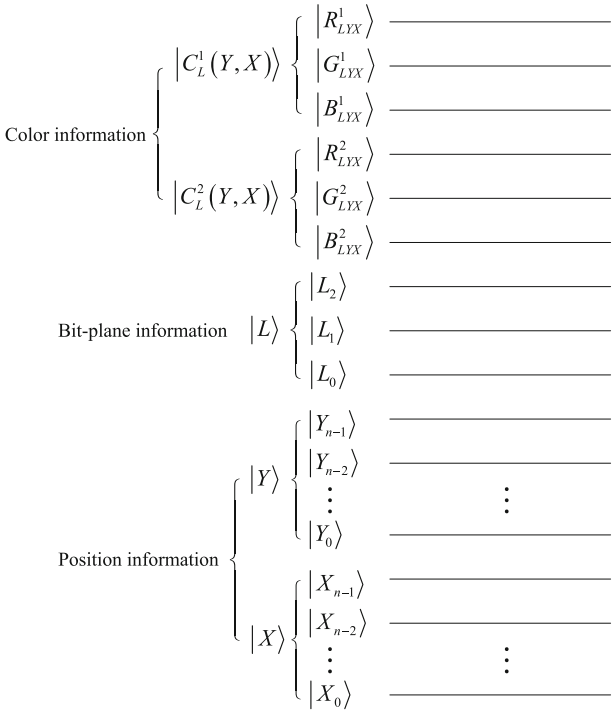


Fig. 2 The quantum circuit of encoding image information in DQRCI representation model

image retrieval from DQRCI quantum image, every pixel in each bit-plane should be recovered individually. The measurement operation Ω for bit-plane informaiton and position information as defined in (6) is used to extract the information of a single pixel

$$\Omega = \sum_{L=0}^{2^3-1} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} |I\rangle^{\otimes 6} \otimes |L\rangle \otimes |YX\rangle \otimes \langle YX| \otimes \langle L| \tag{6}$$

By applying Ω to DQRCI quantum state image $|D\rangle$ in (4), $|H_{LYX}\rangle$ which contains the corresponding information of pixel $|YX\rangle$ in bit-plane $|L\rangle$ is obtained

$$|H_{LYX}\rangle = |C\,(L, Y, X)\rangle \otimes |L\rangle \otimes |YX\rangle \tag{7}$$

The projective measurement operation F is constructed as follows

$$F = \sum_{f=0}^{2^6-1} f\,|f\rangle\,\langle f| \tag{8}$$

Through performing F on $|H_{LYX}\rangle$, the color information of two images can be retrieved, i.e., $C\,(L, Y, X) = 2^5 \times R_{LYX}^1 + 2^4 \times G_{LYX}^1 + 2^3 \times B_{LYX}^1 + 2^2 \times R_{LYX}^2 + 2^1 \times G_{LYX}^2 + 2^0 \times B_{LYX}^2$.

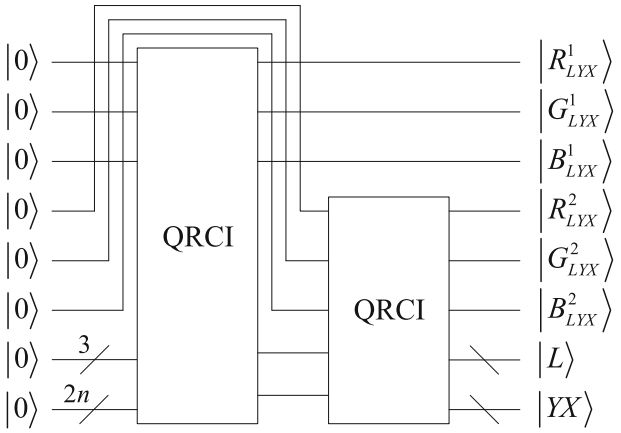


Fig. 3 Modularized preparation circuit of DQRCI

For pixel $|YX\rangle$ in bit-plane $|L\rangle$, the accurate color information of two images equals to the expectation value $\langle C(L,Y,X)|\, F\, |C(L,Y,X)\rangle$

$$\begin{aligned} &\langle C(L,Y,X)|F|C(L,Y,X)\rangle \\ =\ &\langle C(L,Y,X)|\left(\sum_{f=0}^{2^6-1} f\,|f\rangle\langle f|\right)|C(L,Y,X)\rangle \\ =\ &\sum_{f=0}^{2^6-1} f\langle C(L,Y,X)|\,(|f\rangle\langle f|)\,|C(L,Y,X)\rangle \\ =\ &C(L,Y,X) \end{aligned} \tag{9}$$

It can be seen from (9) that the two classical color images can be accurately retrieved from DQRCI quantum state image if all pixels in all eight bit-planes are retrieved.

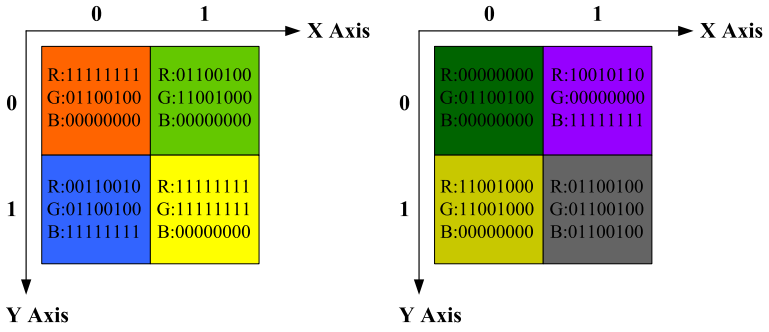


Fig. 4 Two color digital images with size 2 × 2

3 Some simple DQRCI-based image processing operations

3.1 Color complement operation

Color complement operation U_C is defined as

$$U_C = X^{\otimes 6} \otimes I^{\otimes 2n+3} \tag{10}$$

where X represents quantum NOT gate

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{11}$$

The output of performing U_C on the state $|D\rangle$ in (4) can be described as follows

$$U_C |D\rangle = \frac{1}{\sqrt{2^{2n+3}}} \sum_{L=0}^{2^3-1} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} \left|\bar{R}^1_{LYX} \bar{G}^1_{LYX} \bar{B}^1_{LYX} \bar{R}^2_{LYX} \bar{G}^2_{LYX} \bar{B}^2_{LYX}\right\rangle \otimes |L\rangle \otimes |YX\rangle \tag{12}$$

where, $\left|\bar{K}^j_{LYX}\right\rangle = \left|1 - K^j_{LYX}\right\rangle$, $K \in \{R, G, B\}$, $j = 1, 2$.

The quantum circuit of color complement operation U_C in DQRCI is demonstrated in Fig. 5. It can be seen that the color complement operation can be implemented by 6 NOT gates.

3.2 Channel swapping operation

The first type of channel swapping operation U^1_S is defined as

$$U^1_S = I \otimes swap\,(3) \otimes I^{\otimes 2n+5} \tag{13}$$

where, $swap\,(3)$ gate is shown in Fig. 6.

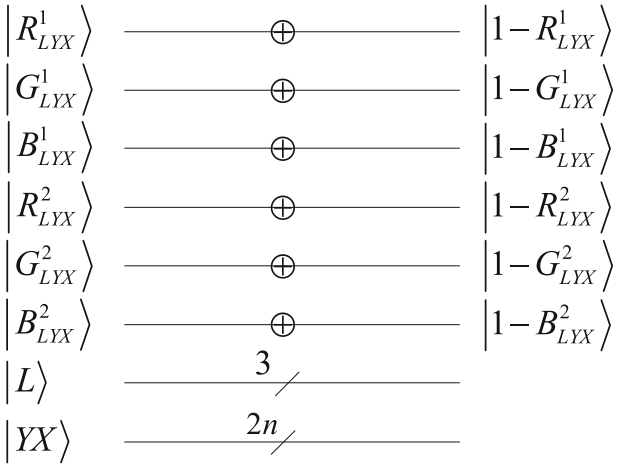


Fig. 5 The quantum circuit of color complement operation U_C in DQRCI

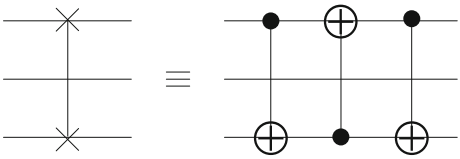


Fig. 6 Notation of $swap$ (3) gate

The result after executing U_S^1 to the state $|D\rangle$ in (4) is presented as below

$$U_S^1 |D\rangle = \frac{1}{\sqrt{2^{2n+3}}} \sum_{L=0}^{2^3-1} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} \left| R_{LYX}^1 R_{LYX}^2 B_{LYX}^1 G_{LYX}^1 G_{LYX}^2 B_{LYX}^2 \right\rangle \otimes |L\rangle \otimes |YX\rangle \tag{14}$$

The second type of channel swapping operation U_S^2 is defined as

$$U_S^2 = I^{\otimes 2} \otimes swap\,(3) \otimes I^{\otimes 2n+4} \tag{15}$$

The production of performing U_S^2 on the state $|D\rangle$ in (4) is expressed as follows

$$U_S^2 |D\rangle = \frac{1}{\sqrt{2^{2n+3}}} \sum_{L=0}^{2^3-1} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} \left| R_{LYX}^1 G_{LYX}^1 G_{LYX}^2 R_{LYX}^2 B_{LYX}^1 B_{LYX}^2 \right\rangle \otimes |L\rangle \otimes |YX\rangle \tag{16}$$

The quantum circuits of channel swapping operations U_S^1 and U_S^2 in DQRCI are illustrated in Fig. 7. It can be seen that both channel swapping operations can be implemented by 3 CNOT gates.

3.3 Bit-plane reversing operation

The bit-plane reversing operation U_R is defined as

$$U_R = I^{\otimes 6} \otimes X^{\otimes 3} \otimes I^{\otimes 2n} \tag{17}$$

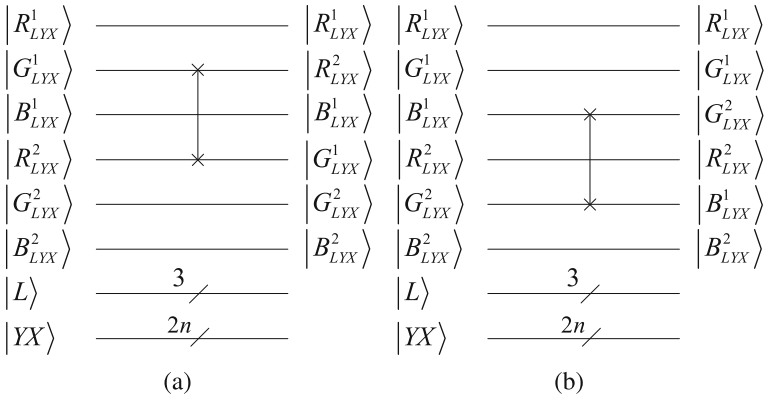


Fig. 7 The quantum circuits of channel swapping operations in DQRCI: **a** U_S^1, **b** U_S^2

The outcome of performing U_R on the state $|D\rangle$ in (4) is shown as below

$$U_R|D\rangle = \frac{1}{\sqrt{2^{2n+3}}} \sum_{L=0}^{2^3-1} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} \left| R^1_{LYX} G^1_{LYX} B^1_{LYX} R^2_{LYX} G^2_{LYX} B^2_{LYX} \right\rangle \otimes |7-L\rangle \otimes |YX\rangle \tag{18}$$

The quantum circuit of bit-plane reversing operation U_R in DQRCI is given in Fig. 8. It can be seen that the bit-plane reversing operation can be implemented by 3 NOT gates.

3.4 Color transformation

Color transformation U can be designed by combining the above operations

$$U = U_R U_S^2 U_S^1 U_C \tag{19}$$

Obviously, the transformation U is reversible, and $U^{-1} = U_C U_S^1 U_S^2 U_R$.

The quantum circuit of color transformation U in DQRCI is shown in Fig. 9. It can be seen that the color transformation can be implemented by 9 NOT gates and 6 CNOT gates.

Taking two color images with size 512×512 as examples, Fig. 10 displays the output ones after applying the transformation U.

From Fig. 10, it can be seen that the designed color transformation U can transform two original color images into meaningless ones, i.e., visual acuity is lost. Therefore, in the following encryption scheme to be put forward, we use the transformation U as an encryption method to hide original image information.

4 Double quantum color images encryption/decryption scheme and validity verification

4.1 Double quantum color images encryption scheme

The proposed double quantum color images encryption scheme based on DQRCI consists of two stages as illustrated in Fig. 11. First, the quantum color transformation is performed

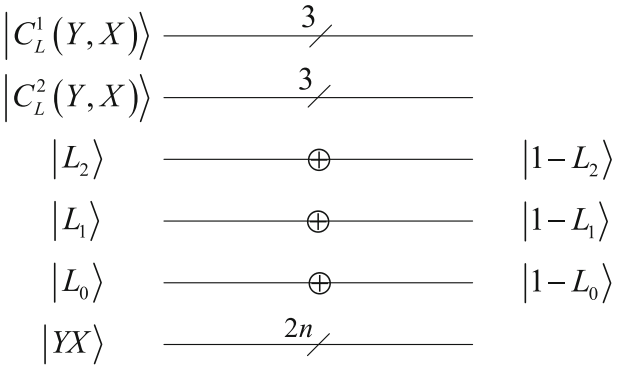


Fig. 8 The quantum circuit of bit-plane reversing operation U_R in DQRCI

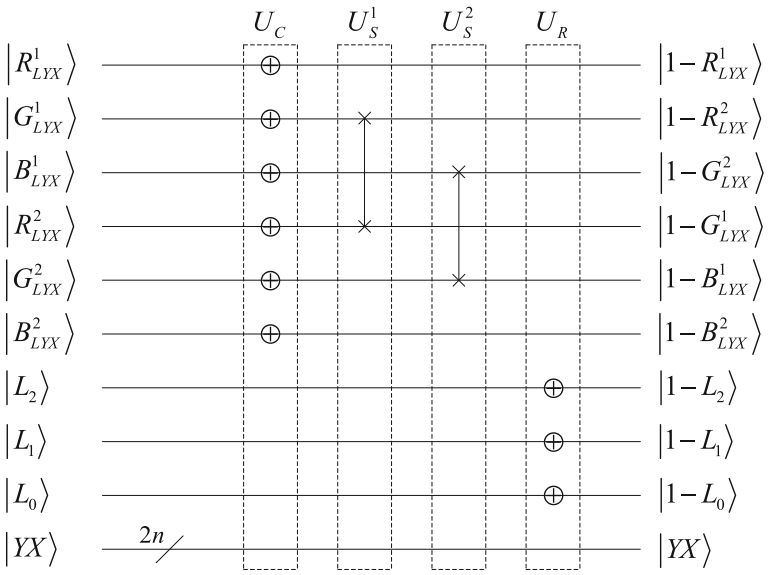
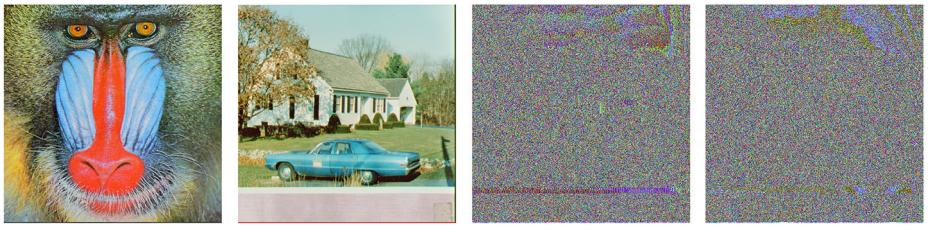


Fig. 9 The quantum circuit of special color transformation U in DQRCI

on color information and bit-plane information without changing the position information. Then, to enhance the security of encryption scheme and make the distribution of pixel values more uniform, the color information is modified by quantum XOR operation, while the bit-plane information and position information remain unchanged. Figure 12 demonstrates the specific flowchart of encryption and decryption scheme.

Input: original DQRCI quantum stage image $|D\rangle$ in (4).
Keys: $x_1(0), y_1(0), z_1(0), x_2(0), y_2(0), z_2(0)$.
Output: encrypted DQRCI quantum stage image $|E\rangle$.



(a) (b) (c) (d)

Fig. 10 Simulation results: **a** Baboon, **b** House, **c** Transformed Baboon, **d** Transformed House

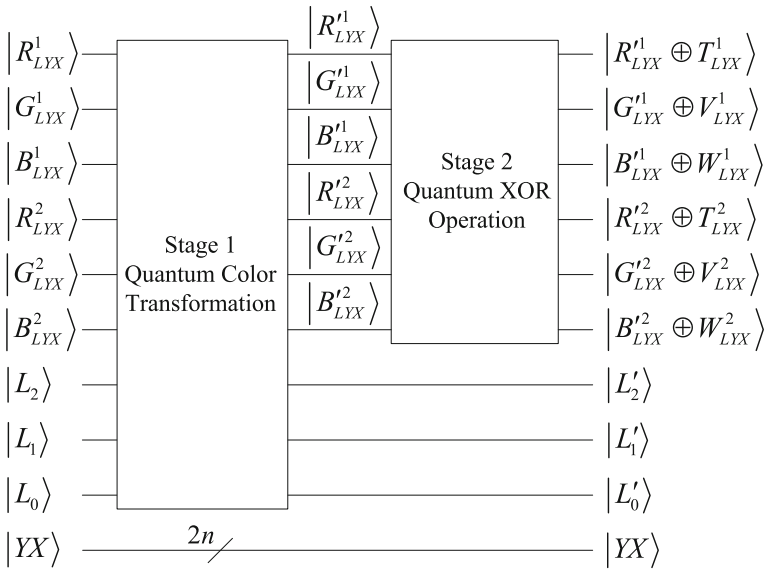


Fig. 11 Encryption process

Stage 1: quantum color transformation

Through performing the color transformation U on $|D\rangle$, $|E'\rangle$ can be obtained

$$\begin{aligned}|E'\rangle &= U\left(\frac{1}{\sqrt{2^{2n+3}}}\sum_{L=0}^{2^3-1}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|R^1_{LYX}G^1_{LYX}B^1_{LYX}R^2_{LYX}G^2_{LYX}B^2_{LYX}\rangle\otimes|L\rangle\otimes|YX\rangle\right)\\ &= \frac{1}{\sqrt{2^{2n+3}}}\sum_{L=0}^{2^3-1}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\left|R'^1_{LYX}G'^1_{LYX}B'^1_{LYX}R'^2_{LYX}G'^2_{LYX}B'^2_{LYX}\right\rangle\otimes|L'\rangle\otimes|YX\rangle\end{aligned} \tag{20}$$

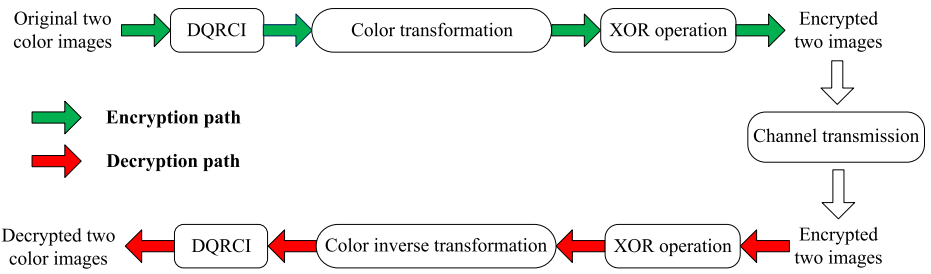


Fig. 12 Flowchart of encryption and decryption scheme

Stage 2: quantum XOR operation

The coupled hyper-chaotic Lorenz system is defined as

$$\begin{cases} \dot{x}_1 = \sigma\left(y_1 - x_1\right) \\ \dot{y}_1 = \rho x_1 - y_1 - x_1 z_1 + k_1\left(x_2 - y_2\right) \\ \dot{z}_1 = x_1 y_1 - \varepsilon z_1 \\ \dot{x}_2 = \sigma\left(y_2 - x_2\right) \\ \dot{y}_2 = \rho x_2 - y_2 - x_2 z_2 + k_2\left(x_1 - y_1\right) \\ \dot{z}_2 = x_2 y_2 - \varepsilon z_2 \end{cases} \tag{21}$$

where σ, ρ and ε are positive control parameters, k_1 and k_2 are coupling parameters [4]. When parameters are set as $\sigma = 10, \rho = 28, \varepsilon = 8/3$, $k_1 = k_2 = 0.05$, the behavior of system (21) is hyper-chaotic. In this stage, we use system (21) to generate key sequences to control quantum XOR operation.

First, coupled hyper-chaotic Lorenz system (21) is iterated with initial values $x_1(0)$, $y_1(0)$, $z_1(0)$, $x_2(0)$, $y_2(0)$, $z_2(0)$ for $N = 2^{2n+3}$ times. When the iterating times satisfy $t_1 = N/4$, $t_2 = 2N/4$ and $t_3 = 3N/4$, $\Delta x_1 = 0.001$ is injected into $x_1(t_1)$, $x_1(t_2)$ and $x_1(t_3)$, respectively. Six sequences $\left\{x_1(0), \ldots, x_1\left(2^{2n+3}-1\right)\right\}$, $\left\{y_1(0), \ldots, y_1\left(2^{2n+3}-1\right)\right\}$, $\left\{z_1(0), \ldots, z_1\left(2^{2n+3}-1\right)\right\}$, $\left\{x_2(0), \ldots, x_2\left(2^{2n+3}-1\right)\right\}$, $\left\{y_2(0), \ldots, y_2\left(2^{2n+3}-1\right)\right\}$ and $\left\{z_2(0), \ldots, z_2\left(2^{2n+3}-1\right)\right\}$ can be generated. Then they are calculated as follows

$$\begin{aligned} \left|T_i^j\right\rangle &= \left|T_{sku}^j\right\rangle = \left|floor\left(x_j(i) \times 10^{14}\right) \bmod 2\right\rangle \\ \left|V_i^j\right\rangle &= \left|V_{sku}^j\right\rangle = \left|floor\left(y_j(i) \times 10^{14}\right) \bmod 2\right\rangle \\ \left|W_i^j\right\rangle &= \left|W_{sku}^j\right\rangle = \left|floor\left(z_j(i) \times 10^{14}\right) \bmod 2\right\rangle \end{aligned} \tag{22}$$

where, $j = 1, 2$, $i = 0, 1, \cdots, 2^{2n+3}-1$, $s = 0, 1, \cdots, 7$, $k, u = 0, 1, \cdots, 2^{2n}-1$ and $floor(\cdot)$ stands for the rounding operation. Obviously, $\left|T_i^j\right\rangle, \left|V_i^j\right\rangle, \left|W_i^j\right\rangle \in \{|0\rangle, |1\rangle\}$.

Quantum XOR operation U_{XOR} can be constructed as

$$U_{XOR} = \prod_{L=0}^{2^3-1}\prod_{Y=0}^{2^n-1}\prod_{X=0}^{2^n-1}\left(I^{\otimes 6} \otimes \sum_{s=0}^{2^3-1}\sum_{k=0}^{2^n-1}\sum_{u=0,sku\neq LYX}^{2^n-1} |s\rangle|ku\rangle\langle ku|\langle s| + \Gamma_{LYX} \otimes |L\rangle|YX\rangle\langle YX|\langle L|\right) \tag{23}$$

where quantum operation $\Gamma_{LYX} = \Gamma_{LYX}^{R_1} \otimes \Gamma_{LYX}^{G_1} \otimes \Gamma_{LYX}^{B_1} \otimes \Gamma_{LYX}^{R_2} \otimes \Gamma_{LYX}^{G_2} \otimes \Gamma_{LYX}^{B_2}$ is used to modify the color information of pixel $|YX\rangle$ in bit-plane $|L\rangle$. $\Gamma_{LYX}^{R_1}$, $\Gamma_{LYX}^{G_1}$, $\Gamma_{LYX}^{B_1}$, $\Gamma_{LYX}^{R_2}$, $\Gamma_{LYX}^{G_2}$, $\Gamma_{LYX}^{B_2}$ are quantum oracles and the corresponding functions can be described as below

$$\begin{aligned} \Gamma_{LYX}^{R_1} &: \left|R'^1_{LYX}\right\rangle \rightarrow \left|R'^1_{LYX} \oplus T^1_{LYX}\right\rangle \\ \Gamma_{LYX}^{G_1} &: \left|G'^1_{LYX}\right\rangle \rightarrow \left|G'^1_{LYX} \oplus V^1_{LYX}\right\rangle \\ \Gamma_{LYX}^{B_1} &: \left|B'^1_{LYX}\right\rangle \rightarrow \left|B'^1_{LYX} \oplus W^1_{LYX}\right\rangle \\ \Gamma_{LYX}^{R_2} &: \left|R'^2_{LYX}\right\rangle \rightarrow \left|R'^2_{LYX} \oplus T^2_{LYX}\right\rangle \\ \Gamma_{LYX}^{G_2} &: \left|G'^2_{LYX}\right\rangle \rightarrow \left|G'^2_{LYX} \oplus V^2_{LYX}\right\rangle \\ \Gamma_{LYX}^{B_2} &: \left|B'^2_{LYX}\right\rangle \rightarrow \left|B'^2_{LYX} \oplus W^2_{LYX}\right\rangle \end{aligned} \tag{24}$$

By applying U_{XOR} to $\left|E'\right\rangle$, the final encrypted image $|E\rangle$ can be obtained

$$\begin{aligned}|E\rangle &= U_{XOR}\left|E'\right\rangle \\ &= \prod_{L=0}^{2^3-1}\prod_{Y=0}^{2^n-1}\prod_{X=0}^{2^n-1}\left(I^{\otimes 6}\otimes\sum_{s=0}^{2^3-1}\sum_{k=0}^{2^n-1}\sum_{u=0,sku\neq LYX}^{2^n-1}|s\rangle|ku\rangle\langle ku|\langle s|+\Gamma_{LYX}\otimes|L\rangle|YX\rangle\langle YX|\langle L|\right)\left|E'\right\rangle \\ &= \frac{1}{\sqrt{2^{2n+3}}}\sum_{L=0}^{2^3-1}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\left|R''^1_{LYX}G''^1_{LYX}B''^1_{LYX}R''^2_{LYX}G''^2_{LYX}B''^2_{LYX}\right\rangle\otimes\left|L'\right\rangle\otimes|YX\rangle\end{aligned} \tag{25}$$

where $\left|R''^1_{LYX}\right\rangle = \left|R'^1_{LYX}\oplus T^1_{LYX}\right\rangle$, $\left|G''^1_{LYX}\right\rangle = \left|G'^1_{LYX}\oplus V^1_{LYX}\right\rangle$, $\left|B''^1_{LYX}\right\rangle = \left|B'^1_{LYX}\oplus W^1_{LYX}\right\rangle$, $\left|R''^2_{LYX}\right\rangle = \left|R'^2_{LYX}\oplus T^2_{LYX}\right\rangle$, $\left|G''^2_{LYX}\right\rangle = \left|G'^2_{LYX}\oplus V^2_{LYX}\right\rangle$, $\left|B''^2_{LYX}\right\rangle = \left|B'^2_{LYX}\oplus W^2_{LYX}\right\rangle$.

4.2 Double quantum color images decryption scheme

The decryption scheme can be described as follows.

Step 1. $\left\{\left|T_i^1\right\rangle\right\}$, $\left\{\left|V_i^1\right\rangle\right\}$, $\left\{\left|W_i^1\right\rangle\right\}$, $\left\{\left|T_i^2\right\rangle\right\}$, $\left\{\left|V_i^2\right\rangle\right\}$ and $\left\{\left|W_i^2\right\rangle\right\}$ can be generated with initial values $x_1(0), y_1(0), z_1(0), x_2(0), y_2(0), z_2(0)$ according to stage 2 in the encryption scheme, where $i = 0, 1, \cdots, 2^{2n+3}-1$. By applying the quantum XOR operation U_{XOR} which is controlled by $\left\{\left|T_i^1\right\rangle\right\}$, $\left\{\left|V_i^1\right\rangle\right\}$, $\left\{\left|W_i^1\right\rangle\right\}$, $\left\{\left|T_i^2\right\rangle\right\}$, $\left\{\left|V_i^2\right\rangle\right\}$, $\left\{\left|W_i^2\right\rangle\right\}$ to $|E\rangle$, $\left|E'\right\rangle$ can be got.

Step 2. The quantum color inverse transformation U^{-1} is performed on $\left|E'\right\rangle$ and the decrypted DQRCI quantum stage image can be obtained.

4.3 Validity verification

The validity verification of quantum image encryption system is to determine whether the decrypted quantum state image is the same as original quantum state image. If consistent, the system is valid, otherwise, the system is invalid. Unfortunately, none of the previous relevant literatures on quantum image encryption has dealt with this in theory.

First, we review the quantum equal (QE) [38], which is used to compare two numbers $|P\rangle = |p_{m-1}\cdots p_1 p_0\rangle$ and $|Q\rangle = |q_{m-1}\cdots q_1 q_0\rangle$ to find out whether they are equal or not. Therein, $|p_i\rangle, |q_i\rangle \in \{|0\rangle, |1\rangle\}, i = 0, 1, \cdots, m-1$. The output qubit $|e\rangle$ represents the comparative result. If $|e\rangle = |1\rangle$, $|P\rangle = |Q\rangle$; otherwise, $|P\rangle \neq |Q\rangle$. Figure 13 shows the specific circuit and modularized circuit of QE.

It is assumed that the original DQRCI quantum state image and the corresponding decrypted image are shown in (26) and (27), respectively

$$|D\rangle = \frac{1}{\sqrt{2^{2n+3}}}\sum_{L=0}^{2^3-1}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\left|R^1_{LYX}G^1_{LYX}B^1_{LYX}R^2_{LYX}G^2_{LYX}B^2_{LYX}\right\rangle\otimes|L_2L_1L_0\rangle\otimes|YX\rangle \tag{26}$$

$$\left|D'\right\rangle = \frac{1}{\sqrt{2^{2n+3}}}\sum_{L'=0}^{2^3-1}\sum_{Y'=0}^{2^n-1}\sum_{X'=0}^{2^n-1}\left|R'^1_{L'Y'X'}G'^1_{L'Y'X'}B'^1_{L'Y'X'}R'^2_{L'Y'X'}G'^2_{L'Y'X'}B'^2_{L'Y'X'}\right\rangle\otimes\left|L'_2L'_1L'_0\right\rangle\otimes\left|Y'X'\right\rangle \tag{27}$$

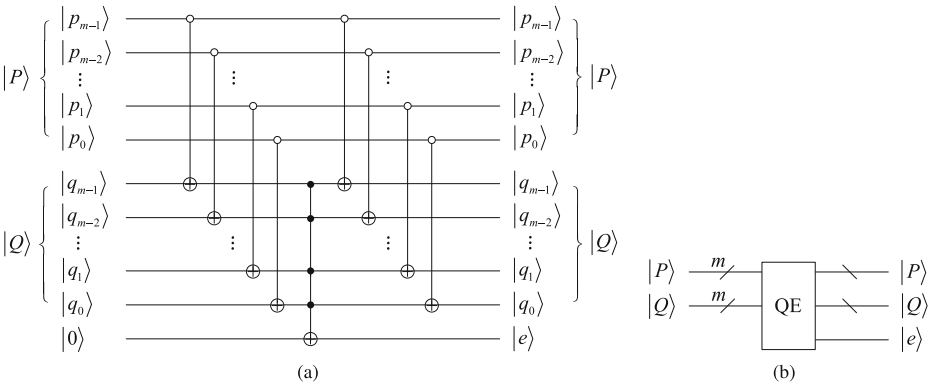


Fig. 13 The quantum realization circuit of QE: **a** Concrete circuit, **b** Modularized circuit

and there is an empty quantum binary image of the same size

$$\left|D''\right\rangle = \frac{1}{2^n} \sum_{Y''=0}^{2^n-1} \sum_{X''=0}^{2^n-1} |0\rangle \otimes \left|Y''X''\right\rangle \tag{28}$$

The quantum circuit of verification process is shown in Fig. 14. The output is

$$|V\rangle = \frac{1}{2^n} \sum_{Y''=0}^{2^n-1} \sum_{X''=0}^{2^n-1} \left|v\left(Y'', X''\right)\right\rangle \otimes \left|Y''X''\right\rangle \tag{29}$$

If for any pixel $\left|Y''X''\right\rangle$, there is $\left|v\left(Y'', X''\right)\right\rangle = |1\rangle$, the encryption system is valid, i.e., the decrypted DQRCI quantum state image is the same as original quantum state image; otherwise, the system is invalid.

5 Numerical simulation and performance comparison

To evaluate our proposed encryption scheme compared with other prior pertinent works, this section gives the simulation analysis. Due to the lack of physical quantum hardware, the simulation is implemented on a classical computer equipped with MATLAB R2016a environment. The quantum states and quantum operations are simulated by complex vectors and unitary matrices, respectively. The keys are set as $x_1\,(0) = 4.175$, $y_1\,(0) = 8.203$, $z_1\,(0) = 1.376$, $x_2\,(0) = 14.362$, $y_2\,(0) = 0.800$, $z_2\,(0) = 2.364$. From Fig. 15, it can be seen that any information of original images cannot be obtained from the encrypted ones which are noise-like. Therefore, the proposed encryption scheme is effective.

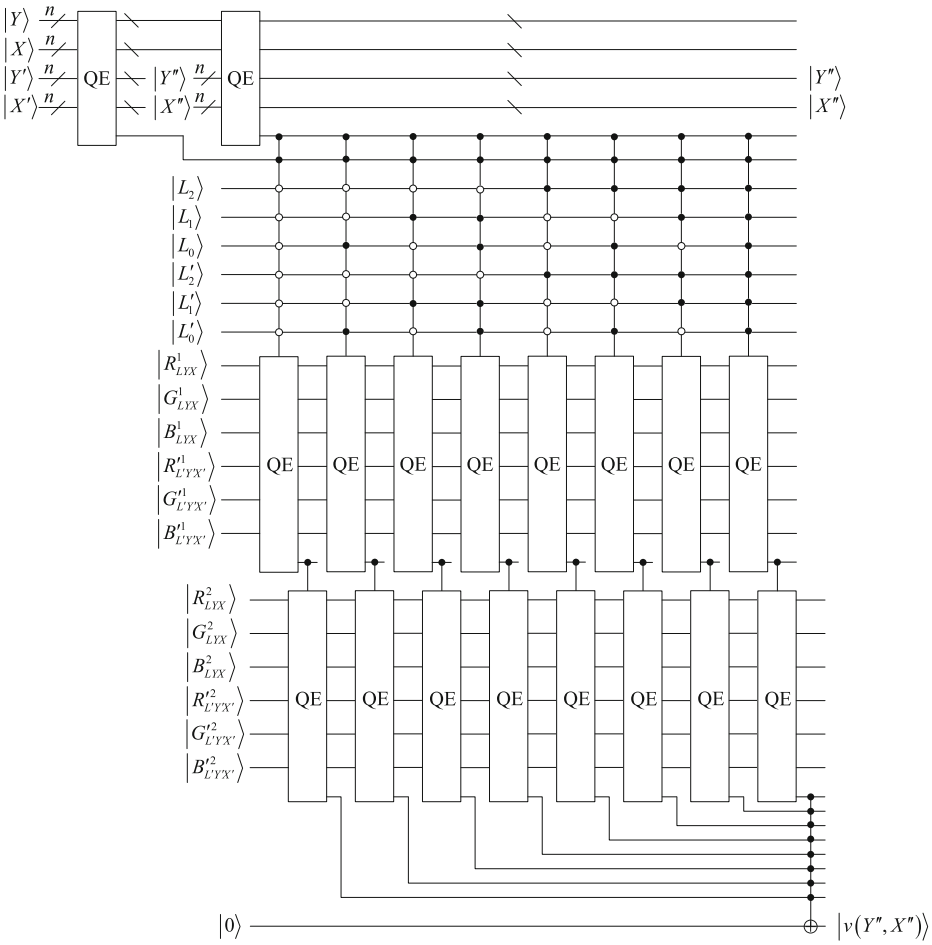


Fig. 14 Quantum circuit for validity verification

5.1 Statistical analysis

5.1.1 Mean square error

Mean square error (MSE) calculated by the following equation can be used to characterize the difference between encrypted image and original one

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (D(i, j) - E(i, j))^2 \tag{30}$$

where $M \times N$ is the size of image, $D(i, j)$ and $E(i, j)$ denote pixel values of pixel (i, j) in original and encrypted image, respectively. The larger the MSE value, the better the security. For images shown in Fig. 15, the MSE values are calculated and listed in Table 1. It shows that the proposed encryption scheme can counteract statistical attack.

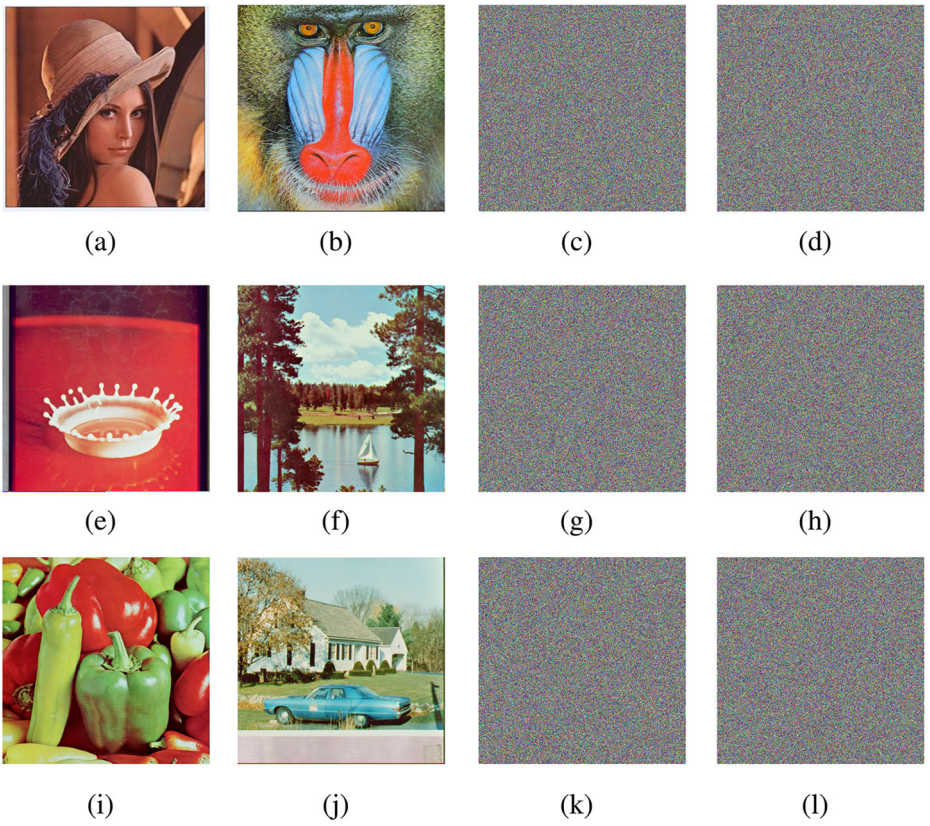


Fig. 15 Three pairs of original color images and the corresponding encrypted ones: **a** Original Lena, **b** Original Baboon, **c** Encrypted Lena, **d** Encrypted Baboon, **e** Original Splash, **f** Original Sailboat, **g** Encrypted Splash, **h** Encrypted Sailboat, **i** Original Peppers, **j** Original House, **k** Encrypted Peppers, **l** Encryped House

5.1.2 Histogram

The histogram of an image reflects the pixel value distribution. Taking Lena and Baboon as examples, the histograms of R, G, B channels before and after encryption are illustrated

Table 1 The MSE values between original color images and the corresponding encrypted ones

Images	R Channel	G Channel	B Channel
Lena	9.117E3	9.810E3	1.068E4
Baboon	8.624E3	7.755E3	9.490E3
Splash	1.136E4	1.234E4	9.940E3
Sailboat	7.311E3	1.149E4	1.150E4
Peppers	8.022E3	1.127E4	1.117E4
House	8.804E3	9.506E3	9.444E3

in Fig. 16. It is shown that the histograms of encrypted images have two remarkable properties: (1) they are totally different from the histograms of original images and (2) their distributions are uniform, which means that the probability of existence of any pixel value is the same. Therefore, the proposed encryption scheme could resist statistical attack and differential attack.

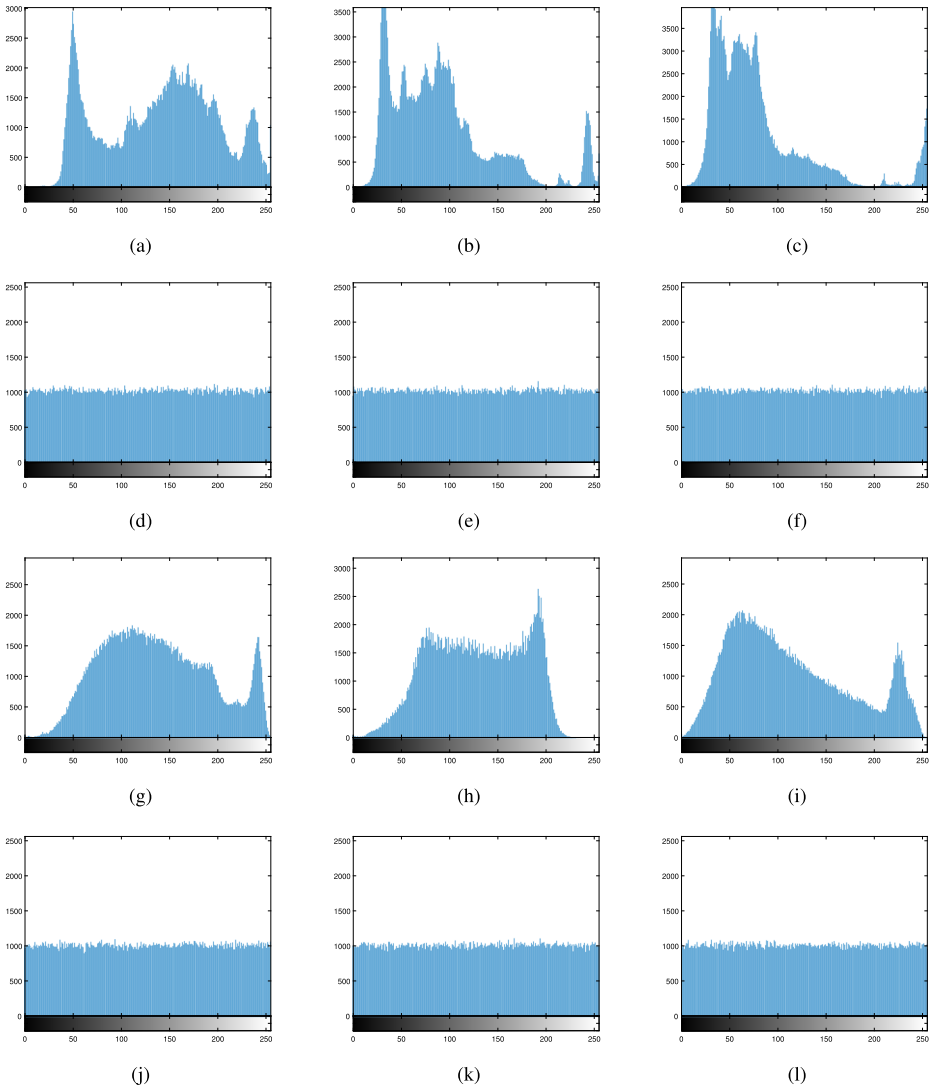


Fig. 16 The histogram distributions: **a** R channel of Lena, **b** G channel of Lena, **c** B channel of Lena, **d** R channel of encrypted Lena, **e** G channel of encrypted Lena, **f** B channel of encrypted Lena, **g** R channel of Baboon, **h** G channel of Baboon, **i** B channel of Baboon, **j** R channel of encrypted Baboon, **k** G channel of encrypted Baboon, **l** B channel of encrypted Baboon

5.1.3 Correlation of adjacent pixels

An ideal encrypted image should have very low correlation in horizontal, vertical and diagonal directions. The degree of correlation can be measured by CC

$$CC = \frac{\sum_{i=1}^{L}\left(x_i - \frac{1}{L}\sum_{i=1}^{L} x_i\right)\left(y_i - \frac{1}{L}\sum_{i=1}^{L} y_i\right)}{\sqrt{\sum_{i=1}^{L}\left(x_i - \frac{1}{L}\sum_{i=1}^{L} x_i\right)^2 \sum_{i=1}^{L}\left(y_i - \frac{1}{L}\sum_{i=1}^{L} y_i\right)^2}} \tag{31}$$

where x_i, y_i stand for the pixel values of two adjacent pixels, respectively, L is the number of adjacent pixels. The correlation is strong when CC is close to 1 or -1. Correspondingly, the correlation is weak when CC is close to 0.

Table 2 lists the CC values of adjacent pixels. It is shown that CC values of encrypted images are close to 0 in all three directions, which means that the encrypted images have an almost random relationship among adjacent pixels. Hence, the proposed encryption scheme is secure against correlation analysis attack.

Table 2 The CC values of original images and encrypted ones

Images	Horizontal direction		Vertical direction		Diagonal direction	
	Original	Encrypted	Original	Encrypted	Original	Encrypted
Lena (R channel)	0.9886	–0.0073	0.9844	0.0041	0.9714	–0.0022
Lena (G channel)	0.9870	–0.0059	0.9797	–0.0012	0.9663	0.0036
Lena (B channel)	0.9846	0.0055	0.9776	0.0025	0.9610	–0.0018
Baboon (R channel)	0.7847	–0.0017	0.8732	–0.0041	0.7578	0.0108
Baboon (G channel)	0.7073	0.0018	0.8373	0.0089	0.6593	0.0048
Baboon (B channel)	0.8483	0.0018	0.8884	–0.0053	0.7890	0.0044
Splash (R channel)	0.9976	–0.0039	0.9848	0.0019	0.9845	–0.0026
Splash (G channel)	0.9896	0.0058	0.9511	0.0056	0.9494	0.0019
Splash (B channel)	0.9892	–0.0020	0.9633	0.0066	0.9616	0.0048
Sailboat (R channel)	0.9129	–0.0068	0.9162	–0.0053	0.8932	0.0053
Sailboat (G channel)	0.9518	0.0028	0.9509	–0.0088	0.9246	–0.0022
Sailboat (B channel)	0.9527	0.0063	0.9458	–0.0029	0.9208	0.0059
Peppers (R channel)	0.9613	0.0032	0.9405	0.0033	0.9345	0.0029
Peppers (G channel)	0.9850	0.0115	0.9769	–0.0038	0.9619	–0.0049
Peppers (B channel)	0.9590	0.0028	0.9556	–0.0054	0.9315	–0.0056
House (R channel)	0.9368	–0.0021	0.9193	0.0056	0.8768	–0.0018
House (G channel)	0.9374	–0.0013	0.8960	0.0052	0.8517	0.0069
House (B channel)	0.9674	–0.0045	0.9598	0.0035	0.9344	–0.0019

5.1.4 Information entropy

Assume an image has Z pixel values z_i $(i = 0, 1, \cdots, Z-1)$. According to Shannon theorem, the corresponding information entropy value IE can be calculated as

$$IE = -\sum_{i=0}^{Z-1} p(z_i) \log_2 p(z_i) \tag{32}$$

where $p(z_i)$ denotes the probability of occurrence of z_i, $\sum_{i=0}^{Z-1} p(z_i) = 1$. The ideal IE of an encrypted image is 8 bits. The closer the IE is to 8, the better the system is to resist entropy attack. Table 3 lists the IE values of images shown in Fig. 15. Obviously, the IE values of encrypted images are very close to 8 bits. Thus, the proposed encryption scheme can frustrate entropy attack.

5.1.5 Spatial frequency

The spatial frequency (SF) of an image reflects its overall activity in the spatial domain [25]. SF can be calculated as

$$SF = \sqrt{(RF)^2 + (CF)^2} \tag{33}$$

where RF and CF denote the row frequency and column frequency of the image, respectively. RF and CF are defined as follows

$$RF = \sqrt{\frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} [K(i, j) - K(i, j-1)]^2} \tag{34}$$

$$CF = \sqrt{\frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} [K(i, j) - K(i-1, j)]^2} \tag{35}$$

where $M \times N$ is the size of image, $K(i, j)$ represents the pixel value of position (i, j). RF and CF reflect the changes of horizontal and vertical directions in the image, respectively. Table 4 lists the RF, CF and SF values of images shown in Fig. 15. It can be seen that the SF values of encrypted images are almost 5 times the values of original ones. Therefore, the encrypted images have good randomness.

Table 3 The IE values of original images and encrypted ones

Images	Original			Encrypted		
	R channel	G channel	B channel	R channel	G channel	B channel
Lena	7.6503	7.3053	7.0746	7.9993	7.9993	7.9994
Baboon	7.7067	7.4744	7.7522	7.9992	7.9993	7.9994
Splash	6.9481	6.8845	6.1265	7.9992	7.9994	7.9993
Sailboat	7.3124	7.6429	7.2136	7.9994	7.9993	7.9992
Peppers	7.3388	7.4963	7.0583	7.9993	7.9993	7.9992
House	7.4156	7.2295	7.4354	7.9992	7.9994	7.9993

Table 4 The RF, CF and SF values of original images and encrypted ones

Images	Original			Encrypted		
	RF	CF	SF	RF	CF	SF
Lena (R channel)	9.2123	8.3342	12.4228	104.2119	104.1662	147.3456
Lena (G channel)	9.4301	8.5914	12.7569	104.3760	104.4719	147.6778
Lena (B channel)	9.4774	8.7249	12.8820	104.5566	104.5085	147.8313
Baboon (R channel)	21.7618	28.6594	35.9852	104.4863	104.3843	147.6939
Baboon (G channel)	24.7664	32.6431	40.9749	104.3879	104.3269	147.5836
Baboon (B channel)	26.5479	30.0674	40.1104	104.4132	104.4993	147.7235
Splash (R channel)	6.7573	5.8971	8.9687	104.3514	104.1910	147.4617
Splash (G channel)	11.7004	9.6653	15.1762	104.3237	104.4239	147.6069
Splash (B channel)	8.7217	9.5670	12.9459	104.3651	104.3841	147.6080
Sailboat (R channel)	12.7161	12.9580	18.1551	104.5793	104.3632	147.7447
Sailboat (G channel)	18.5109	20.1373	27.3526	104.4244	104.4301	147.6824
Sailboat (B channel)	18.4664	19.0139	26.5054	104.2486	104.4522	147.5738
Peppers (R channel)	12.1888	11.7168	16.9071	104.4134	104.5980	147.7935
Peppers (G channel)	14.5613	14.3069	20.4137	104.4729	104.3983	147.6942
Peppers (B channel)	11.4430	11.4449	16.1842	104.7140	104.7264	147.0967
House (R channel)	15.3398	14.6298	21.1977	104.2923	104.3230	147.5133
House (G channel)	16.8727	16.4644	23.5746	104.5702	104.5057	147.8390
House (B channel)	14.3658	15.3465	21.0212	104.3500	104.3588	147.5795

5.2 Key security analysis

5.2.1 Key sensitivity analysis

For an ideal image encryption algorithm, the keys should be sensitive enough to counteract brute-force attack. The sensitivity performance of proposed encryption system can be evaluated by changing one of the correct keys slightly, while the other keys remain untouched. To analyze the key sensitivity, six groups of incorrect keys are utilized to decrypt the encrypted images. Figures 17a–f depict the decryptd images with incorrect keys $x_1\,(0) + 10^{-14}$, $y_1\,(0) + 10^{-14}$, $z_1\,(0) + 10^{-14}$, $x_2\,(0) + 10^{-14}$, $y_2\,(0) + 10^{-14}$ and $z_2\,(0) + 10^{-14}$, respectively, while the other keys are all right. From Fig. 17, it is easy to find that a very little deviation from correct keys will result in an apparent distortion of the decrypted image. Thus, the proposed encryption scheme is very sensitive to keys.

5.2.2 Key space analysis

Under current computation ability, the key space of an ideal image encryption scheme should larger than 2^{100} to resist brute-force attack [33]. In our encryption scheme, the keys are six initial values of coupled hyper-chaotic Lorenz system, i.e., $x_1\,(0)$, $y_1\,(0)$, $z_1\,(0)$, $x_2\,(0)$, $y_2\,(0)$, $z_2\,(0)$. Hence, the key space is about $S = 10^{14} \times 10^{14} \times 10^{14} \times 10^{14} \times 10^{14} \times 10^{14} = 10^{84} \approx 2^{279} \gg 2^{100}$, which is large enough to counteract the brute-force attack.

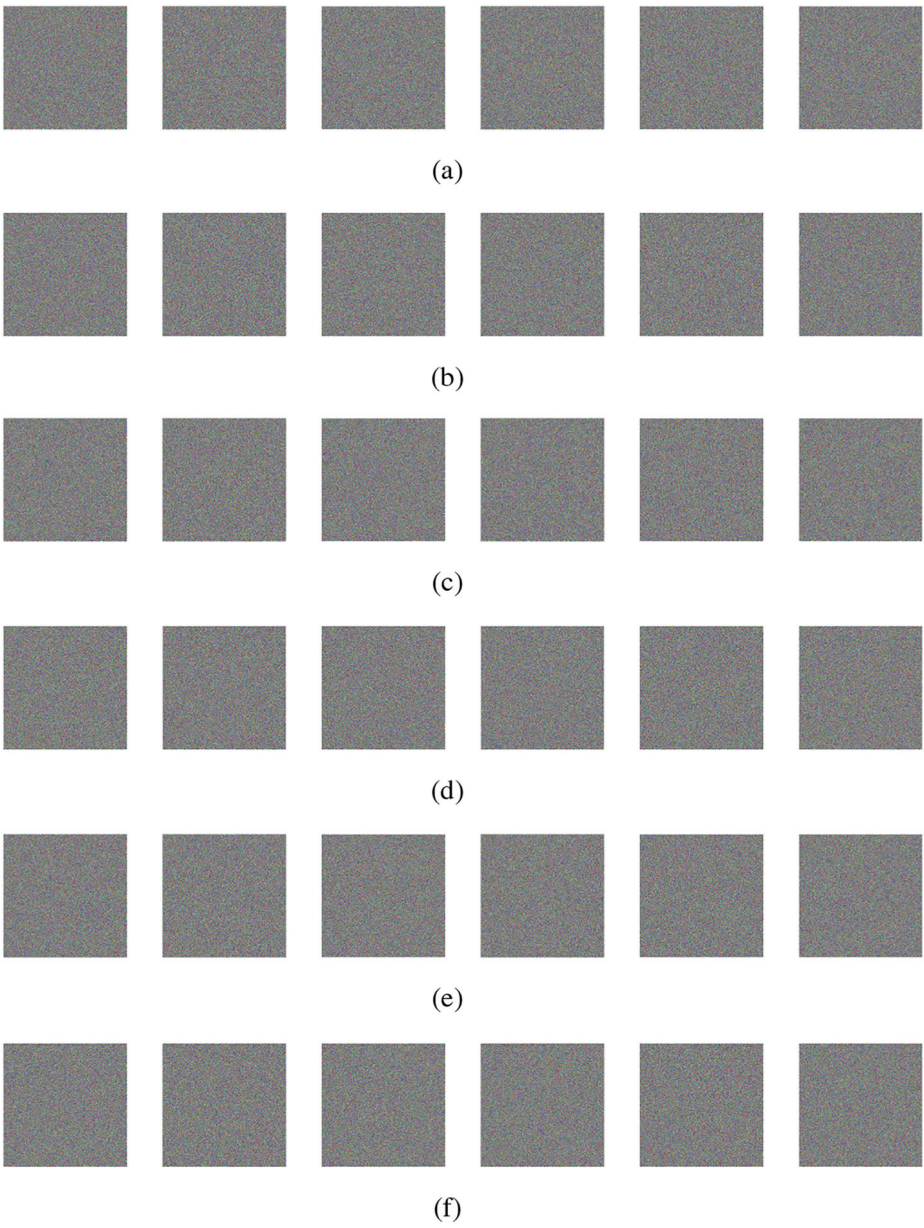


Fig. 17 Decrypted images with: **a** incorrect key $x_1\ (0)+10^{-14}$, **b** incorrect key $y_1\ (0)+10^{-14}$, **c** incorrect key $z_1\ (0)+10^{-14}$, **d** incorrect key $x_2\ (0)+10^{-14}$, **e** incorrect key $y_2\ (0)+10^{-14}$, **f** incorrect key $z_2\ (0)+10^{-14}$

5.3 Computational complexity analysis

There is no doubt that computational complexity is an essential criterion for assessing a quantum image encryption scheme. Therefore, in this subsection, the computational complexity of proposed double quantum color images encryption scheme is discussed. In our

encryption scheme, the computational complexity depends on quantum color transformation and quantum XOR operation. CNOT gate is chosen as the basic quantum gate. Ref. [19] shows the computational complexity of CNOT gate is far exceed the complexity of NOT gate, so we assume NOT gate has a computational complexity of δ ($\delta \ll 1$). The color transformation encompasses 9 NOT gates and 2 swap gates. It is known that one swap gate can be broken down into three CNOT gates [39]. So the computational complexity of color transformation is $(6 + 9\delta)$. According to the parallel characteristics of quantum computation, the corresponding computational complexity of XOR operation could be evaluated via the computational complexity of quantum operation Γ_{LYX} which is composed of six $(2n + 3)$-CNOT gates. n-CNOT gate can be constructed by $(4n - 8)$ 2-CNOT gates and 6 CNOT gates are involved in realizing the 2-CNOT gate [24]. Therefore, Γ_{LYX} can be realized by $(288n + 144)$ basic gates. In other words, the computational complexity of quantum XOR operation is $(288n + 144)$. Thus, the total computational complexity of proposed encryption scheme is $(288n + 150 + 9\delta)$.

5.4 Performance comparison

This subsection compares our encryption scheme with the previous pertinent work put forward by Liu et al. [13]. The comparison consequences include the following aspects.

5.4.1 Key space comparison

The Liu's algorithm in Ref. [13] uses quantum Arnold transform (QAT) to scramble pixel positions and the gray information is changed by utilizing qubit random rotation. According to the analysis in Ref. [13], the key space of QAT is about 2^{15} and the key space of random rotation matrix which depends on the image size is larger than $2^{256\times256}$. Therefore, the total key space is more than $2^{256\times256+15}$, which means their algorithm has a larger key space compared to what we investigated. However, under current computation ability, our key space is still large enough to resist brute-force attack. Despite this, our proposed encryption system is much reliable and outperform than theirs, as can be seen in the following parts.

5.4.2 Histogram comparison

Generally, the flatter the histogram of encrypted image and the fewer peaks appear in the histogram, the higher the security of image encryption algorithm. Figure 18 plots the histograms of original images and the corresponding encrypted ones by using the algorithm put forward in Ref. [13]. Obviously, the histograms of original images are different from each other, while the histograms of encrypted ones are similar. However, from the comparison between Figs. 16 and 18. it can be seen that the histograms of encrypted images with our scheme have more uniform distributions. Thus, our proposed double quantum color images encryption scheme is more efficient and applicable.

5.4.3 Correlation coefficient comparison

In this part of research, as regards the performance of correlation coefficient, our proposed encryption scheme is compared with the algorithm in Ref. [13]. It can be perceived from Tables 2 and 5 that the CC values of encrypted images are relatively smaller with our scheme. That is to say, our proposed double quantum color images encryption scheme has a stronger ability to cancel the correlation of adjacent pixels.

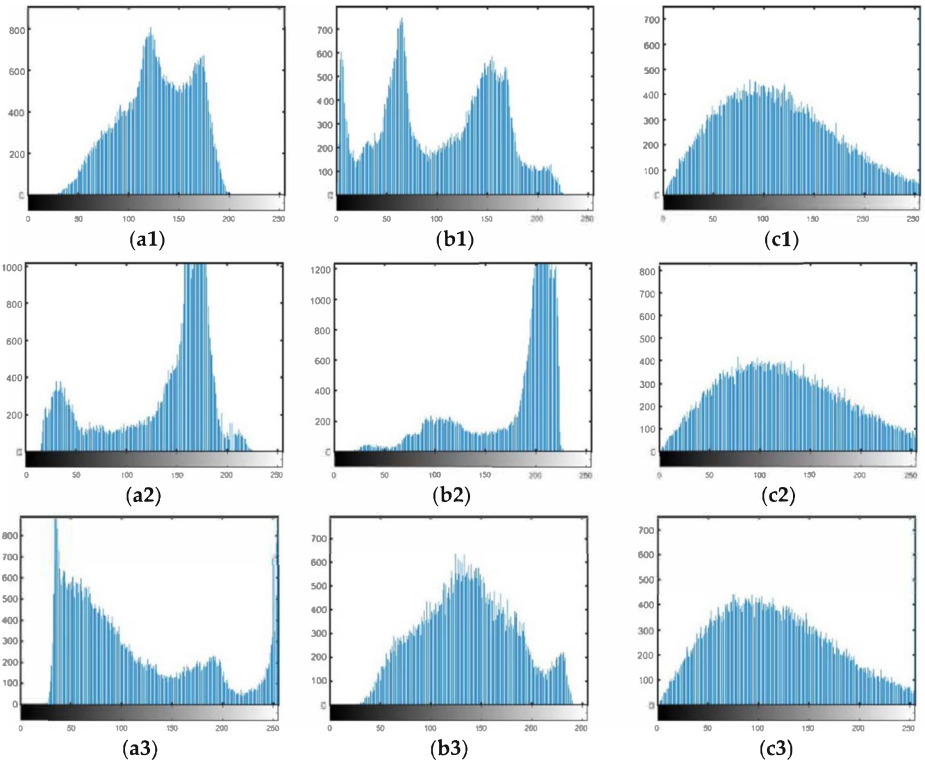


Fig. 18 The histograms of original images and cipher images by using algorithm put forward in Ref. [13]. (Figure adapted from [13])

5.4.4 Information entropy comparison

As mentioned previously, an image encryption algorithm is reliable iff the information entropy value of encrypted image is close to ideal value, i.e., 8 bits, to counteract the entropy attack. The calculated IE values by using the algorithm in Ref. [13] are listed in Table 6. It can be seen from Tables 3 and 6 that the information entropy values of encrypted images

Table 5 The CC values by using the algorithm put forward in Ref. [13]

Images	Horizontal direction		Vertical direction		Diagonal direction	
	Original	Encrypted	Original	Encrypted	Original	Encrypted
Figure 2(a1) [13]	0.5720	–0.0368	0.6781	–0.0111	0.5722	0.0135
Figure 2(b1) [13]	0.9557		0.9231		0.8861	
Figure 2(a2) [13]	0.8702	–0.0351	0.6628	0.0396	0.6315	–0.0260
Figure 2(b2) [13]	0.9045		0.9315		0.8633	
Figure 2(a3) [13]	0.9939	0.0004	0.9859	–0.0121	0.9791	0.0128
Figure 2(b3) [13]	0.9548		0.9565		0.9079	

Table 6 The IE values by using the algorithm put forward in Ref. [13]

Images	Original	Encrypted
Figure 2(a1) [13]	7.1273	7.7459
Figure 2(b1) [13]	7.5693	
Figure 2(a2) [13]	7.1208	7.7289
Figure 2(b2) [13]	6.7040	
Figure 2(a3) [13]	7.4457	7.7578
Figure 2(b3) [13]	7.5046	

are relatively larger with our scheme. In other words, our proposed double quantum color images encryption scheme is more stable and secure against entropy attack.

5.4.5 Computational complexity comparison

The computational complexity is compared in this part. As analyzed in the previous subsection, the total computational complexity of our proposed encryption scheme is $O(n)$. According to the discussion in Ref. [13], the image encryption algorithm consists of five steps and the overall complexity is $O\left(n^2\right)$, which is more complex than our scheme. Hence, we can give the conclusion that our proposed double quantum color images encryption scheme can reach a quadratic speedup than the algorithm in Ref. [13].

6 Conclusion

In this paper, in order to store and process two color images in quantum computer simultaneously, a double quantum color images representation model, i.e., DQRCI, is newly investigated. In DQRCI, the color information of two images is stored into the first qubit sequence, while the bit-plane information and position information are stored into the second and third qubit sequences, respectively. Besides, some simple DQRCI-based image processing operations are discussed and the corresponding quantum circuits are designed, which indicate that these operations have very low computational complexity based on DQRCI. Furthermore, to ensure the security of DQRCI quantum state image, an encryption scheme is proposed. Owing to DQRCI model exploits the basis states of qubit sequences to encode color information, two classical original color images can be retrieved accurately from the encrypted DQRCI image through using correct keys. By utilizing quantum computation, the validity verification of proposed encryption system in theory is given. Numerical simulation and performance comparison show that the proposed double quantum color images encryption scheme is secure against statistical attack and brute-force attack. Moreover, our quantum image encryption scheme is superior compared with the previous pertinent work in terms of security and computational complexity. Quantum image encryption is the simplest and most efficient approach for protecting quantum image information. In the future, we will try our best to design more effective quantum image representation model, processing algorithm and encryption scheme.

Acknowledgements This work was supported by the program of excellent team in Harbin Institute of Technology.

References

1. Feynman RP (1982) Simulating physics with computers. Int J Theor Phys 21(6/7):467–488
2. Fijany A, Williams CP (1998) Quantum wavelet transform: fast algorithm and complete circuits. arXiv:quantph/9809004
3. Gong LH, He XT, Cheng S, Hua TX, Zhou NR (2016) Quantum image encryption algorithm based on quantum image XOR operations. Int J Theor Phys 55(7):3234–3250
4. Grassi G, Severance FL, Miller DA (2009) Multi-wing hyperchaotic attractors from coupled Lorenz systems. Chaos Soliton Fract 41(1):284–291
5. Grover L (1996) A fast quantum mechanical algorithm for database search. In: Proceedings of the 28th annual ACM symposium theory of computing, pp 212–219
6. Hua TX, Chen J, Pei DJ, Zhang WQ, Zhou NR (2015) Quantum image encryption algorithm based on image correlation decomposition. Int J Theor Phys 54(2):526–537
7. Jiang N, Wang J, Mu Y (2015) Quantum image scaling up based on nearest-neighbor interpolation with integer scaling ratio. Quantum Inf Process 14(11):4001–4026
8. Latorre J (2005) Image compression and entanglement. arXiv:quant-ph/0510031
9. Le PQ, Dong F, Hirota K (2011) A flexible representation of quantum images for polynomial preparation, image compression and processing operations. Quantum Inf Process 10(1):63–84
10. Li P, Zhao Y (2017) A simple encryption algorithm for quantum color image. Int J Theor Phys 56(6):1961–1982
11. Liang H, Tao X, Zhou N (2016) Quantum image encryption based on generalized affine transform and logistic map. Quantum Inf Process 15(7):2701–2724
12. Liu K, Zhang Y, Lu K et al (2018) An optimized quantum representation for color digital images. Int J Theor Phys 57(10):2938–2948
13. Liu X, Xiao D, Liu C (2018) Double quantum image encryption based on Arnold transform and qubit random rotation. Entropy 20(11):867
14. Nielsen MA, Chuang IL (2000) Quantum computation and quantum information. Cambridge University Press
15. Ran QW, Wang L, Ma J, Tan LY, Yu SY (2018) A quantum color image encryption scheme based on coupled hyper-chaotic Lorenz system with three impulse injections. Quantum Inf Process 17(8):188
16. Sang J, Wang S, Shi X et al (2016) Quantum realization of Arnold scrambling for IFRQI. Int J Theor Phys 55(8):3706–3721
17. Sang JZ, Wang S, Li Q (2016) A novel quantum representation of color digital images. Quantum Inf Process 16(2):42
18. Shor P (1994) Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings of the 35th annual symposium on foundations of computer science, pp 124–134
19. Smolin JA, DiVincenzo DP (1996) Five two-bit quantum gates are sufficient to implement the quantum Fredkin gate. Phy Rev A 53(4):2855–2856
20. Sun B, Iliyasu AM, Yan F, Dong FY, Hirota K (2013) An RGB multi-channel representation for images on quantum computers. J Adv Comput Intell Intell Inf 17(3):404–417
21. Tan RC, Lei T, Zhao QM et al (2016) Quantum color image encryption algorithm based on a hyper-chaotic system and quantum Fourier transform. Int J Theor Phys 55(12):5368–5384
22. Venegas-Andraca S, Ball J (2010) Processing images in entangled quantum systems. Quantum Inf Process 9(1):1–11
23. Venegas-Andraca S, Bose S (2003) Storing, processing, and retrieving an image using quantum mechanics. Quantum Inf Compu 5105(8):134–147
24. Vlatko V, Adriano B, Artur E (1996) Quantum networks for elementary arithmetic operations. Phys Rev A 54(1):147–153
25. Wang J, Geng YC, Han L, Liu JQ (2018) Quantum image encryption algorithm based on quantum key image. Int J Theor Phys 58(1):308–322
26. Wang L, Ran Q, Ma J, Yu S, Tan L (2019) QRCI: a new quantum representation model of color digital images. Opt Commun 438:147–158
27. Yan F, Iliyasu AM, Jiang Z (2014) Quantum computation-based image representation, processing operations and their applications. Entropy 16(10):5290–5338
28. Yan F, Iliyasu AM, Le PQ (2017) Quantum image processing: a review of advances in its security technologies. Int J Quantum Inf 15(03):1730001
29. Yang YG, Xia J, Jia X, Zhang H (2013) Novel image encryption/decryption based on quantum Fourier transform and double phase encoding. Quantum Inf Process 12(11):3477–3493

30. Yang YG, Sun SJ et al (2014) Quantum cryptographic algorithm for color images using quantum Fourier transform and double random-phase encoding. Inform Sciences 277(2):445–457
31. Yang YG, Pan QX, Sun SJ, Xu P (2015) Novel image encryption based on quantum walks. Sci Rep-UK 5:7784
32. Yang YG, Tian J, Lei H et al (2016) Novel quantum image encryption using one-dimensional quantum cellular automata. Inform Sci 345:257–270
33. Yap WS, Phan RCW, Goi BM et al (2016) On the effective subkey space of some image encryption algorithms using external key. J Vis Commun Image R 40:51–57
34. Zhang Y, Lu K, Gao YH, Wang M (2013) NEQR: a novel enhanced quantum representation of digital images. Quantum Inf Process 12(8):2833–2860
35. Zhang Y, Lu K, Gao YH, Xu K (2013) A novel quantum representation for log-polar images. Quantum Inf Process 12(9):3103–3126
36. Zhou R, Wu Q, Zhang M et al (2013) Quantum image encryption and decryption algorithms based on quantum image geometric transformations. Int J Theor Phys 52(6):1802–1817
37. Zhou NR, Hua TX, Gong LH et al (2015) Quantum image encryption based on generalized Arnold transform and double random-phase encoding. Quantum Inf Process 14(4):1193–1213
38. Zhou RG, Hu W, Fan P (2017) Quantum watermarking scheme through Arnold scrambling and LSB steganography. Quantum Inf Process 16(9):212
39. Zhou NR, Chen WW, Yan XY, Wang YQ (2018) Bit-level quantum color image encryption scheme with quantum cross-exchange operation and hyper-chaotic system. Quantum Inf Process 17:1–24

Ling Wang, a Ph.D. candidate in National Key Laboratory of Tunable Laser Technology, Harbin Institute of Technology. Her research interests include quantum image representation, quantum image encryption and quantum steganography.

Qiwen Ran, Professor and Ph.D. supervisor in physical electronics, Harbin Institute of Technology. His research interests include wavelet theory, satellite laser communication, information optics, applied mathematics and quantum image processing

Jing Ma, Professor and Ph.D. supervisor in physical electronics, Harbin Institute of Technology. His research interests include satellite laser communication, laser interferometry, optical information processing and laser holography.