Int J Theor Phys (2016) 55:5368–5384
DOI 10.1007/s10773-016-3157-x

Quantum Color Image Encryption Algorithm Based on A Hyper-Chaotic System and Quantum Fourier Transform

Ru-Chao Tan[1] · Tong Lei[2] · Qing-Min Zhao[1] · Li-Hua Gong[1,3] · Zhi-Hong Zhou[3]

Received: 27 May 2016 / Accepted: 30 August 2016 / Published online: 12 September 2016

Abstract To improve the slow processing speed of the classical image encryption algorithms and enhance the security of the private color images, a new quantum color image encryption algorithm based on a hyper-chaotic system is proposed, in which the sequences generated by the Chen's hyper-chaotic system are scrambled and diffused with three components of the original color image. Sequentially, the quantum Fourier transform is exploited to fulfill the encryption. Numerical simulations show that the presented quantum color image encryption algorithm possesses large key space to resist illegal attacks, sensitive dependence on initial keys, uniform distribution of gray values for the encrypted image and weak correlation between two adjacent pixels in the cipher-image.

Keywords Hyper-chaotic system · Quantum Fourier transform · Quantum color image encryption

1 Introduction

In recent years, information security has received more and more concerns, and a variety of digital image encryption methods have been widely applied in secure validation systems [1, 2]. Chaotic cryptosystems commonly have super-speed with low costs, which makes

✉ Li-Hua Gong
lhgong@ncu.edu.cn; ncuglh@163.com

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

[2] 14 Base Class, School of Mathematics, Shandong University, Ji'nan 250100, China

[3] Shanghai Key Laboratory of Integrate Administration Technologies for Information Security, Shanghai Jiao Tong University, Shanghai 200240, China

them to be better candidates than many other classical encryption algorithms for multimedia data [3]. In 1989, Matthews firstly presented the chaos-based encryption algorithm [4], and Fridrich firstly introduced chaotic systems into image encryption in 1998 by designing substitution and diffusion in the spatial domain [5]. The interrelated correlation between cryptography and chaos was investigated [6]. Patidar et al. proposed a color image encryption algorithm based on substitution-diffusion framework by adopting chaotic standards and logistic maps [7]. In particular, logistic map was universally used in the field of image encryption [8], though it is not secure enough to use one-dimensional chaotic map merely due to the small key space [9]. Subsequently, a hyper-chaotic system with unfixed parameters for image encryption was investigated [10]. Because of the unique characteristics of the chaotic system, such as high sensitivity, topological transitivity, non-periodicity and pseudo-randomness, the image encryption mechanisms based on hyper-chaotic system have been discussed frequently and a battery of chaos-based image encryption schemes have been proposed [11–13].

With the rapid development of network technology, internet-based multimedia communication is of increasing importance. In accordance with random classical computations, M data needs M steps of loading operations for a single processor [14], which reduces the computational efficiency and results in the bottleneck of classical computers. Nowadays, quantum computation is becoming a potentially important and effective tool to meet the high real-time computational requirements [15, 16]. Based on the principles of quantum physics, Feynman presented a computation model named quantum computers, which seems more powerful than classical ones [17]. Shor's polynomial time scheme for factoring integers and Grover's database searching algorithm have indicated the power of future quantum computers [18]. Additionally, quantum image processing extending classical image processing applications into a quantum computer is a novel and infusive subject among quantum computation. The image color and position could be encoded into one quantum state by a flexible representation of quantum image (FRQI) [19], which keeps the classical properties of color and position. The real ket model was performed on image quartering iteratively and a balanced quad-tree index was built [20], where each pixel was mapped into a basis state of a four-dimensional qubit sequence. The qubit lattice model [21, 22] allows people to store information without preprocessing with three primary colors, i.e., Red, Green and Blue. Some classical frequency domain transformations have been extended into their quantum versions, for example, quantum Fourier transform (QFT) [16]. Undoubtedly, QFT would play a vital role in quantum computation [23–25]. However, there is another kind of transforms, which are shown to be a powerful tool in developing quantum algorithms [26, 27]. Due to the quantum chaotic systems could be characterized by the sensitive dependence on initial values, a new color image encryption algorithm based on quantum chaotic system was presented [28]. In 2014, Yang et al. proposed a quantum cryptographic algorithm for color images by combining quantum Fourier transform with double random-phase encoding [29].

However, some of the presented chaos-based image encryption schemes suffer security threats [30, 31], such as the way of generating the key stream, relatively small key space, the required round of encryption times (the trade off between security and the overall performance), and etc. Quantum networks, emerging as a branch of quantum physics to understand the features of quantum information, have some advantages in breaking the classical computing limits [32]. In particular, quantum image encryption technology has unique characteristics, such as large capacity, high processing speed, high robustness, natural parallelism and high security. The security of the most classical cryptosystems is founded on

the supposition of computational complexity and might be susceptible to the strong ability of quantum computation [33]. In this paper, through the combination of hyper chaotic systems and quantum image encryption technology, it can be seen from the simulation that the advantages of quantum image encryption is apparently in overcoming the shortcomings of chaos due to the enlarged key space, the accelerated processing speed, the improved security. Therefore, more and more security algorithms, including quantum image encryption algorithms, were devised based on quantum information and quantum computation [16].

The rest of this paper is arranged as follows. In Section 2, quantum representation for color images and the Chen's hyper-chaotic system are related. A color image encryption scheme is designed in Section 3 while the security analyses are given in Section 4. Finally, a brief conclusion is drawn in Section 5.

2 Quantum Image Representation and Hyper-Chaotic System

2.1 Quantum Representation for Color Image

Generally, a color image contains information with three colorants of red (R), green (G) and blue (B), which are described by different grayscales. Visually, the color images are matched with the approximate spectrum quantitative properties of human eyes. The quantum representation for color image can be defined as [29]:

$$\begin{aligned} |I(\theta_\lambda)\rangle &= \frac{1}{2^n}\sum_{m=0}^{2^{2n}-1} |c_m\rangle \otimes |m\rangle \\ |c_m\rangle &= |r_m\rangle\,|g_m\rangle\,|b_m\rangle \end{aligned} \tag{1}$$

where $|r_m\rangle = \cos\theta_{1m}|0\rangle + \sin\theta_{1m}|1\rangle$, $|g_m\rangle = \cos\theta_{2m}|0\rangle + \sin\theta_{2m}|1\rangle$, $|b_m\rangle = \cos\theta_{3m}|0\rangle + \sin\theta_{3m}|1\rangle$, $\theta_\lambda \in \left[0, \frac{\pi}{2}\right]$, λ=1, 2, 3 and $m = 0, 1, \ldots, 2^{2n}-1$. n is the number of quantum bits required to encode. Quantum states $|0\rangle$ and $|1\rangle$ are the 2D computational basis quantum states, θ_λ is the primary phase encoding information of red, green or blue vectors, $|c_m\rangle$ and $|m\rangle$ encode color information and the corresponding position of the pixel, respectively. The preparation of quantum color image is shown in Fig. 1.

The three components of the color image are equivalent to three separate gray images, respectively. For a gray image, the position qubit $|m\rangle = |yx\rangle = |y\rangle|x\rangle = |y_{n-1}y_{n-2}\ldots y_0\rangle\,|x_{n-1}x_{n-2}\ldots x_0\rangle$ encodes the corresponding position information of the

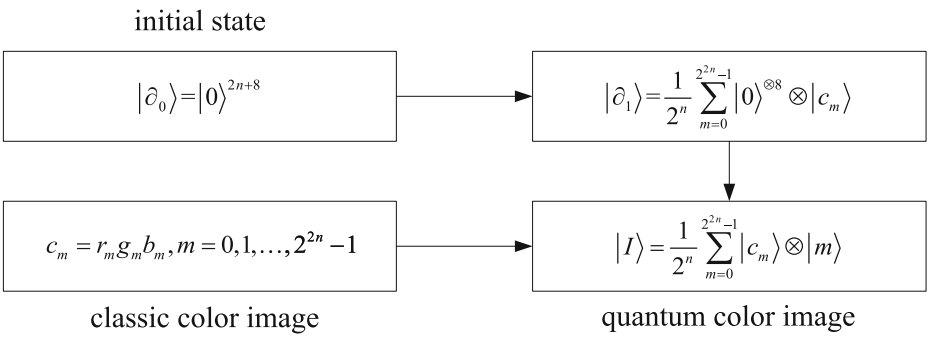

Fig. 1 Preparation of quantum color image

quantum images, where $|y_{n-1}y_{n-2}\ldots y_0\rangle$ encodes the information of the first n-qubit along the vertical location while $|x_{n-1}x_{n-2}\ldots x_0\rangle$ encodes the information of the rest n-qubit along the horizontal location.

2.2 Hyper-Chaotic System

In 1999, the Chen's system was put forward in a three-dimensional way.

$$\begin{cases} \bar{x} = a\,(y - x) \\ \bar{y} = cx - ax - xz - cy \\ \bar{z} = xy - bz \end{cases} \tag{2}$$

If the control parameters a, b, c in (2) are taken 35, 3, 28, respectively, the system would be chaotic. The Chen's chaotic system could be used to generate the hyper-chaotic system state [34].

$$\begin{cases} \bar{X} = d\,(y - x) \\ \bar{Y} = ex + hy - xz + w \\ \bar{Z} = y^2 - lz \\ \bar{W} = -qx \end{cases} \tag{3}$$

where d, e, h, l and q are the parameters of the system. While they take 27.5, 3, 19.3, 2.9, 3.3, respectively, the system would be in a hyper-chaotic state under the conditions of any given chaotic system state with a set of initial values $\bar{X}_0$, $\bar{Y}_0$, $\bar{Z}_0$, $\bar{W}_0$. The hyper-chaotic system is more effective and more appropriate for image encryption than the chaotic system [13]. With parameters $d = 27.5$, $e = 3$, $h = 19.3$, $l = 2.9$, $q = 3.3$, and the hyper-chaos attractors shown in Fig. 2, the Lyapunov exponents of the hyper-chaos system are 1.6170, 0.1123, 0, −12.8425. Apparently, the hyper-chaos system has two positive Lyapunov exponents, thus the prediction time of a hyper-chaotic system is shorter than that of a chaotic system [35] and the hyper-chaotic system is better than chaos system for security algorithm.

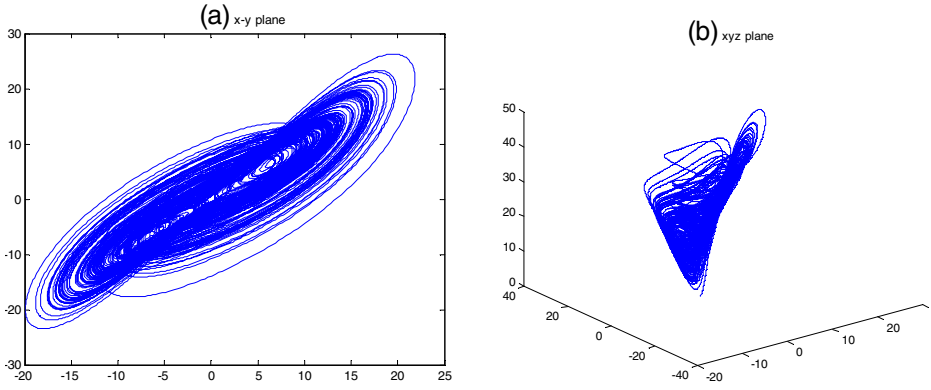

Fig. 2 Hyper-chaos attractors of Chen's hyper-chaotic system with $q = 3.3$

3 Quantum Color Image Encryption and Decryption Algorithm

3.1 Quantum Color Image Encryption Based on the Hyper-Chaotic System

Assume the quantum original image is $|I(\theta_\lambda)\rangle = \frac{1}{2^n}\sum_{m=0}^{2^{2n}-1}|c_m\rangle \otimes |m\rangle$, where $|c_m\rangle = |r_m\rangle\,|g_m\rangle\,|b_m\rangle, m = 0, 1, \ldots, 2^{2n}-1, |r_m\rangle = \cos\theta_{1m}\,|0\rangle + \sin\theta_{1m}\,|1\rangle, |g_m\rangle = \cos\theta_{2m}\,|0\rangle + \sin\theta_{2m}\,|1\rangle, |b_m\rangle = \cos\theta_{3m}\,|0\rangle + \sin\theta_{3m}\,|1\rangle, \theta_\lambda \in \left[0, \frac{\pi}{2}\right]$, λ=1, 2, 3. The three color components of the original image have $2^n \times 2^n$ pixels, respectively. Thus, 2^{2n} iterations are involved to produce 2^{2n} numbers for XOR operations. The whole process of the proposed encryption algorithm is as follows.

Step. 1 By choosing the initial parameters $\bar{X}_0$, $\bar{Y}_0$, $\bar{Z}_0$ and $\bar{W}_0$, four sequences $\bar{X}_m$, $\bar{Y}_m$, $\bar{Z}_m$ and $\bar{W}_m$ are generated by the fourth order Runge Kutta algorithm with 2^{2n} iterations.
Step 2 $\bar{X}_m$, $\bar{Y}_m$, $\bar{Z}_m$ and $\bar{W}_m$ are discretized with (4), then the four corresponding integer sequences T_m (T takes X, Y, Z and W, respectively.) could be obtained.

$$T_m = \left| f(\overline{T_m} - f(\overline{T_m})) \right| \times 10^{15} \bmod 256 \tag{4}$$

where $f(x)$ rounds x to the nearest integer less than or equal to x and mod returns the remainder after division.
Step. 3 Start from the first pixel of the plaintext, each pixel is decomposed into three gray components, and each cipher-text a_{rm}, a_{gm} or a_{bm} could be obtained with XOR operation $\oplus$.

$$\begin{cases} a_{rm} = r_m \oplus (X_m \bmod 256) \\ a_{gm} = g_m \oplus (2Y_m \bmod 256) \\ a_{bm} = b_m \oplus (3Z_m \bmod 256) \end{cases} \tag{5}$$

Step. 4 Based on the integer sequences X_m, Y_m, Z_m and W_m of the hyper-chaotic system, three of them are formed as a combination Q_L.

$$L = \bmod(X_m, 4), \quad m = 0, 1, \ldots, 2^{2n} - 1. \tag{6}$$

where X_m is the integer sequence of the hyper-chaotic system. In order to scramble the pixel values better and enhance the sensitivity of the keys, from Table 1, the corresponding state variable combination Q_L is used to perform XOR operation with each cipher-text a_{rm}, a_{gm} or a_{bm}.

$$\begin{cases} A_{rm} = a_{rm} \oplus Q_L \\ A_{gm} = a_{gm} \oplus Q_L \\ A_{bm} = a_{bm} \oplus Q_L \end{cases} \tag{7}$$

Table 1 Combination rule of the hyper-chaotic sequences

Serial numbers (L)	State variable combinations (Q_L)
0	(X_m, Y_m, Z_m)
1	(X_m, Y_m, W_m)
2	(X_m, Z_m, W_m)
3	(Y_m, Z_m, W_m)

Step 5 Image data matrices $|P\rangle$ are achieved by compounding A_{rm}, A_{gm} and A_{bm} from (7).

$$|P\rangle = \frac{1}{2^n}\sum_{m=0}^{2^{2n}-1} |A_{rm}\rangle \left|A_{gm}\right\rangle |A_{bm}\rangle |m\rangle \tag{8}$$

where $|A_{rm}\rangle = \cos\theta'_{1m}|0\rangle + \sin\theta'_{1m}|1\rangle$, $\left|A_{gm}\right\rangle = \cos\theta'_{2m}|0\rangle + \sin\theta'_{2m}|1\rangle$, $|A_{bm}\rangle = \cos\theta'_{3m}|0\rangle + \sin\theta'_{3m}|1\rangle$, $m = 0, 1, \ldots, 2^{2n}-1$.

Step. 6 Set quantum rotation gate $R(\xi_m, \psi_m, \zeta_m) = T_X(\xi_m) \otimes T_Y(\psi_m) \otimes T_Z(\zeta_m)$, where ξ_m, ψ_m and ζ_m represent the rotation angles around x, y, z axes, respectively.

$$T_X(\xi_m) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\xi_m & -\sin\xi_m \\ 0 & \sin\xi_m & \cos\xi_m \end{pmatrix} \tag{9a}$$

$$T_Y(\psi_m) = \begin{pmatrix} \cos\psi_m & 0 & \sin\psi_m \\ 0 & 1 & 0 \\ -\sin\psi_m & 0 & \cos\psi_m \end{pmatrix} \tag{9b}$$

$$T_Z(\zeta_m) = \begin{pmatrix} \cos\zeta_m & -\sin\zeta_m & 0 \\ \sin\zeta_m & \cos\zeta_m & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{9c}$$

$R(\xi_m, \psi_m, \zeta_m)$ is applied to rotate the corresponding A_{rm}, A_{gm} and A_{bm} in the spatial domain.

$$\begin{bmatrix} A_{r'm} \\ A_{g'm} \\ A_{b'm} \end{bmatrix} = R(\xi_m, \psi_m, \zeta_m) \begin{bmatrix} A_{rm} \\ A_{gm} \\ A_{bm} \end{bmatrix} \tag{10}$$

$|P_1\rangle = \frac{1}{2^n}\sum_{m=0}^{2^{2n}-1} |A_{r'm}\rangle \left|A_{g'm}\right\rangle |A_{b'm}\rangle \otimes |m\rangle$ could be obtained from (10), and $|A_{r'm}\rangle = \cos(\theta'_{1m}+\xi_m)|0\rangle + \sin(\theta'_{1m}+\xi_m)|1\rangle$, $\left|A_{g'm}\right\rangle = \cos(\theta'_{2m}+\psi_m)|0\rangle + \sin(\theta'_{2m}+\psi_m)|1\rangle$, $|A_{b'm}\rangle = \cos(\theta'_{3m}+\zeta_m)|0\rangle + \sin(\theta'_{3m}+\zeta_m)|1\rangle$.

3.2 Quantum Fourier Transform

The quantum Fourier transform was concluded from the traditional discrete Fourier transform [16](Fig. 3).

$$\mathrm{QFT}:\ U_{\mathrm{QFT}}|t\rangle = \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} e^{2\pi \mathrm{i}kt/N}|k\rangle \tag{11}$$

where U_{QFT} is defined to be a linear operator with the following action on the orthonormal basis states $|0\rangle, \ldots, |N-1\rangle$, QFT is a 2^n unitary transformation for a single state into superposition, k and t represent two integers ranging from 0 to $N-1$. So far, the QFT has been demonstrated experimentally by using the quantum Hadamard gates and the conditional phase gates [16, 36].

A controlled phase rotation gate ρ'_w(CROT) [37] used in the QFT is defined as

$$\rho'_w |H\rangle_u |J\rangle_v = \begin{cases} |H\rangle_u e^{\mathrm{j}\rho_w}|J\rangle_v, & |H\rangle_u = |1\rangle = |J\rangle_v; \\ |H\rangle_u |J\rangle_v, & \text{else.} \end{cases} \tag{12}$$

where qubit number u acts as the control qubit $|H\rangle_u \in \{|0\rangle, |1\rangle\}$, and qubit number v acts as the target qubit $|J\rangle_v \in \{|0\rangle, |1\rangle\}$, $w = |f\lfloor u - v\rfloor|$ is the integer distance between qubit

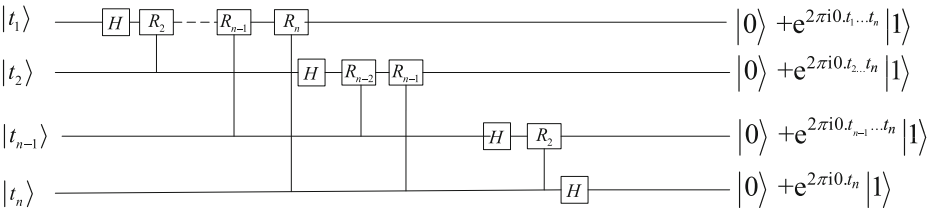

Fig. 3 Circuit for quantum Fourier transform

numbers u and v, where $f\lfloor x \rfloor$ rounds x to the nearest integer less than or equal to x, integer distance represents integer absolute value of $f\lfloor u - v \rfloor$. Moreover, in the case of the exact QFT,

$$\rho_w = \frac{\pi}{2^w} \tag{13}$$

Equation 13 defines an exponential hierarchical structure of phase rotation angles, the base of the exponential in (13) relates directly to the base-2 arithmetic used in transcribing the abstract QFT unitary transformation into a realization with qubits of two possible states. Due to the number-theoretical relationships, the qubit-based QFT will be executed perfectly in this way, while the desired reinforcements (quantum interference) and amplitude cancellations will be precisely taken place [37].

Assume R channel $|I(\theta)\rangle$ is extracted from the color image $|I(\theta_\lambda)\rangle$ to generate a representation of image in quantum states, it could be defined as [38],

$$|I(\theta)\rangle = \frac{1}{2^n} \sum_{m=0}^{2^{2n}-1} h_m \otimes |m\rangle \tag{14}$$

$$h_m = \frac{1}{2^n} \sum_{m=0}^{2^{2n}-1} \left(|0\rangle + e^{j\theta_m} |1\rangle \right) |m\rangle \tag{15}$$

where, $m = 0, 1, \ldots, 2^{2n} - 1$, there is a $2n + 1$ qubits unitary transform E_κ that turns the color angle θ_m corresponding to the position $|m\rangle$ of the quantum image $|I(\theta)\rangle$ into a color angle σ_m. Given the angles θ_m and σ_m, there exists angle $\phi_m = \sigma_m - \theta_m$; thus, we can construct a $2n + 1$ qubits-based unitary transform E_κ as:

$$E_\kappa = \left(I_0 \otimes \sum_{m=0, m\neq\kappa}^{2^{2n}-1} |m\rangle \langle m| \right) + F_\kappa \otimes |\kappa\rangle \langle \kappa| \tag{16}$$

$$F_\kappa = \begin{pmatrix} 1 & 0 \\ 0 & \phi'_\kappa |H\rangle_u |J\rangle_v \end{pmatrix} \tag{17}$$

F_κ is a phase gate, the controlled phase matrix E_κ is a unitary matrix, $E_\kappa E_\kappa^* = I_0^{\otimes 2n+1}$, where E_κ^* is the Hermitian conjugate of E_κ, I_0 is a two-dimensional identity matrix, $\phi'_\kappa |H\rangle_u |J\rangle_v$ matches the corresponding values in (12). Sequences of controlled phase matrices in (16) are designed to change every angle encoding color without destroying that

of the other positions. Thus, the angles encoding colors $\theta_m = \left(\theta_1, \theta_2, \ldots, \theta_{2^{2n}-1}\right)$ can be transformed.

$$\begin{aligned} & E_\eta E_\kappa \left|I(\theta)\right\rangle \\ = & \frac{1}{2^n}\left[\sum_{m=0,m\neq\kappa,\eta}^{2^{2n}-1}\left(|0\rangle + e^{\mathrm{j}\theta_m}|1\rangle\right)|m\rangle + \left(|0\rangle + e^{\mathrm{j}(\theta_\kappa+\phi_\kappa)}|1\rangle\right)|\kappa\rangle + \left(|0\rangle + e^{\mathrm{j}(\theta_\eta+\phi_\eta)}|1\rangle\right)|\eta\rangle\right] \\ = & \frac{1}{2^n}\left[\sum_{m=0,m\neq\kappa,\eta}^{2^{2n}-1}\left(|0\rangle + e^{\mathrm{j}\theta_m}|1\rangle\right)|m\rangle + \left(|0\rangle + e^{\mathrm{j}\sigma_\kappa}|1\rangle\right)|\kappa\rangle + \left(|0\rangle + e^{\mathrm{j}\sigma_\eta}|1\rangle\right)|\eta\rangle\right] \end{aligned} \tag{18}$$

From (18), it is clear that

$$\begin{aligned} E\left|I(\theta)\right\rangle &= \prod_{j=0}^{2^{2n}-1} E_j \left|I(\theta)\right\rangle \\ &= \frac{1}{2^n}\sum_{m=0}^{2^{2n}-1}\left(|0\rangle + e^{\mathrm{j}(\theta_m+\phi_m)}|1\rangle\right)|m\rangle \\ &= \frac{1}{2^n}\sum_{m=0}^{2^{2n}-1}\left(|0\rangle + e^{\mathrm{j}\sigma_m}|1\rangle\right)|m\rangle \end{aligned} \tag{19}$$

Likewise, the similar operations E' and E'' could implement on the G and B channels also.

$$E'\left|I(\theta')\right\rangle = \frac{1}{2^n}\sum_{m=0}^{2^{2n}-1}\left(|0\rangle + e^{\mathrm{j}\sigma'_m}|1\rangle\right)|m\rangle \tag{20}$$

$$E''\left|I(\theta'')\right\rangle = \frac{1}{2^n}\sum_{m=0}^{2^{2n}-1}\left(|0\rangle + e^{\mathrm{j}\sigma''_m}|1\rangle\right)|m\rangle \tag{21}$$

Step 7: The new image $|P_2\rangle$ is obtained by implementing quantum Fourier transform, and then quantum random phase operation in the Fourier transform domain is performed [39].

$$\begin{aligned} |P_2\rangle &= \mathrm{QFT}\,|P_1\rangle \\ &= \mathrm{QFT}\left(\frac{1}{2^n}\sum_{m=0}^{2^{2n}-1}|A_{r'm}\rangle\left|A_{g'm}\right\rangle|A_{b'm}\rangle|m\rangle\right) \end{aligned} \tag{22}$$

$$\begin{aligned} |P_3\rangle &= (E''\otimes E'\otimes E)\,|P_2\rangle \\ &= (E''\otimes E'\otimes E)\left(\mathrm{QFT}\left(\frac{1}{2^n}\sum_{m=0}^{2^{2n}-1}|A_{r'm}\rangle\left|A_{g'm}\right\rangle|A_{b'm}\rangle|m\rangle\right)\right) \end{aligned} \tag{23}$$

Step 8: Execute the inverse quantum Fourier transform on $|P_3\rangle$ to obtain the final encrypted image $|P_4\rangle$.

$$\begin{aligned} |P_4\rangle &= \mathrm{IQFT}(|P_3\rangle) \\ &= \mathrm{IQFT}\left((E''\otimes E'\otimes E)\left(\mathrm{QFT}\left(\frac{1}{2^n}\sum_{m=0}^{2^{2n}-1}|A_{r'm}\rangle\left|A_{g'm}\right\rangle|A_{b'm}\rangle|m\rangle\right)\right)\right) \end{aligned} \tag{24}$$

3.3 Quantum Color Image Decryption Process

The encryption process is completely reversible, so the decryption process is similar to the encryption process.

Step1: Perform quantum Fourier transform on $|P_4\rangle$.

$$\mathrm{QFT}\left(|P_4\rangle\right) = \mathrm{QFT}(\mathrm{IQFT}(|P_3\rangle)) = |P_3\rangle \tag{25}$$

Step 2: $|P_2\rangle$ is obtained by applying calculation of random phase conjugate on $|P_3\rangle$,

$$\begin{aligned} &(E'' \otimes E' \otimes E)^* \, |P_3\rangle \\ &= (E'' \otimes E' \otimes E)^* ((E'' \otimes E' \otimes E) \, |P_2\rangle) \\ &= ((E'')^* \otimes (E')^* \otimes E^*)((E'' \otimes E' \otimes E) \, |P_2\rangle) = |P_2\rangle \end{aligned} \tag{26}$$

then the inverse quantum Fourier transform is performed.

$$\mathrm{IQFT} \, |P_2\rangle = \mathrm{IQFT}(\mathrm{QFT} \, |P_1\rangle) = |P_1\rangle \tag{27}$$

Step 3: Execute the decrypted operation on $|P_1\rangle$ with the key $R^{-1}(\xi, \psi, \zeta)$.

$$\begin{aligned} &R^{-1}(\xi, \psi, \zeta) \, |P_1\rangle = (T_X(\xi) \otimes T_Y(\psi) \otimes T_Z(\zeta))^{-1} \, |P_1\rangle \\ &= T_X^{-1}(\xi) \otimes T_Y^{-1}(\psi) \otimes T_z^{-1}(\zeta) \left(\frac{1}{2^n} \sum_{m=0}^{2^{2n}-1} |A_{r'm}\rangle \left|A_{g'm}\right\rangle |A_{b'm}\rangle \, |m\rangle \right) \\ &= T_X^{-1}(\xi) \otimes T_Y^{-1}(\psi) \otimes T_Z^{-1}(\zeta) \left(T_X(\xi) \otimes T_Y(\psi) \otimes T_Z(\zeta) \left(\frac{1}{2^n} \sum_{m=0}^{2^{2n}-1} |A_{rm}\rangle \left|A_{gm}\right\rangle |A_{bm}\rangle \, |m\rangle \right) \right) \\ &= \frac{1}{2^n} \sum_{m=0}^{2^{2n}-1} |A_{rm}\rangle \left|A_{gm}\right\rangle |A_{bm}\rangle \, |m\rangle \end{aligned} \tag{28}$$

Step 4: The keys involved in the whole encryption process are the initial parameters $\bar{X}_0$, $\bar{Y}_0$, $\bar{Z}_0$ and $\bar{W}_0$. The solutions are based on $\bar{X}_0$, $\bar{Y}_0$, $\bar{Z}_0$ and $\bar{W}_0$, and it could be successful to restore the original image in turn.

4 Security Analysis

4.1 Theoretical Analyses and Experimental Simulation

Traditional encryption technology is widely used in real life, which can protect the classic data from unauthorized modification and interception, but once the classic data suffer the brute-force attacks, there is no irreversible change. Infer from the quantum Uncertainty principle and No-cloning theorem, if an illegal attacker wants to obtain information from the unknown quantum state, the quantum state must be first measured, it would lead to the quantum state collapsing randomly into an eigenstate of the measurement operators irreversibly [40], moreover, unknown quantum state couldn't be reproduced.

Since a practical and useful quantum computer is still unavailable, the experiments are limited to classical simulations on a classical computer with MATLAB. The 200×200 color image "Lena" is chosen as the original image, which is shown in Fig. 4a. $\bar{X}_0$=0.146, $\bar{Y}_0$= − 0.329, $\bar{W}_0$=1.000 are set as the initial parameters of the hyper-chaotic system. The encrypted image is given in Fig. 4b. The encrypted image does not show any information of the original image visually.

Fig. 4 Results of test images: (**a**) the original image (**b**) the encrypted image

4.2 Statistical Analysis

(1) Information entropy

The information entropy is often used to measure the randomness of the cipher images. The entropy $H(m)$ of a message source S is:

$$H(m) = \sum_{m=0}^{2^N-1} p(s_m) \log_2 \frac{1}{p(s_m)} \tag{29}$$

where $p(s_m)$ represents the probability of symbol s_m and the entropy is expressed in bits. After encrypting a message, the ideal entropy of the encrypted image should be approaching 8 bits [41]. If the entropy is close to 8 bits, then it means the encryption system could resist the brute-force attack. With the proposed image encryption algorithm, counting times of each pixel in three primary colors (R, G, and B) and calculating the corresponding probability, three colors corresponding to the information entropy are shown in Table 2. 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 (Fig. 5).

Table 2 The information entropy of image Lena

Image channels	Information Entropy (bits)	
	Original image	Encrypted image
Lena (R)	7.3137	7.9950
Lena (G)	7.5880	7.9953
Lena (B)	7.1151	7.9955
Splash (R)	6.9197	7.9959
Splash (G)	6.8978	7.9951
Splash (B)	6.0673	7.9957
Beans (R)	5.2691	7.9949
Beans (G)	5.7069	7.9957
Beans (B)	6.5544	7.9957

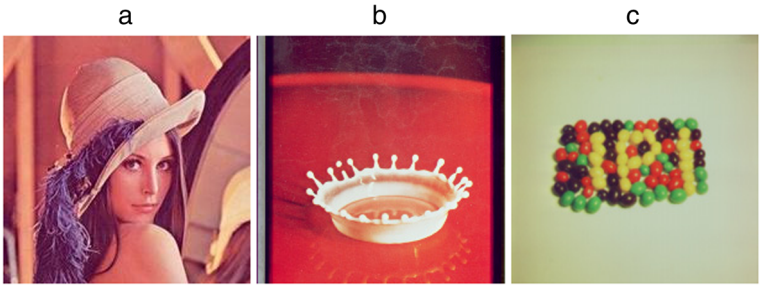

Fig. 5 **a** original image Lena (**b**) original image Splash (**c**) original image Beans

(2) Histogram

A good image encryption scheme should always generate a uniform histogram of the cipher-image for any plain-image. Figure 6a, Fig. 7a and Fig. 8a are the histograms of three primary colors of the original image while Fig. 6b, Fig. 7b and Fig. 8b are those of their corresponding encrypted image. It can be seen that the histograms of the original image "Lena" are not evenly distributed and their shape difference is distinctly, while the histograms of the encrypted image tend to be a similar shape. It demonstrates that an attacker can hardly launch any effective statistical attack since the gray values are distributed uniformly.

(3) Correlation between adjacent pixels

A color image is divided into three channels, i.e., R, G and B, and each channel is regarded as a gray-scale image. In ordinary images with definite visual content, each pixel is highly correlated with its adjacent pixels. A desirable encryption scheme should generate an encrypted image with rather weak correlation between adjacent pixels. The horizontal pixels correlation coefficient is:

$$\rho_{xy} = \frac{cov\,(x, y)}{\sqrt{D\,(x)\,D\,(y)}} \tag{30}$$

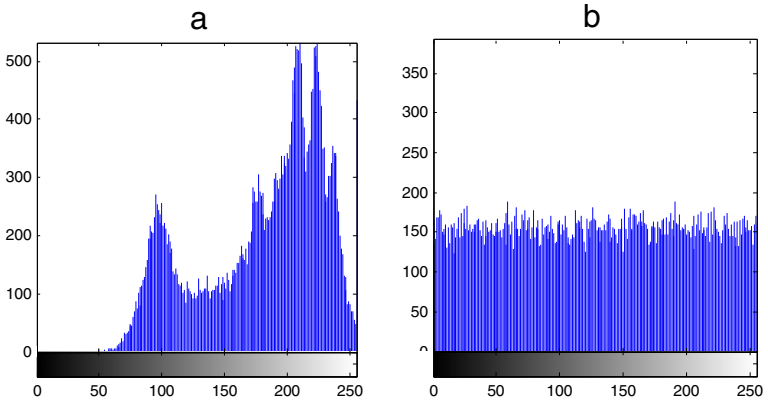

Fig. 6 Histograms of R channel: (**a**) Lena, (**b**) encrypted Lena

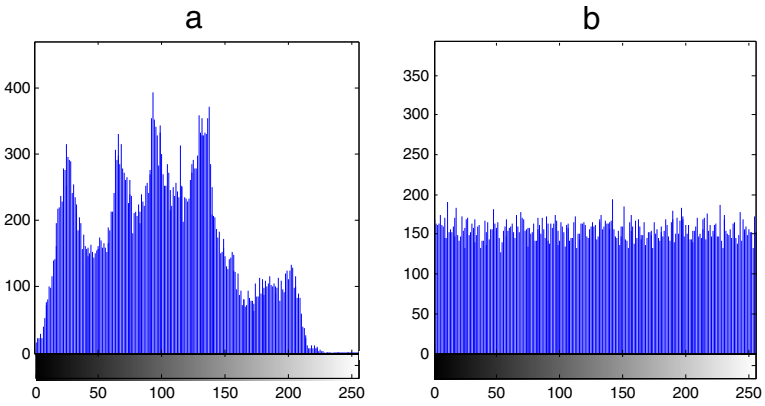

Fig. 7 Histograms of G channel: (**a**) Lena, (**b**) encrypted Lena

The covariance $\mathrm{cov}(x, y)$ and the variance $D(x)$ can be expressed respectively:

$$cov(x, y) = \frac{1}{n}\sum_{i=1}^{n}\left(x_i - \bar{x}\right)\left(y_i - \bar{y}\right) \tag{31}$$

$$\mathrm{D}(x) = \frac{1}{n}\sum_{j=1}^{n}\left(x_j - \bar{x}\right)^2 \tag{32}$$

where $\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i$, $\bar{y} = \frac{1}{n}\sum_{i=1}^{n} y_i$. Similarly, the correlation coefficients of the vertical and diagonal directions could be obtained also. The correlation coefficients of three primary colors in horizontal, vertical and diagonal directions are shown in Table 3.

Figs. 9, 10 and 11 show the correlation distributions between two adjacent pixels of R channel in the horizontal, vertical and diagonal directions.

Based on the data and figures above, three primary colors (RGB) of the original image in all directions between the adjacent pixels have close correlation. The correlation coefficients of the encrypted image are much little, which shows that the information was

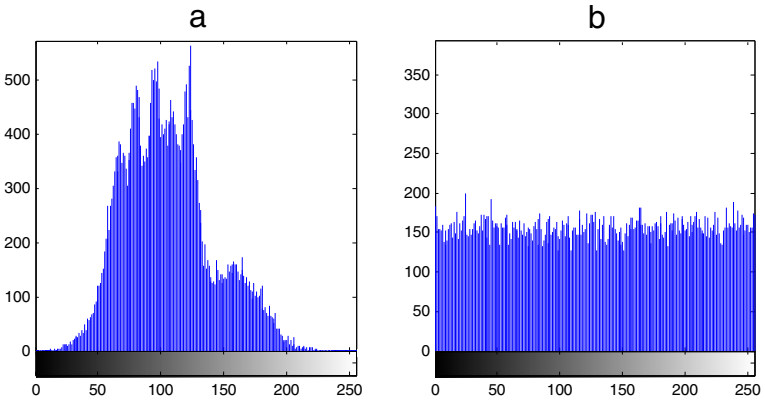

Fig. 8 Histograms of B channel: (**a**) Lena, (**b**) encrypted Lena

Table 3 Correlation coefficients between adjacent pixels

Correlation coefficient	Horizontal	Vertical	Diagonal
Original Lena (R)	0.9535	0.9151	0.8791
Encrypted Lena (R)	0.0224	−0.0195	0.0211
Original Lena (G)	0.9610	0.9208	0.8938
Encrypted Lena (G)	−0.0122	0.0088	−0.0074
Original Lena (B)	0.9159	0.8500	0.7961
Encrypted Lena (B)	−0.0129	0.0129	0.0020
Original Beans (R)	0.9624	0.9600	0.9259
Encrypted Beans (R)	0.0134	−0.0122	−0.0009
Original Beans (G)	0.9730	0.9701	0.9413
Encrypted Beans (G)	0.0100	−0.0002	0.0128
Original Beans (B)	0.9837	0.9889	0.9742
Encrypted Beans (B)	0.0019	−0.0107	−0.0098

excellently hidden after the original image being encrypted. Thus the attacker cannot implement any statistical attack from the aspect of correlation.

(4) Key space and key sensitivity Key space should be large enough to resist the brute-force attack, and it is also an important indicator of a security encryption algorithm. It is recommended that the ideal key space should be larger than 2^{100} while considering the current computer computation speed [42]. The time complexity for color image decryption in our presented algorithm is computed by: $C\left(\bar{X}_0, \bar{Y}_0, \bar{Z}_0, \bar{W}_0\right) = \Theta\left(\bar{X}_0 \times \bar{Y}_0 \times \bar{Z}_0 \times \bar{W}_0\right)$, where $\bar{X}_0$, $\bar{Y}_0$, $\bar{Z}_0$ and $\bar{W}_0$ are the initial keys of the hyper-chaotic system. Considering that the calculation precision is 10^{-15}, the size of key space for initial parameters would be approximately 2^{200}. Moreover, the quantum rotation gate $R\left(\xi_m, \psi_m, \zeta_m\right)$ and random phase gates E, E' and E'' could be also used as the secret keys, which are more than 2^{100}, thus the encryption algorithm has high security.

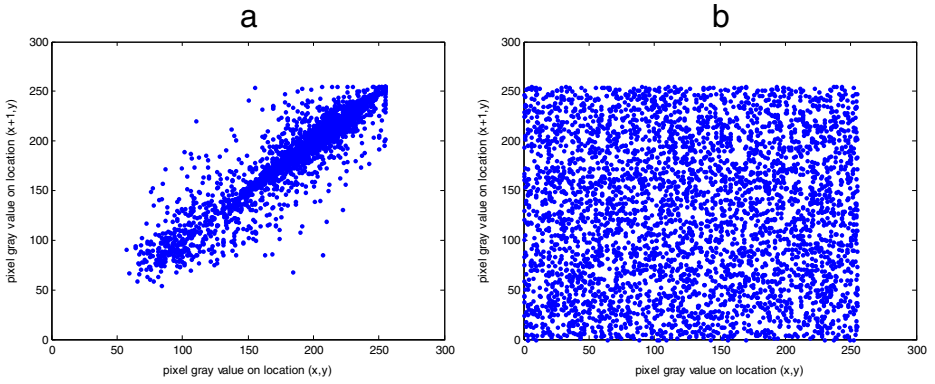

Fig. 9 Correlation distributions between two horizontal adjacent pixels in R channel: (**a**) original image Lena and (**b**) encrypted image

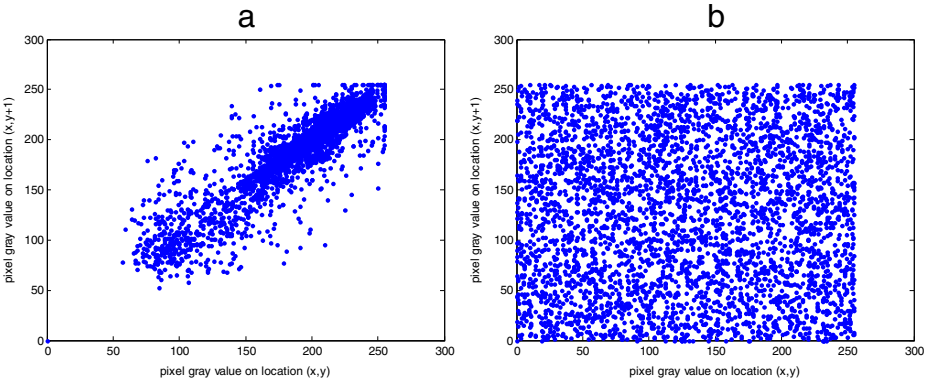

Fig. 10 Correlation distributions between two vertical adjacent pixels in R channel: (**a**) original image Lena and (**b**) encrypted image

Key is the secret parameters of the encryption schemes. A good encryption scheme must have enough sensitivity to the key, i.e., the deciphered results are significantly different even if only the key is changed slightly. To detect the sensitivity of the key, the key could be changed little deviation to observe the effect of the decrypted image. As all of the secret keys are right, the image is shown in Fig. 12a; The decrypted image is shown in Fig. 12b with the wrong keys $\bar{X}_0+10^{-15}$; Similarly, if $\bar{Y}_0$, $\bar{Z}_0$, $\bar{W}_0$ deviate 10^{-15} respectively, while all of the other three keys are correct, the corresponding decrypted images are shown in Figs. 12c, d and e. It is convinced that the correct image could be reconstructed if the decryption keys and the domain positions match accurately, which ensures high security of the image encryption algorithm.

(5) Computational complexity

Assume the original image 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. According to the parallel characteristics of quantum computing, the gray-scale information for each pixel of the quantum image is performed with the quantum XOR operation $\oplus$, which is realized by using a $2n-$ CNOT gate. It is understood that each $n-$ CNOT

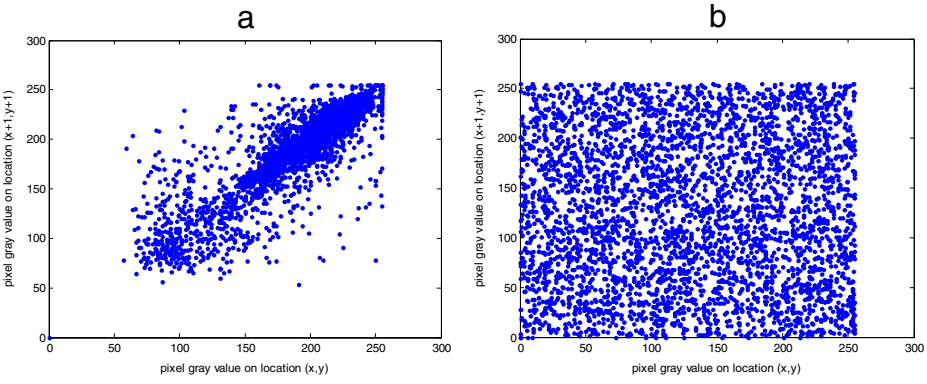

Fig. 11 Correlation distributions between two diagonal adjacent pixels in R channel: (**a**) original image Lena and (**b**) encrypted image

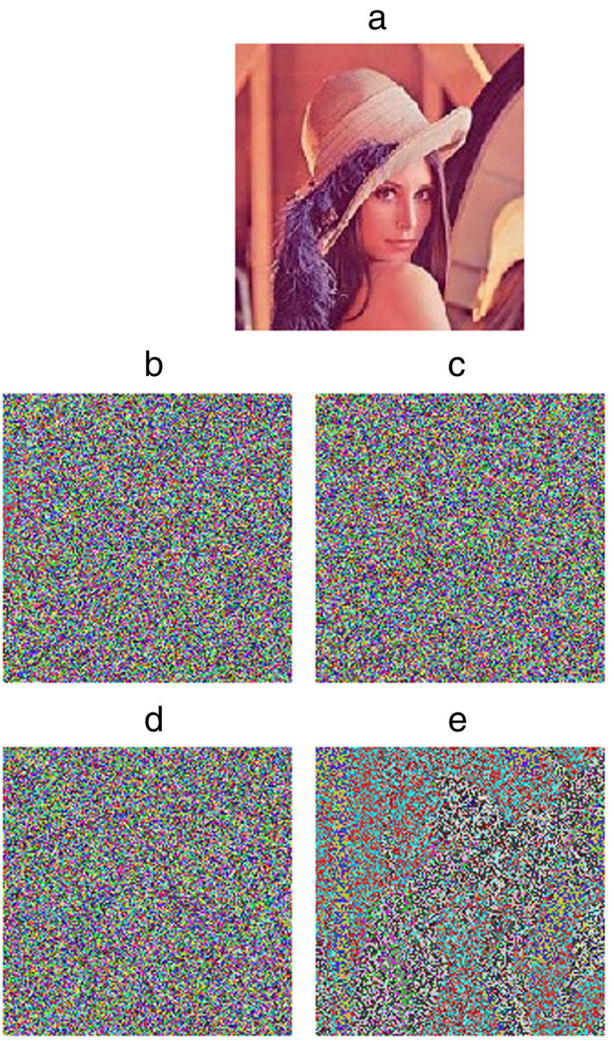

Fig. 12 Decrypted images with: (**a**) correct keys, (**b**) incorrect $\bar{X}_0+10^{-15}$, (**c**) incorrect $\bar{Y}_0+10^{-15}$, (**d**) incorrect $\bar{Z}_0+10^{-15}$, (**e**) incorrect $\bar{W}_0+10^{-15}$

gate can be decomposed into $4n-8$ Toffoli gates, and the Toffoli gate can be realized by six Controlled-NOT gates [40]. In the proposed image encryption algorithm, the hyper-chaotic sequences are scrambled and diffused by the XOR operation, and the mix of three components involves six times of CNOT gate operations, thus the quantum image XOR operation needs $128n-256$ basic gates. Consequently, the computational complexity of the quantum image XOR operation is $O(n)$. The complexity of quantum random-phase operation for a quantum image is $O(n)$, thus the random phase operation and rotation operation are of the same computational complexity. For an n-qubit input, the computation time of quantum Fourier transform is $O\left(n^2\right)$ [43]. Consequently, the total computational complexity is $O\left(n^2\right)$ by neglecting the small complexity. The classical image XOR operations could be accomplished by performing 6×2^{2n} XOR operations,

and the classical random-phase encoding could be realized by 2^{2n} multiplication operations, thus the computational complexity of XOR operation is $O\left(2^{2n}\right)$. Consequently, the computational complexity of the classical Fourier transform operation is $O\left(n2^{2n}\right)$. As a result, the whole computational complexity $O\left(n2^{2n}\right)$ of the classical encryption algorithm is required. In brief, the computational complexity of the presented quantum color image encryption algorithm is lower than that of its classical counterparts.

5 Conclusion

The measurement principle and superposition of quantum states are utilized to establish the interaction among image pixels. A new quantum color image encryption and decryption scheme based on a hyper-chaotic system is proposed, which exploits the interesting properties of a hyper-chaotic system. The initial parameters of the hyper-chaotic system are applied into the quantum color image encryption scheme to increase the number of keys and enlarge the key space. Consecutively, the positions in an image could be divided into groups with the same color. Theoretical analyses and experimental results indicate that the proposed scheme possesses the advantages of acceptable encryption speed, large key space and high level of security, and could be implemented efficiently.

Acknowledgments This work is supported by the National Natural Science Foundation of China (Grant Nos. 61462061 and 61561033), the Natural Science Foundation of Jiangxi Province, China (Grant No. 20151BAB207002) and the Opening Project of Shanghai Key Laboratory of Integrate Administration Technologies for Information Security (Grant No. AGK201602).

References

1. Ji, X., Bai, S., Guo, Y., et al.: A new security solution to JPEG using hyper-chaotic system and modified zigzag scan coding [J]. Commun. Nonlinear Sci. Numer. Simul. **22**(1), 321–333 (2015)
2. Li, X.W., Kim, S.T., Lee, I.K.: Color image encryption using a high-quality elemental image array [J]. Opt. Commun. **332**, 75–82 (2014)
3. Yang, J., Zhu, F.: Synchronization for chaotic systems and chaos-based secure communications via both reduced-order and step-by-step sliding mode observers [J]. Commun. Nonlinear Sci. Numer. Simul. **18**(4), 926–937 (2013)
4. Matthews, R.: On the derivation of a "chaotic" encryption algorithm [J]. Cryptologia **13**(1), 29–42 (1989)
5. Fridrich, J.: Symmetric ciphers based on two-dimensional chaotic maps [J]. Int. J. Bifurcation Chaos **8**(6), 1259–1284 (1998)
6. Kulsoom, A., Xiao, D., Abbas, S.A.: An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules [J]. Multimedia Tools Appl. **75**(1), 1–23 (2016)
7. Li, C., Li, S., Lo, K.T.: Breaking a modified substitution–diffusion image cipher based on chaotic standard and logistic maps [J]. Commun. Nonlinear Sci. Numer. Simul. **16**(2), 837–843 (2011)
8. Machkour, M., Saaidi, A.: Benmaati M L. A novel image encryption algorithm based on the two-dimensional logistic map and the latin square image cipher [J]. 3D Res. **6**(4), 1–18 (2015)
9. Zhang, Y.Q., Wang, X.Y.: A new image encryption algorithm based on non-adjacent coupled map lattices [J]. Appl. Soft Comput. **26**, 10–20 (2015)
10. Vargas, J.A.R., Grzeidak, E., Hemerly, E.M.: Robust adaptive synchronization of a hyperchaotic finance system [J]. Nonlinear Dyn. **80**(1-2), 239–248 (2015)
11. Yuan, H.M., Liu, Y., Gong, L.H., et al.: A new image cryptosystem based on 2D hyper-chaotic system [J]. Multimedia Tools Appl., 1–22 (2016)
12. Ramadan, N., Ahmed, H.E.H., Elkhamy, S.E., et al.: Chaos-Based Image encryption using an improved quadratic chaotic map [J]. American J. Signal Process. **6**(1), 1–13 (2016)
13. Gao, T., Chen, Z.: A new image encryption algorithm based on hyper-chaos [J]. Phys. Lett. A **372**(4), 394–400 (2008)

14. 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]. J. Chem. Phys. **145**(2), 024703 (2016)
15. Yan, F., Iliyasu, A.M., Venegas-Andraca, S.E.: A survey of quantum image representations [J]. Quantum Inf. Process. **15**(1), 1–35 (2016)
16. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information [M]. Cambridge University Press, Cambridge (2010)
17. Feynman, R.P.: Simulating physics with computers [J]. Int. J. Theor. Phys. **21**(6/7), 467–488 (1982)
18. Batle, J., Ooi, C.H.R., Farouk, A., et al.: Do multipartite correlations speed up adiabatic quantum computation or quantum annealing? [J]. Quantum Inf. Process., 1–19 (2016)
19. Le, P.Q., Dong, F., Hirota, K.: A flexible representation of quantum images for polynomial preparation, image compression, and processing operations [J]. Quantum Inf. Process. **10**(1), 63–84 (2011)
20. Jiang, N., Zhao, N., Wang, L.: LSB Based quantum image steganography algorithm [J]. Int. J. Theor. Phys. **55**(1), 107–123 (2016)
21. Zhang, Y., Lu, K., Gao, Y., et al.: NEQR: A novel enhanced quantum representation of digital images [J]. Quantum Inf. Process. **12**(8), 2833–2860 (2013)
22. Venegas-Andraca, S.E.: Quantum walks: a comprehensive review [J]. Quantum Inf. Process. **11**(5), 1015–1106 (2012)
23. Nam, Y.S., Blümel, R.: Optical simulator of the quantum Fourier transform [J]. EPL (Europhysics Letters) **114**(2), 20004 (2016)
24. Calude, C.S., Calude, E., Dinneen, M.J.: Guest Column: Adiabatic quantum computing challenges [J]. Acm. Sigact. News **46**(1), 40–61 (2015)
25. Ren, G., Du, J.: Statistical properties of thermal state under quantum Hadamard transform [J]. Int. J. Theor. Phys. **52**(3), 779–787 (2013)
26. Jiang, N., Wu, W.Y., Wang, L.: The quantum realization of Arnold and Fibonacci image scrambling [J]. Quantum Inf. Process. **13**(5), 1223–1236 (2014)
27. Liang, H.R., Tao, X.Y., Zhou, N.R.: Quantum image encryption based on generalized affine transform and logistic map [J]. Quantum Inf. Process., 1–24 (2016)
28. El-Latif, A.A.A., Li, L., Wang, N., et al.: A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces [J]. Signal Process. **93**(13), 2986–3000 (2013)
29. 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 [J]. Inform. Sci. **277**, 445–457 (2014)
30. Liu, X.: Analysis and improvement for image encryption algorithm based on multiple chaotic mapping [J]. Open Autom. Control Syst. J. **7**, 1560–1565 (2015)
31. Wu, X., Kan, H., Kurths, J.: A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps [J]. Appl. Softw. Comput. **37**, 24–39 (2015)
32. Devoret, M.H., Schoelkopf, R.J.: Superconducting circuits for quantum information: an outlook [J]. Science **339**(6124), 1169–1174 (2013)
33. Yang, Y.G., Xia, J., Jia, X., et al.: Novel image encryption/decryption based on quantum Fourier transform and double phase encoding [J]. Quantum Inf. Process. **12**(13), 3477–3493 (2013)
34. Li, C., Sprott, J.C., Yuan, Z., et al.: Constructing chaotic systems with total amplitude control [J]. Int. J. Bifurcation Chaos **25**(12), 1530025 (2015)
35. Vaidyanathan, S., Pham, V.T., Volos, C.K.: A 5-D hyperchaotic Rikitake dynamo system with hidden attractors [J]. Eur. Phys. J. Spec. Top. **224**(8), 1575–1592 (2015)
36. Balthazar, W.F., Caetano, D.P., Souza, C.E.R., et al.: Using polarization to control the phase of spatial modes for application in quantum information [J]. Braz. J. Phys. **44**(6), 658–664 (2014)
37. Nam, Y.S., Blümel, R.: Structural stability of the quantum Fourier transform [J]. Quantum Inf. Process. **14**(4), 1179–1192 (2015)
38. Song, X.H., Niu, X.M.: Comment on: Novel image encryption/decryption based on quantum Fourier transform and double phase encoding [J]. Quantum Inf. Process. **13**(6), 1301–1304 (2014)
39. Zhou, N.R., Hua, T.X., Gong, L.H., et al.: Quantum image encryption based on generalized Arnold transform and double random-phase encoding [J]. Quantum Inf. Process. **14**(4), 1193–1213 (2015)
40. Hua, T., Chen, J., Pei, D., et al.: Quantum image encryption algorithm based on image correlation decomposition [J]. Int. J. Theor. Phys. **54**(2), 526–537 (2015)
41. Chen, J., Zhu, Z., Fu, C., et al.: A fast image encryption scheme with a novel pixel swapping-based confusion approach [J]. Nonlinear Dyn. **77**(4), 1191–1207 (2014)
42. 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]. J. Vis. Commun. Image Represent. **40**, 51–57 (2016)
43. Wang, S., Sang, J., Song, X., et al.: Least significant qubit (LSQb) information hiding algorithm for quantum image [J]. Measurement **73**, 352–359 (2015)