Multimedia Tools and Applications (2020) 79:29243–29263
https://doi.org/10.1007/s11042-020-09542-w

A novel hyper-chaotic image encryption scheme based on quantum genetic algorithm and compressive sensing

Guangfeng Cheng[1] · Chunhua Wang[1] · Cong Xu

Received: 27 April 2020 / Revised: 27 July 2020 / Accepted: 4 August 2020 /
Published online: 10 August 2020

Abstract

Over the last few years, lots of chaotic image encryption schemes have been proposed. However, most of the schemes are permutation-diffusion architectures which still have some shortcomings, such as weak key streams, small key spaces, small information entropy, and so on. To eliminate the above weaknesses, in this paper, we propose a hyper-chaotic image encryption scheme based on quantum genetic algorithm (QGA) and compressive sensing (CS), which is a new image encryption scheme and has not been proposed so far. Firstly, QGA can update the population with the quantum rotation gate, which can enhance the randomness of the population and avoid falling into local optimum. Then compressive sensing technology is used to reduce data storage and speed up the encryption and decryption process. Moreover, we utilize the SHA-512 hash function of the plain image to calculate the initial values of the hyper-chaotic system, which is capable of enhancing the relationships between encryption schemes and plain images. The simulation experiments and security analysis reveal that the proposed scheme is more efficient in resisting statistical attack and plaintext attack and shows better performance in peak signal-to-noise ratio (PSNR) and information entropy compared with other image encryption schemes based on chaos theory.

Keywords Hyper-chaotic system · Image encryption · Quantum genetic algorithm (QGA) · Compressive sensing (CS)

1 Introduction

With the rapid development of network science and digital communication technology, the work and life of people are becoming more and more convenient. As a result, digital media for

✉ Chunhua Wang
wch1227164@hnu.edu.cn

[1] College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, People's Republic of China

information transmission, such as images, videos and so on, are widely adopted in computer networks in various civil and military fields. However, when people conveniently use digital image processing technology for data transmission, the problem of image information security has also appeared, which attracts the cautious attention of many researchers, therefore they study the image encryption technology carefully [2–8, 12–16, 18–20, 22, 23, 25, 27–35, 37, 39–41]. The existing results reveal the encryption schemes based on chaos theory have better performance than traditional encryption algorithms on image processing [1, 24], because chaotic systems or maps can show better ability on randomness and ergodicity for data with high sensitivity to control parameters and initial conditions [17, 36, 38]. Nowadays chaotic image encryption has become an attractive research area.

As the image encryption schemes based on chaotic systems become more and more popular, many such image encryption schemes have been proposed [2–8, 12–16, 18–20, 22, 23, 25, 27–35, 37, 39–41]. For example, some image encryption schemes based on S-box structures were proposed [3, 7, 18, 25, 35, 41]. But the image encryption schemes based on S-box structures have the shortcomings of small key space and simple encryption structure [35]. To eliminate the drawbacks, some image encryption schemes based on bit-plane or bit-level were proposed one after another [2, 16, 19, 29, 31, 37]. In [37], the authors developed an image encryption scheme based on three-dimensional bit matrix permutation. An image is considered as a natural three-dimensional (3D) bit matrix (width, height, and bit length). In the permutation stage, a random visiting mechanism to the bit level of the plain-image was proposed which replaced traditional sequential visiting to the plain-image. However, Wu et al. found that the image encryption scheme based on three-dimensional bit matrix permutation cannot resist chosen plaintext attack effectively [29]. Then, an enhanced algorithm was proposed to overcome the presented drawbacks and ensure a secure image communication. Due to the cross-development of biotechnology and computer technology, some scholars studied the image encryption schemes based on DNA computing [4, 12–14, 27, 30, 34]. The authors in [12] proposed an image encryption scheme using high-dimensional chaotic systems and cycle operation for DNA sequences which are projected to diffuse the pixel values of the image. In [14], an encryption algorithm combining fractional order hyper chaotic Chen system and DNA operations was proposed. Besides, some chaos-based image encryption schemes using cellular automata (CA) were developed [15, 20, 23, 28, 32]. In [32], the authors proposed a color image encryption scheme based a non-uniform cellular automata framework, which consists of confusion and diffusion steps. Nevertheless, Li et al. found out some security drawbacks about the encryption scheme based a non-uniform cellular automata framework [15]. By using specific chosen plaintexts, key streams can be obtained accurately. The results mean that the encryption scheme vulnerable to chosen plaintext attack. The authors in [20] proposed a highly secure image encryption scheme for secure image communication and storage. The scheme is based on a chaotic skew tent map and CA. Moreover, some researchers have designed image encryption schemes by combining chaotic systems and compressive sensing (CS) [5, 8, 40]. In [5], CS is utilized to compress and encrypt the confused image to minimize data and save the transmission time over the network. The measurement matrix of CS is produced by a memristive chaotic system. In [22], a reversible image encryption scheme using the hyper-chaotic feeded genetic algorithm (GA) was introduced. However, the scheme based on traditional GA is easy to trap in local optimum [26], which results in the encrypted image with inadequate security. Thus, the adversary may obtain useful information by cracking the scheme.

In order to address the above issues, this paper presents a new hyper-chaotic image encryption scheme based on quantum genetic algorithm (QGA) and compressive sensing. In the proposed scheme, each pixel of an image is encoded by the probability amplitude and updated by the quantum rotation gate. Besides, to ensure the real-time performance, we adopt CS to reduce data storage and speed up the encryption and decryption process. To guarantee that our scheme is highly sensitive to the plain image, we use the SHA-512 hash function value of the plain image to calculate the initial values of the hyper-chaotic system.

Our contributions are as follows.

(1) The image encryption scheme based on QGA has not been proposed so far. In addition, our proposed scheme can let the produced cipher images to be optimized by QGA and provides a mechanism for the legal receiver to be able to securely decrypt them.

(2) In contrast of the above image encryption schemes which only use the binary-encoded data for pixel value, each pixel of an image is encoded by the probability amplitude in this paper. If we want to obtain an image, we must decode qubits correctly. Therefore, this kind of data encoding method can greatly improve the data security of the encryption scheme.

(3) According to the experimental analyses applied to measure the new scheme, the results illustrate that in contrast of other hyper-chaotic image encryption schemes, the proposed scheme possesses better encryption performances.

The rest of this paper is organized as follows. Section 2 introduces the related knowledge. In Section 3, the details of our proposed cryptosystem are presented. The experimental results and security analysis are given in Section 4. Finally, conclusion is drawn in Section 5.

2 Preliminaries

2.1 The hyper-chaotic system

Chaotic systems have been used widely in various communication systems because of its high sensitivity to initial values and system parameters. Furthermore, a hyper-chaotic system has more complex dynamic behavior and can reduce the transient effect. In our proposed scheme, a hyper-chaotic system is adopted [21]:

$$\begin{cases} \dot{x} = a(y-x) + yz \\ \dot{y} = bx-y-xz + w \\ \dot{z} = xy-cz \\ \dot{w} = dw-xz \end{cases} \tag{1}$$

where x, y, z and w are state variables and a, b, c and d are real constant system parameters of the chaotic system (1). When $a = 10$, $b = 8/3$, $c = 55$, $d = 1.3$, the system is hyper-chaotic.

2.2 Quantum genetic algorithm (QGA)

QGA is an intelligent optimization algorithm combining GA and quantum features [11]. In contrast to GA, QGA has three obvious advantages. Firstly, QGA uses quantum bits instead of using monotonous binary bits to encode feasible solutions in the solution space. Secondly, QGA adds the operation of chromosome renewal through the quantum rotation gate instead of using simple crossing and mutating. Thirdly, each qubit is an indeterminate state, which belongs to the superposition states of '0' and '1', so the decoding operation will be different from the encoding operation.

2.2.1 Encoding operation of qubit

In QGA, instead of a definite value, the gene on the chromosome is expressed by the probability amplitude. In this way, each qubit may represent '0' or '1' and is also likely to represent the superposition state of '0' and '1'. As a result, the encoding method of qubits can contain more information than the conventional GA in equal encoding length [11]. A qubit is expressed as follows:

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix} \tag{2}$$

where α and β are complex numbers, representing the probability amplitudes of '0' and '1' respectively. In addition, α and β satisfy the following formula:

$$\alpha^2 + \beta^2 = 1 \tag{3}$$

Therefore, the state of a qubit can be expressed as:

$$\Psi = \alpha|0 + \beta|1 \tag{4}$$

where α and β are the probability amplitudes, Ψ is the state of a qubit.

2.2.2 Quantum rotation gate

In QGA, the chromosome in the way of the above encoding method is no longer a certain state. The operation to generate the next generation cannot continue to adopt the traditional operations simply including selection, crossover, and mutation. However, the quantum rotation gate is adopted to act on the states of the quantum chromosome and makes them interfere with each other. Moreover, the quantum rotation should be reversible, which ensures the encryption process is reversible. As a result, the distribution of probability amplitude varies with their phases respectively. The quantum rotation gate is described as follows:

$$U = \begin{bmatrix} cos\theta & -sin\theta \\ sin\theta & cos\theta \end{bmatrix} \tag{5}$$

where θ represents the rotation phase.

Therefore, the update process of each qubit is realized by Eq. (6).

$$\begin{bmatrix} \alpha^{'} \\ \beta^{'} \end{bmatrix} = U \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \tag{6}$$

where $\alpha^{'}$ and $\beta^{'}$ represent the probability amplitudes of a qubit after the action of quantum revolving gate. The inverse process is described by Eq. (7).

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = U^{-1} \begin{bmatrix} \alpha^{'} \\ \beta^{'} \end{bmatrix} \tag{7}$$

where U^{-1} is the inverse matrix of U.

2.3 Compressive sensing (CS)

Compressive sensing, introduced by Donoho [9], is able to be utilized to encrypt and compress images in a single step, where the measurement matrix, as the key, is shared between the sender and the receiver. Moreover, CS theory can effectively reduce the data storage and promote the encryption process.

Assume that a two-dimensional signal x of size $N \times N$ with K-sparse is described by

$$x = \psi f \tag{8}$$

where f represents the transform coefficient vector. ψ is an orthogonal basis of size $N \times N$. Next, the compression signal y is handled by a measurement matrix Φ of size $M \times N$, shown as

$$y = \Phi x = \Phi \psi f = \eta f \tag{9}$$

where $\eta = \Phi\psi$. To accurately reconstruct x from y, the optimization problem should be solved by Eq. (10).

$$min\|f\|_1 \text{ s.t.} y = \eta f \tag{10}$$

The basic model of CS mainly comprises three major steps: sparse representation of signal, compression measurement and reconstruction of signal. During image processing, sparse representation methods include discrete Fourier transform (DFT), discrete cosine transform (DCT), or discrete wavelet transform (DWT) matrix [8], etc. In terms of compression measurement, some measurement matrices are proposed, including Gaussian random matrix, partial orthogonal matrix, Hadamard matrix and circular matrix. And circular matrix is adopted in this paper. For signal reconstruction, some algorithms are introduced such as orthogonal matching pursuit (OMP) algorithm, subspace pursuit (SP) algorithm and smooth l_0 norm (SL_0) algorithm [40]. In this paper, we utilize the SL_0 algorithm to recover the signal with the original size.

Particularly, the circular matrix, where each row is controlled by the previous row moving to the right, is adopted as measurement matrix [5]. Moreover, the first-row vector is produced by the hyper-chaotic system. The measurement matrix Φ of size $M \times N$ is described as

$$\begin{cases} \Phi(i,1) = \mu \times \Phi(i-1,\mathrm{N}) \\ \Phi(i,2:\mathrm{N}) = \Phi(i-1,1:N-1) \end{cases} \tag{11}$$

where $2 \le i \le M$, $\mu > 1$. Due to the adoption of the hyper-chaotic system, which is highly sensitive to the initial values and system parameters, in case of the initial values or system parameters are changed lightly, we can obtain different measurement matrices, thereby generate completely different compression results.

3 Proposed cryptosystem

3.1 The generation of initial values of the chaotic system

In some previous papers, there are weak relationships between encryption schemes and plain images, which may lead to resisting the plaintext attack poorly. To overcome the issue, we utilize the SHA-512 hash function of the original image to calculate the initial values of the hyper-chaotic system. Firstly, before the plain image is encrypted, the 512-bit hash value of the plain image is computed as the secret key K. Then K is divided into 64 blocks k_1, k_2, …, k_{64} and each block with 8 bits is converted to a decimal digit. Next, the initial values of the chaotic system are calculated by the following steps.

Step 1: Convert K into 64 decimal numbers k_1, k_2, …, k_{64}, and then obtain h_1, h_2, h_3, h_4, by Eq. (12).

$$\begin{cases} h_1 = \dfrac{(k_1 \oplus k_2 \oplus k_3 \oplus \ldots\ldots \oplus k_{16})}{256} + t_1 \\ h_2 = \dfrac{(k_{17} \oplus k_{18} \oplus k_{18} \oplus \ldots\ldots \oplus k_{32})}{256} \times t_2 \\ h_3 = \dfrac{(k_{33} \oplus k_{34} \oplus k_{35} \oplus \ldots\ldots \oplus k_{48} \oplus t_3)}{256} \\ h_4 = \dfrac{\sum\limits_{i=49}^{64} \left((-1)^i \times k_i\right)}{256} \end{cases} \tag{12}$$

where t_1, t_2, t_3 are parts of secret keys, $x \oplus y$ is the XOR operation between x and y.

Step 2: Utilize h_1, h_2, h_3, h_4 to calculate x_0, y_0, z_0, w_0 as the initial values of the chaotic system by Eq. (13).

$$\begin{cases} x_0 = \mathrm{mod}\left(\mathrm{abs}\left((h_1 + h_4) * 10^8\right), 1\right) \\ y_0 = \mathrm{mod}\left(\mathrm{abs}\left((h_2 + h_3) * 10^8\right), 1\right) \\ z_0 = \mathrm{abs}(h_3) - \mathrm{floor}(h_3) \\ w_0 = \mathrm{abs}(h_4) - \mathrm{floor}(h_4) \end{cases} \tag{13}$$

where mod(x,y) denotes the value of the remainder of x divided by y, abs(x) returns the absolute value of x, and floor(x) is the largest integer smaller than x.

3.2 The generation of measurement matrix for CS

In this paper, the circular matrix, where each row is produced by the previous row moving to the right, is adopted as the measurement matrix. The measurement matrix Φ of size $M \times N$ is generated by the following steps:

Step 1: Utilize the initial values (x_0, y_0, z_0, w_0) generated in Section 3.1 to iterate the hyper-chaotic system for $T_1 + N$ times. To avoid the transient effect, we discard the former T_2 values. Thereby we obtain four chaotic sequences X, Y, Z and W and each sequence consists of N elements.

Step 2: Obtain XX, YY, ZZ and WW by computing X, Y, Z and W respectively according to Eq. (14).

$$\begin{cases} XX(i) = \mathrm{mod}\left(\mathrm{abs}(X(i) - Y(i)) \times 10^8, 1\right) \\ YY(i) = \mathrm{mod}\left(\mathrm{abs}(Y(i) - Z(i)) \times 10^8, 1\right) \\ ZZ(i) = \mathrm{mod}\left(\mathrm{abs}(X(i) + Y(i) + Z(i)) \times 10^8, 1\right) \\ WW(i) = \mathrm{mod}\left(\mathrm{abs}(W(i)) \times 10^8, 3\right) \end{cases} \tag{14}$$

where $X(i)$, $Y(i)$, $Z(i)$ and $W(i)$ are the ith elements of X, Y, Z and W, respectively. $XX(i)$, $YY(i)$, $ZZ(i)$ and $WW(i)$ are the ith element of XX, YY, ZZ and WW, respectively, $i = 1, 2, \ldots, N$.

Step 3: Obtain one sequence Q of length N by selecting the elements from the three sequences XX, YY and ZZ according to the sequence WW. The detail is described by Eq. (15).

$$Q(i) = \begin{cases} XX(i), \text{if } WW(i) = 0 \\ YY(i), \text{if } WW(i) = 1 \\ ZZ(i), \text{if } WW(i) = 2 \end{cases} \tag{15}$$

where $XX(i)$, $YY(i)$, $ZZ(i)$ and $WW(i)$ are the ith element of XX, YY, ZZ and WW, respectively, $i = 1, 2, \ldots, N$.

Step 4: Let the original row vector is equal to the sequence Q, that is to say, $\Phi(1) = Q$. Finally, the measurement matrix Φ of size $M \times N$ is constructed by Eq. (11).

3.3 Encryption process

The flow chart of the encryption scheme is presented as Fig. 1. The details of the encryption process are presented as follows:

Step 1: We suppose that the size of the original image P is $N \times N$. According to DCT, we obtain the sparse coefficient matrix P_1 of size $N \times N$ by the sparsification of the original image P.

Step 2: Get the initial values (x_0, y_0, z_0, w_0) of the hyper-chaotic system from the original image as described in Section 3.1.

Step 3: Construct the measurement matrix Φ of size $M \times N$ as presented in Section 3.2, where $M = N \times CR$ and CR represents compression ratio of the plain image.

Step 4: Obtain the matrix P_2 of size $M \times N$ by compressing P_1 ($N \times N$) according to Eq. (9). In other words, the size of population is $L = M \times N$ in QGA.

Step 5: Here every value in P_2 is encoded by 8 bits, and every bit is encoded by a probability amplitude vector including two elements α and β. Firstly, rearrange P_2 into the 1-D vector P_3 with length L. Then utilize the above initial values (x_0, y_0, z_0, w_0) to iterate the hyper-chaotic system for $8 \times L \times R + T_2$ times. R is the number of genetic rounds. To avoid the transient effect, we discard the former T_2 values. Thereby we get the R chaotic sequences with the length of $8 \times L$: $S_r = \{s_{r,1}, s_{r,2}, s_{r,3} \ldots s_{r,8L}\}$, where r is the range of 1 to R. Next, we convert every value in P_3 into a binary format which is added into the binary matrix B with the size of $8 \times L$. As mentioned in Section 2.2.1, the encoding length of each qubit is 2. To construct the initial population, α and β are added into the probability amplitude matrix H of size $16 \times L$ by Eq. (16).

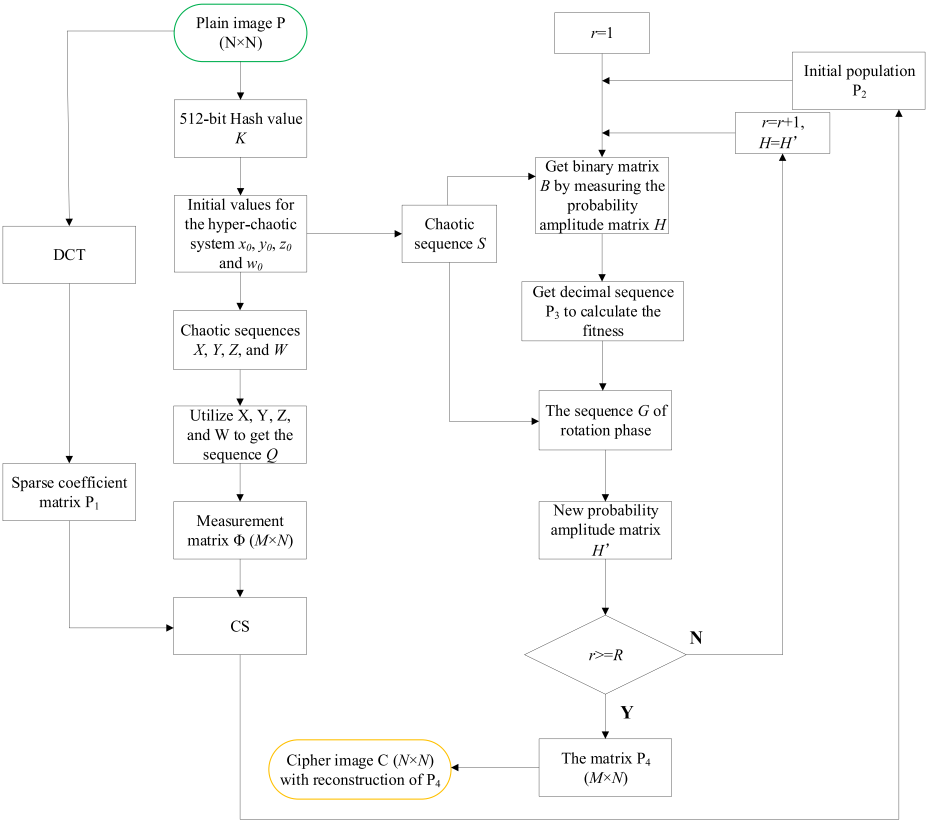

Plain image P (N×N)
512-bit Hash value K
Initial values for the hyper-chaotic system x_0, y_0, z_0 and w_0
Chaotic sequences X, Y, Z, and W
Utilize X, Y, Z, and W to get the sequence Q
Measurement matrix Φ (M×N)
CS
DCT
Sparse coefficient matrix P1
Chaotic sequence S
r=1
Initial population P2
r=r+1, H=H'
Get binary matrix B by measuring the probability amplitude matrix H
Get decimal sequence P3 to calculate the fitness
The sequence G of rotation phase
New probability amplitude matrix H'
r>=R
N
Y
The matrix P4 (M×N)
Cipher image C (N×N) with reconstruction of P4

Fig. 1 the flow chart of the encryption scheme

$$H(i) = \begin{cases} \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \text{if } B(i) = 0 \\ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \text{if } B(i) = 1 \end{cases} \tag{16}$$

where $i = 1, 2, \ldots, 8L$. After that, we begin the QGA loop by the following steps:

Step 5.1: Set $r = 1$, where r is the number of QGA rounds.

Step 5.2: The probability amplitude matrix H is measured by Eq. (17). As a result, we can get a binary matrix B.

$$B(i) = \begin{cases} 1, \text{if } H(i,1)^2 \leq S_r(i) \leq H(i,2)^2 \\ 0, \mathit{otherwise} \end{cases} \tag{17}$$

Step 5.3: Convert the binary matrix B into the decimal sequence P_3, and then calculate the fitness of P_3. In this paper, the fitness function of the sequence is calculated by the entropy.

Step 5.4: Construct the sequence G of rotation phase by computing the value and direction of the rotation phase for every qubit by Eq. (18).

$$G(i)=\begin{cases} S_r(i)\times\pi, \text{if } B(i)=1 \text{ and } H(i,1)\times H(i,2)>0 \\ -S_r(i)\times\pi, \text{if } B(i)=0 \text{ and } H(i,1)\times H(i,2)<0 \\ \operatorname{sign}(S_r(i)-0.5)\times S_r(i)\times\pi, \textit{otherwise} \end{cases} \tag{18}$$

where $i = 1, 2, \ldots, 8L$. sign(x) correspondingly returns 1, −1 or 0 if the x is positive, negative or zero, respectively. In this paper, we define that the phase of the qubit rotates clockwise if the phase is negative. Otherwise, the phase of the qubit rotates counterclockwise.

Step 5.5: After obtaining the sequence of rotation phase, we can obtain the new probability amplitude matrix H' by Eq. (5) and Eq. (6).
Step 5.6: Set $r = r + 1$ and $H = H'$, then loop executes Step 5.2 to Step 5.6 R times, and the 1-D decimal sequence P_3 is obtained.

Step 6: Rearrange P_3 into the matrix P_4 of size $M \times N$. Then P_4 is reconstructed with the SL_0 algorithm and the cipher image C is obtained.

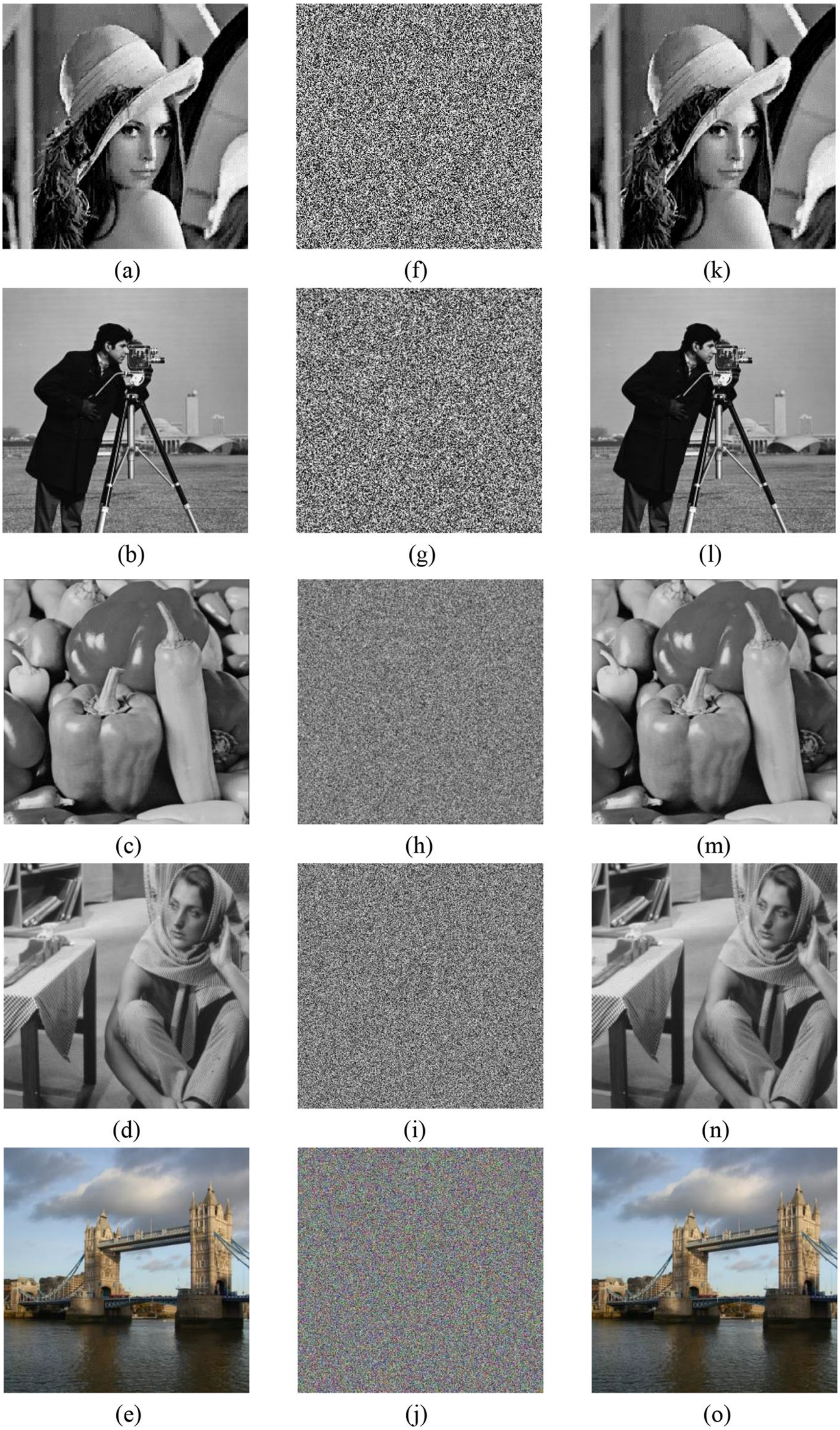
3.4 Decryption process

In this paper, the decryption process is the inverse operation of the encryption process. Before the decryption, the receiver should obtain secret keys from the sender. Secret keys include the 512-bit hash value K, the parameters (μ, t_1, t_2, t_3), discarding numbers T_1 and T_2 of chaotic sequences, the compression ratio CR and the total number R of QGA rounds. After that, the detailed steps of the decryption process are introduced as follows:

Step 1: The initial values (x_0, y_0, z_0, w_0) of the hyper-chaotic system and the measurement matrix Φ are calculated as presented in Section 3.1 and Section 3.2 respectively.
Step 2: Obtain the sparse coefficient matrix C_1 of size $N \times N$ by DCT of the cipher image C.
Step 3: C_1 of size ($N \times N$) is compressed by Eq. (9), and then we can obtain the matrix C_2 of size $M \times N$. That is to say, the size of the population in QGA is $L = M \times N$.
Step 4: Get a binary matrix B and a probability amplitude matrix H by initializing the population. Then we perform the inverse process of QGA.

Step 4.1: Set $r = 1$.
Step 4.2: The binary matrix B is obtained by measuring the probability amplitude matrix H according to Eq. (17).
Step 4.3: Get the sequence G of rotation phase by Eq. (19).

$$G(i)=\begin{cases} S_{R+1-r}(i)\times\pi, \text{if } B(i)=1 \text{ and } H(i,1)\times H(i,2)>0 \\ -S_{R+1-r}(i)\times\pi, \text{if } B(i)=0 \text{ and } H(i,1)\times H(i,2)<0 \\ \operatorname{sign}(S_{R+1-r}(i)-0.5)\times S_{R+1-r}(i)\times\pi, \textit{otherwise} \end{cases} \tag{19}$$



(a) (f) (k)

(b) (g) (l)

(c) (h) (m)

(d) (i) (n)

(e) (j) (o)

◀ **Fig. 2:** **a-e** the plain images of Lena (256×256), Cameraman (256×256), Pepper (512×512), Barbara (512×512), London (512×512); **e-h** the cipher images of (a)-(e) respectively; **i-l** the decrypted images for (e)-(h) respectively.

where S is constructed as presented in Section 3.3, $i = 1, 2, \ldots, 8L$. sign(x) returns 1, −1 or 0 if the x is positive, negative or zero, respectively.

Step 4.4: Obtain the new probability amplitude matrix H' by Eq. (5) and Eq. (7).
Step 4.5: Set $r = r + 1$, and $H = H'$, then loop executes Step 4.2 to Step 4.5 R times, and the 1-D decimal sequence C_3 is achieved.

Step 5: After rearranging C_3 into the matrix C_4 of size $M \times N$, we reconstruct C_4 with the SL_0 algorithm. Finally, the plain image P is obtained.

4 Simulation results and security analysis

4.1 Simulation results

The simulation process is carried out by MATLAB on the computer to examine the validity and reliability of the proposed scheme given above. The plain images are tested as shown Fig. 2. For color images, R, G, and B three components are encrypted respectively. After the encryption process, they will be combined to obtain an encrypted color image.

4.2 Statistical analysis

4.2.1 Histogram

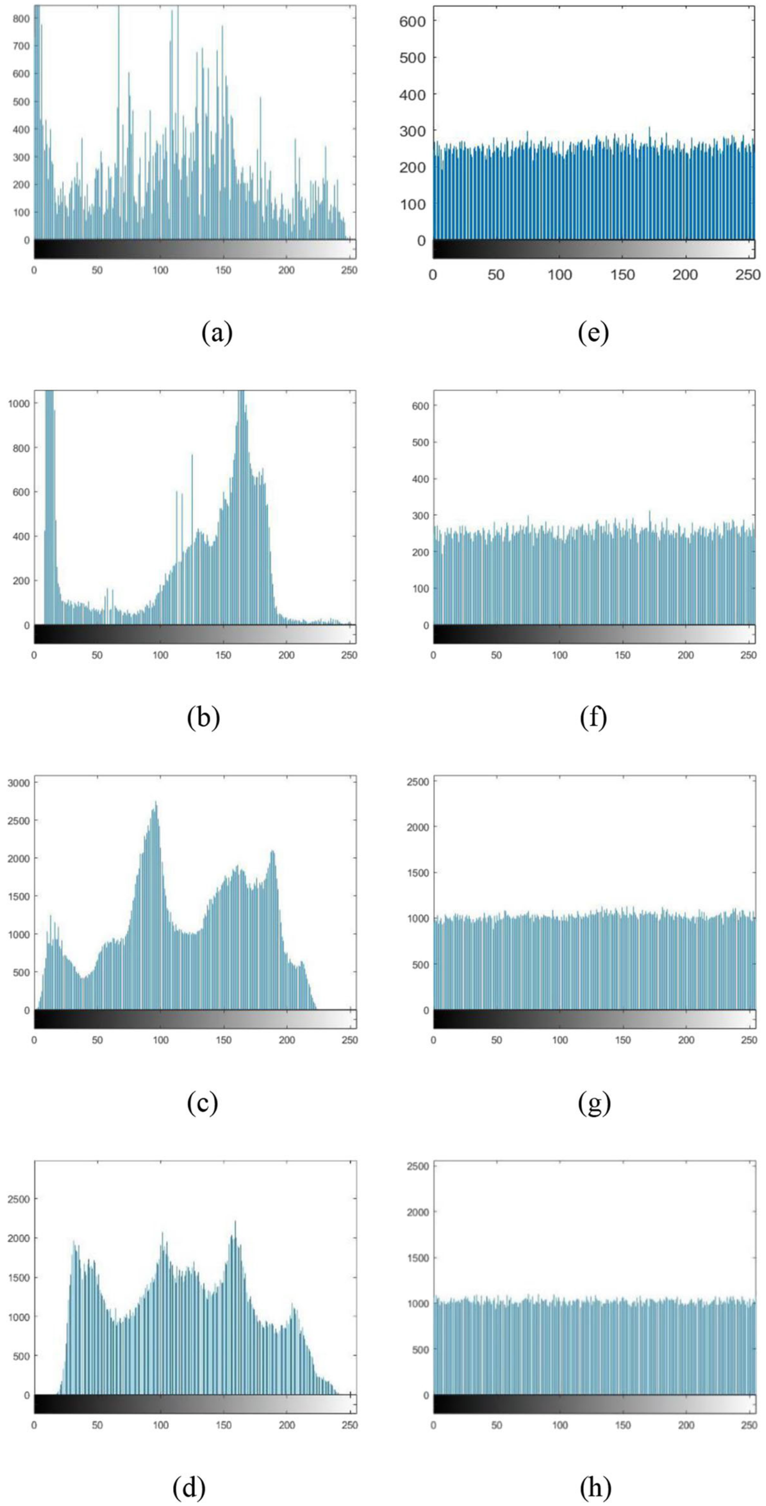
The histogram demonstrates the statistical characteristics and distribution information of pixel value in an image. To prevent the attacker from getting any meaningful information, the histogram of an ideal image after encrypted should be uniform and be completely different from the histogram of plaintext image.

The experimental results of histograms are shown in Fig. 3. The results illustrate that the histogram of each plain image has a specific distribution before encrypted. After the encryption process, the histogram of each cipher image is evenly and almost the same as each other. As a result, the enemy is unlikely to get the original image from the statistical characteristics of the cipher image even any valuable information.

4.2.2 Correlation of adjacent pixels

After the process of a secure encryption scheme, the cipher image should overcome the shortcoming which is a high correlation between two adjacent pixels of the original image in three directions. The correlation coefficients are calculated by formulae (20–23):

$$r_{xy} = cov(x, y) / \sqrt{D(x)D(y)} \tag{20}$$


0 100 200 300 400 500 600 700 800
0 50 100 150 200 250
0 100 200 300 400 500 600
0 50 100 150 200 250
0 200 400 600 800 1000
0 50 100 150 200 250
0 100 200 300 400 500 600
0 50 100 150 200 250
0 500 1000 1500 2000 2500 3000
0 50 100 150 200 250
0 500 1000 1500 2000 2500
0 50 100 150 200 250
0 500 1000 1500 2000 2500
0 50 100 150 200 250
0 500 1000 1500 2000 2500
0 50 100 150 200 250

(a) (e)

(b) (f)

(c) (g)

(d) (h)

◀ **Fig. 3:** **a**-**d** the histogram of plain images of Lena (256×256), Cameraman (256×256), Pepper (512×512), Barbara (512×512); **e**-**h** the histogram of cipher images of Lena (256×256), Pepper (512×512), London (512×512), respectively.

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{21}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \tag{22}$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)) \tag{23}$$

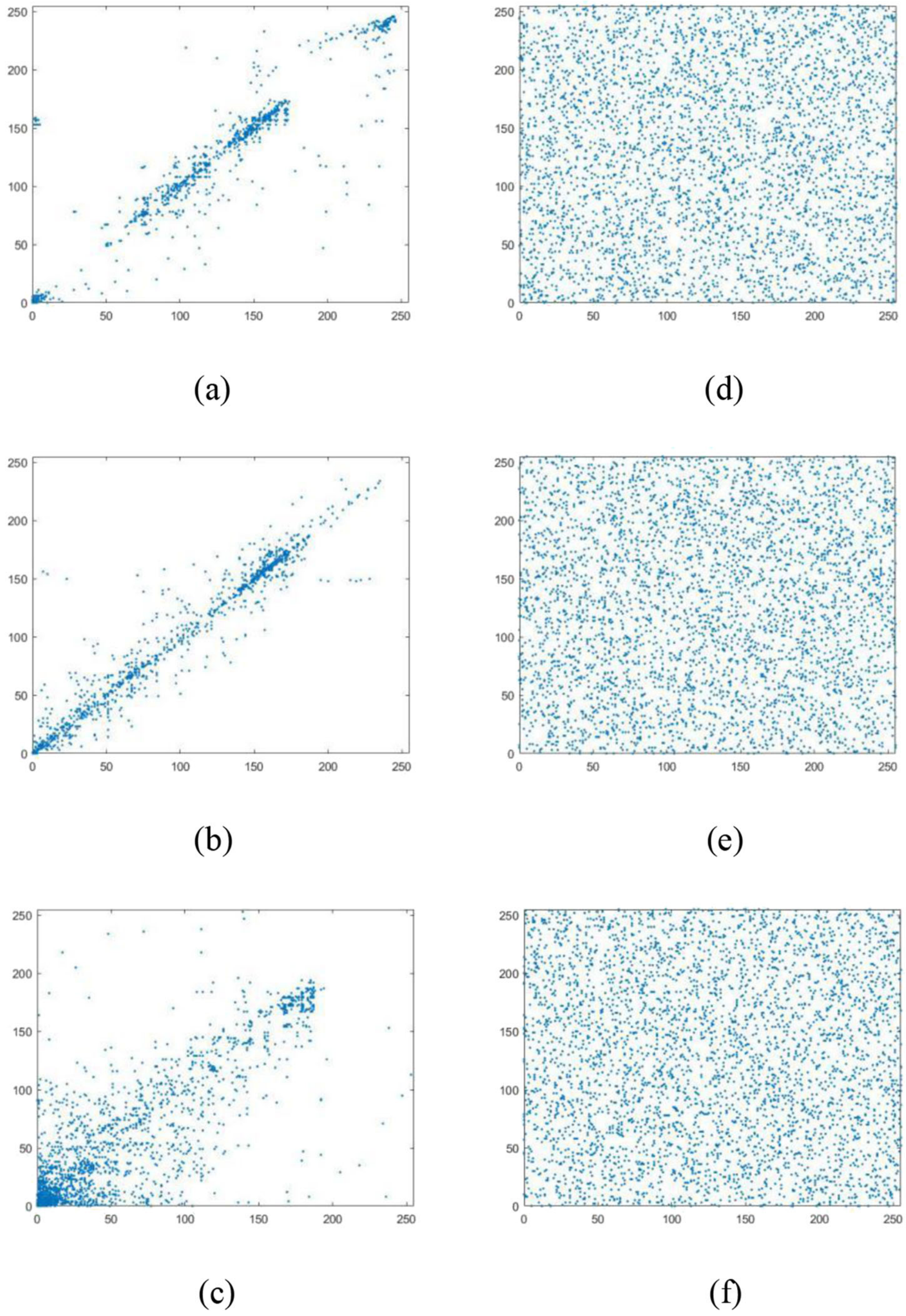
where, in an image, x and y are gray values of two adjacent pixels, $E(x)$ denotes the average of all pixel values, $D(x)$ shows the variance of all pixel values, $cov(x,y)$ is the corresponding covariance. We analyze the correlation of adjacent pixels by selecting 5000 pairs of two-adjacent pixels in plain image and corresponding cipher image. After that, the correlation coefficients are calculated in three different directions (horizontal, vertical and diagonal). In this part, we take the original image of Lena as an example. The results of the correlation coefficients in different directions are shown in Fig. 4. Apparently, the original image has high correlation coefficients regardless of horizontal, vertical or diagonal direction. However, the correlation coefficients of the cipher image are very low. In addition, the correlation distribution among adjacent pixels of the encrypted image is more uniform than the plain image. Besides, the correlation coefficients of cipher image Lena compared with other schemes [22, 31, 33, 34] are given in Table 1, we can see that the correlation coefficients among adjacent pixels in the cipher image in our proposed scheme are lower than that in the plain image. Hence, the proposed scheme has the ability of resisting the statistical attack.

4.3 Sensitivity analysis

4.3.1 Differential attack

To avoid the differential attack by the enemy, the secure encryption scheme should have the ability to guarantee that there will be much difference between encrypted images with any tiny changes in the original image. Here we use two standards to evaluate the effect for differential attack analysis. They are Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) which are defined respectively as follows:

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M \times N} \times 100\% \tag{24}$$



(a) (d)

(b) (e)

(c) (f)

Fig. 4 Correlation distributions of "Lena" (256×256): (**a**) horizontal of plain image; (**b**) vertical of plain image; (**c**) diagonal of plain image; (**d**) horizontal of cipher image; (**e**) vertical of cipher image; (**f**) diagonal of cipher image

Table 1 Correlation coefficients between adjacent pixels of plain image and cipher image

Image	Encryption scheme	Direction		
		Horizontal	Vertical	Diagonal
Plain image(Lena)		0.9567	0.9611	0.9169
Cipher image(Lena)	Ours	0.0076	0.0093	− 0.0160
Cipher image(Cameraman)		0.0064	0.0082	0.0091
Cipher image(Pepper)		0.0037	− 0.0014	0.0073
Cipher image(Barbara)		0.0053	0.0035	− 0.0017
Cipher image(Lena)	Bit level encryption	−0.0230	0.0019	− 0.0034
Cipher image(Lena)	DNA encryption	−0.0033	0.0094	0.0021
Cipher image(Lena)	HFGA encryption	0.000006	0.000002	0.000012
Cipher image(Lena)	dynamic diffusion encryption	−0.0156	− 0.0022	− 0.0028

$$UACI = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} \frac{\left|C'(i,j) - C(i,j)\right|}{255}}{M \times N} \times 100\% \tag{25}$$

where M and N are the numbers of row and column of the tested image respectively, C is the corresponding cipher image of the original image and C' is the encrypted image of the original image with a slight change. D is described by formula (26):

$$D(i,j) = \begin{cases} 1, \text{if } C(i,j) \neq C'(i,j) \\ 0, \text{if } C(i,j) = C'(i,j) \end{cases} \tag{26}$$

In the testing process, we use the original images Lena to analyze the sensitivity of the plain image. The NPCR and UACI are shown in Table 2. The experiment results indicate that the value of NPCR and UACI in our proposed scheme are 99.65% and 33.64% respectively, and they are both closer to the theoretical value than most of the other schemes [22, 31, 33, 34]. Therefore, our proposed scheme can effectively resist differential attack.

4.3.2 Key sensitivity

In security analysis, key sensitivity plays a significant role in resisting the brute force attack. To achieve this goal, the secure scheme must be sensitive to the key. On one hand, a slight change of the secure key should lead to a completely different cipher image. On the other

Table 2 NPCR and UACI analysis

Scheme	Image	NPCR (%)	UACI (%)
Ours	Lena	99.65	33.64
	Cameraman	99.73	33.72
	Pepper	99.84	33.68
	Barbara	99.63	33.59
Bit level encryption	Lena	99.62	33.51
DNA encryption	Lena	99.61	32.95
HFGA encryption	Lena	99.98	33.53
dynamic diffusion encryption	Lena	99.61	33.46

hand, the encrypted image cannot be decrypted correctly with the key with a tiny change in the decryption process.

For example, there is a tiny difference in one of the secret keys. The parameter μ of original keys is 1.257 while the parameter μ of modified keys is $1.257 + 10^{-14}$. In the encryption process, we use the original keys to encrypt the original image. In the decryption phase, we use the original keys and the modified keys to decrypt the cipher image respectively. The results of the key sensitivity analysis for the proposed scheme are shown in Fig. 5. Fig. 5(a) is the original image and Fig. 5(b) is the corresponding encrypted image. The decrypted image with correct keys is shown in Fig. 5(c). While Fig. 5(d) is the decrypted image with modified keys. Obviously, with the modified key which has a slight change, the decrypted image is completely different from the original image. Therefore, our proposed scheme is sensitive enough to the secure key.

4.4 Information entropy

Information entropy is an important feature of the randomness of an image. When the entropy of a gray image is 8, we define the image as a real random image. The information entropy is described as the following formula:

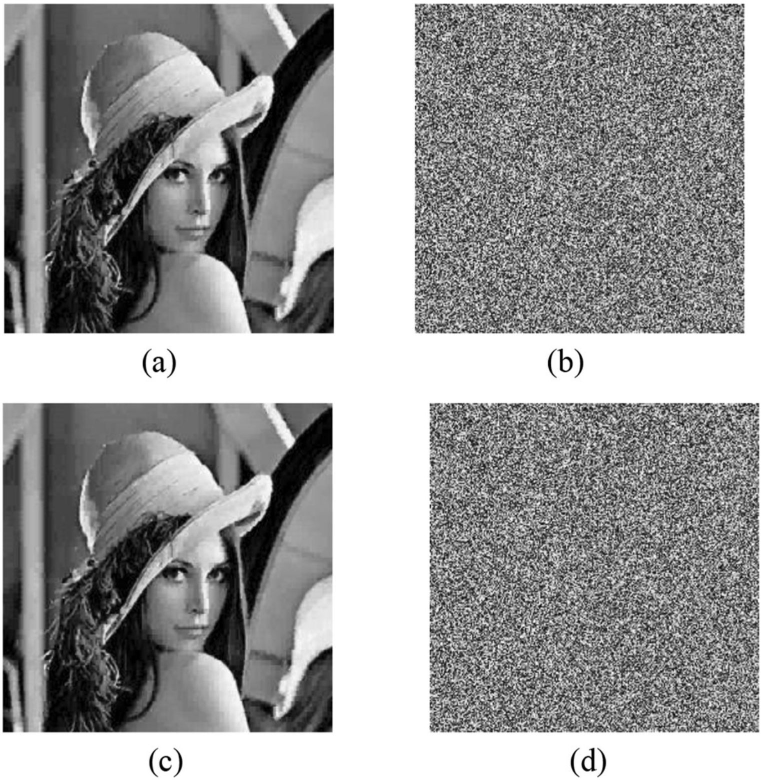


Fig. 5. **a** plain image, **b** cipher image, **c** decrypted image with the correct secret key, and **d** decrypted image with the modified secret key.

Table 3 Information entropy

Scheme	Image	Plain image	Cipher image
Ours	Lena	7.5827	7.9995
	Cameraman	6.9719	7.9993
	Pepper	7.5937	7.9994
	Barbara	7.6321	7.9993
Bit level encryption	Lena		7.9974
DNA encryption	Lena		7.9993
HFGA encryption	Lena		7.9994
dynamic diffusion encryption	Lena		7.9979

$$H = -\sum_{i=0}^{2^N-1} p(m_i) log_2 p(m_i) \tag{27}$$

where N is the number of bits for m_i and is equal to 8. And $p(m_i)$ is the probability of m_i. Hence, the closer to the theoretical value 8 the information entropy, the more uniform the distribution of a gray image.

In the information entropy test, we calculate the value of information entropy for the encrypted image compared with the original image. Besides, we make a comparison between our proposed scheme and other schemes. The results of the information entropy are shown in Table 3. We can see that in our proposed scheme, the information entropy of different cipher images is greater than the plain image respectively and closer to the theoretical value 8. Moreover, for the plain image of Lena, the cipher image of the proposed scheme has a greater information entropy than the cipher image of other schemes [22, 31, 33, 34]. Therefore, it is proved that the scheme shows better performance than others in avoiding the information entropy attack.

4.5 Robustness analysis

4.5.1 Peak signal-to-noise ratio analysis

As a significant feature for the security of an encryption scheme, the *PSNR* (peak signal-to-noise ratio) should be as small as possible. *PSNR* is described as follows:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} [P(i,j) - C(i,j)]^2 \tag{28}$$

$$PSNR = 10 \times lg\left(\frac{I_{max}^2}{MSE}\right) \tag{29}$$

Table 4 PSNR for the encryption

Image	Ours	Bit level encryption	DNA encryption	HFGA encryption	dynamic diffusion encryption
Lena	7.9161	9.1772	9.3228	8.9534	8.4100
Cameraman	8.4372	8.9762	9.2664	8.6912	9.0835
Pepper	8.8626	9.0442	8.9327	8.7349	8.9448
Barbara	8.7594	9.3658	9.1872	9.0784	9.2196

where P is the original image and C is the corresponding cipher image. I_{max}^2 represents the maximum of the pixel values in the image. The results of the *PSNR* test shown in Table 4 reveal that compared with other schemes [22, 31, 33, 34], our scheme is capable of resisting noise attack.

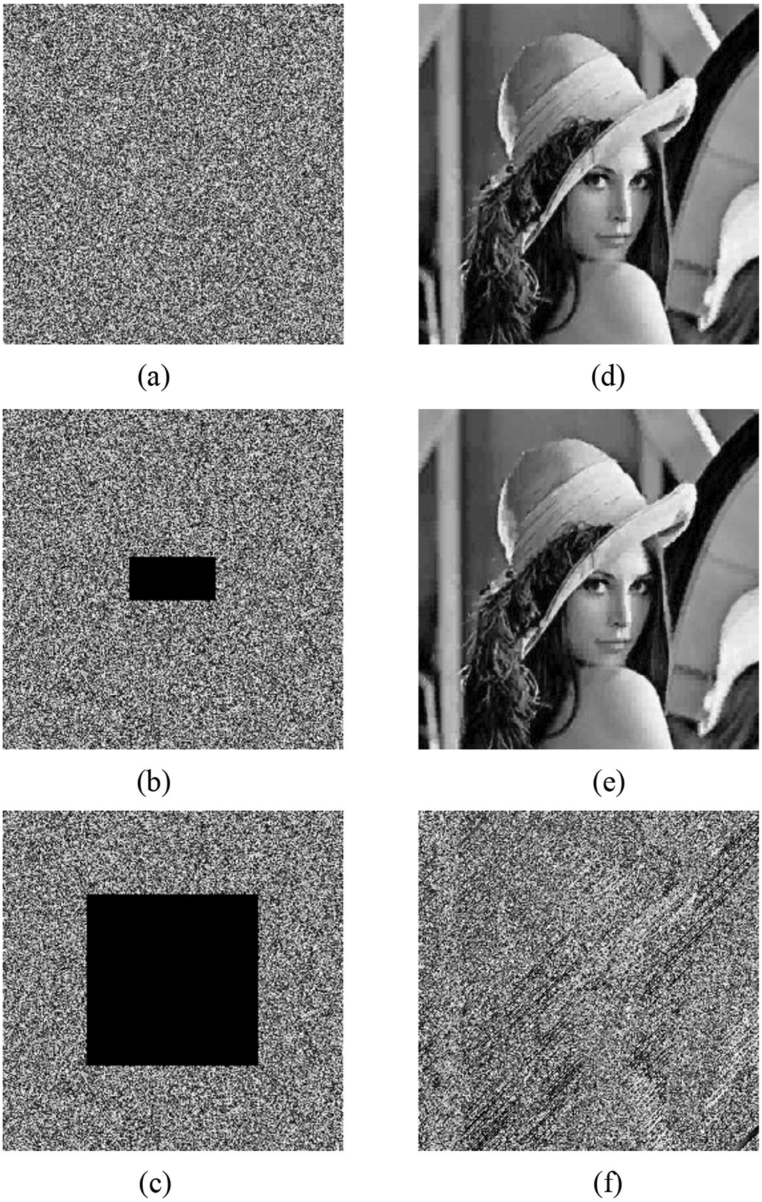


Fig. 6. **a**-**c** the cipher images with no loss, 1/32 loss, 1/4 loss, respectively; **d**-**f** the corresponding decrypted images of (a)-(c).

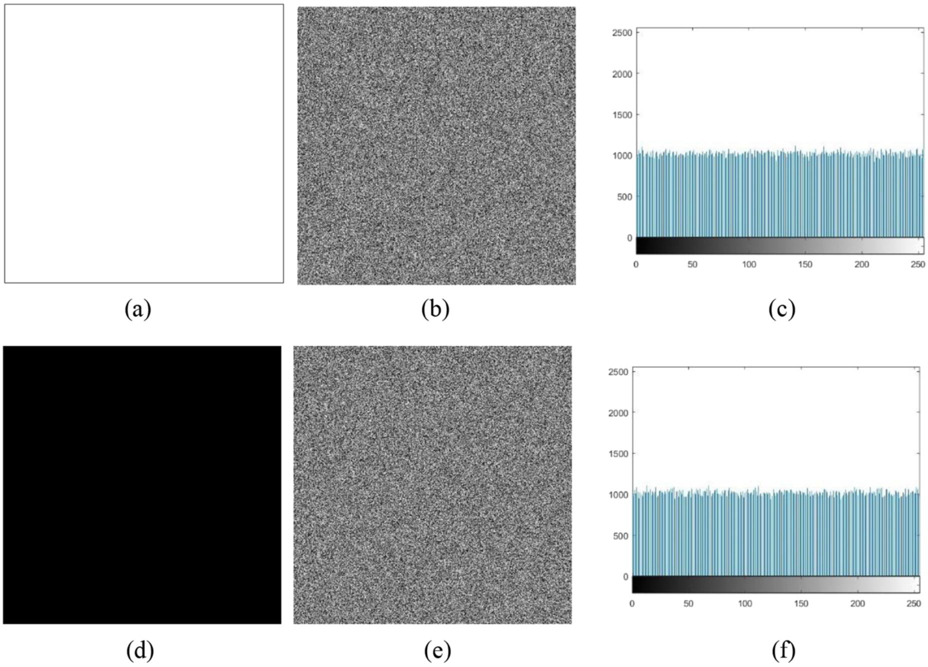
4.5.2 Cropping attack

Encrypted images are vulnerable to cropping attacks even data loss if transmitted and stored in unsafe communication channels. The cipher image received by the receiver will be unsuccessfully decrypted due to the loss of some information. Therefore, we must consider the robustness of the proposed scheme. For example, if the data loss size is 1/32 and 1/4 of the cipher image of Lena, the decrypted results are as shown in Fig. 6. We can find that our encryption scheme can resist cropping attack to a certain degree.

4.6 Known-plaintext and chosen-plaintext attacks

In this section, we test the anti-attack ability of the proposed image encryption scheme against classical cryptographic attacks (known-plaintext and chosen-plaintext). Besides, the chosen-plaintext attack is the most effective attack in modern cryptography, so the ability of anti-chosen plaintext attack needs to be improved when designing an encryption scheme [4].

In the test, some special images (black and white) are used as the plain image to simulate the process of the known-plaintext attack or chosen-plaintext attack, and the size of input images is 512 × 512. The encryption results shown in Fig. 7 indicate that the proposed scheme is valid enough in resisting the known-plaintext attack or chosen-plaintext attack because any available information cannot be obtained by the attacker.



(a) (b) (c)

(d) (e) (f)

Fig. 7. **a** white image, **b** the encrypted image of the white image, **c** the histogram of the encrypted white image, **d** black image, **e** the encrypted image of the black image, **f** the histogram of the encrypted black image.

4.7 Key space analysis

For a secure image encryption scheme, the key space should be larger than 2^{100} [10]. In our scheme, the secret keys are double-precision. Therefore, the key space is $(10^{16})^7 \times 2^{256} \approx 2^{626} > 2^{100}$. The result demonstrates that the proposed scheme performs well in resisting the brute-force attack.

5 Conclusion

In this paper, a new hyper-chaotic image encryption scheme based on QGA and CS is introduced. Firstly, QGA can update the population with the quantum rotation gate, which can enhance the randomness of the population and avoid falling into local optimum. Moreover, CS is used to reduce data storage and speed up the encryption and decryption process. Furthermore, we utilize the SHA-512 hash function of the plain image to calculate the initial values of the hyper-chaotic system, which is capable of enhancing the relationships between encryption schemes and plain images. Experimental simulations and comparisons have also verified the security of the proposed scheme. The security analysis demonstrates that the proposed scheme is efficient and practical in communications. In the future, we intend to convert the encryption scheme into the multimedia field.

Acknowledgments This work is supported by the Major Research Plan of the National Natural Science Foundation of China (No.91964108), the National Natural Science Foundation of China (No.61971185) and the Open Fund Project of Key Laboratory in Hunan Universities (No.18 K010).

References

1. Baptista MS (1998) Cryptography with chaos. Phys Lett A 240:50–54
2. Cai S, Huang L, Chen X, Xiong X (2018) A symmetric plaintext-related color image encryption system based on bit permutation. Entropy. 20:282
3. Çavuşoğlu Ü, Kaçar S, Pehlivan I, Zengin A (2017) Secure image encryption algorithm design using a novel chaos based S-box. Chaos, Solitons Fractals 95:92–101
4. Chai X, Fu X, Gan Z, Lu Y, Chen Y (2019) A color image cryptosystem based on dynamic DNA encryption and chaos. Signal Process 155:44–62
5. Chai X, Zheng X, Gan Z, Han D, Chen Y (2018) An image encryption algorithm based on chaotic system and compressive sensing. Signal Process 148:124–144
6. Cheng G, Wang C, Chen H (2019) A novel color image encryption algorithm based on hyperchaotic system and permutation-diffusion architecture. International Journal of Bifurcation and Chaos 29(9):1950115
7. Devaraj P, Kavitha C (2016) An image encryption scheme using dynamic S-boxes. Nonlinear Dynamics 86: 927–940
8. Di X, Wang L, Xiang T et al (2017) Multi-focus image fusion and robust encryption algorithm based on compressive sensing. Opt Laser Technol 91:212–225
9. Donoho DL (2006) Compressed sensing. IEEE Trans Inf Theory 52(4):1289–1306
10. Gonzalo A, Li S (2006) Some basic cryptographic requirements for chaos-based cryptosystems. International Journal of Bifurcation and Chaos 16(8):2129–2151
11. Han K, Kim J (2000). Genetic quantum algorithm and its application to combinatorial optimization problem. In proceedings of the 2000 Congress on Evolutionary Computation. USA: IEEE, 1354–1360
12. Hu T, Liu Y, Gong L et al (2017) An image encryption scheme combining chaos with cycle operation for DNA sequences. Nonlinear Dynamics 87:51–66
13. Jain A, Rajpal N (2016) A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps. Multimed Tools Appl 75:5455–5472

14. Kayalvizhi S, Malarvizhi S (2020) A novel encrypted compressive sensing of images based on fractional order hyper chaotic Chen system and DNA operations. Multimed Tools Appl 79:3957–3974
15. Li M, Lu D, Wen W, Ren H, Zhang Y (2018) Cryptanalyzing a color image encryption scheme based on hybrid hyper-chaotic system and cellular automata. IEEE Access 6:47102–47111
16. Li Y, Wang C, Chen H (2017) A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. Opt Lasers Eng 90:238–246
17. Lin H, Wang C (2020) Influences of electromagnetic radiation distribution on chaotic dynamics of a neural network. Appl Math Comput 369:124840
18. Liu Y, Tong X, Ma J (2016) Image encryption algorithm based on hyper-chaotic system and dynamic S-box. Multimed Tools Appl 75:7739–7759
19. Liu J, Yang D, Zhou H, Chen S (2018) A digital image encryption algorithm based on bit-planes and an improved logistic map. Multimed Tools Appl 77:10217–10233
20. Mondal B, Singh S, Kumar P (2019) A secure image encryption scheme based on cellular automata and chaotic skew tent map. Journal of Information Security and Applications 45:117–130
21. Niu Y, Wang X, Wang M et al (2010) A new hyperchaotic system and its circuit implementation. Commun Nonlinear Sci Numer Simul 15:3518–3524
22. Parisa Gholizadeh P, Hadi Shahriar S, Morteza M (2018) Hyper-chaotic Feeded GA (HFGA): a reversible optimization technique for robust and sensitive image encryption. Multimed Tools Appl 77:20385–20414
23. Rasul E, Hossein Javedani S, Abdul Hanan A et al (2015) A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata. Opt Lasers Eng 71:33–41
24. Schmitz R (2001) Use of chaotic dynamical systems in cryptography. Journal of the Franklin Institute 338: 429–441
25. Wang X, Çavuşoğlu Ü, Kacar S, Akgul A, Pham VT, Jafari S, Alsaadi F, Nguyen X (2019) S-box based image encryption application using a chaotic system without equilibrium. Appl Sci 9:781
26. Wang L, Shen T (2001) An improved adaptive genetic algorithm and its application to image segmentation. Image Extraction, Segmentation, and Recognition 4550:115–120
27. Wang S, Wang C, Xu C (2020) An image encryption algorithm based on a hidden attractor chaos system and the Knuth-Durstenfeld algorithm. Opt Lasers Eng 128:105995
28. Wang X, Xu D (2015) A novel image encryption scheme using chaos and Langton's ant cellular automaton. Nonlinear Dynamics 79:2449–2456
29. Wu J, Liao X, Yang B (2018) Cryptanalysis and enhancements of image encryption based on three-dimensional bit matrix permutation. Signal Process 142:292–300
30. Wu J, Liao X, Yang B (2018) Image encryption using 2D Hénon-sine map and DNA approach. Signal Process 153:11–23
31. Xu L, Li Z, Li J, Hua W (2016) A novel bit-level image encryption algorithm based on chaotic maps. Opt Lasers Eng 78:17–25
32. Yaghouti Niyat A, Moattar MH, Niazi TM (2017) Color image encryption based on hybrid hyper-chaotic system and cellular automata. Opt Lasers Eng 90:225–237
33. Yin Q, Wang C (2018) A new chaotic image encryption scheme using breadth-first search and dynamic diffusion. International Journal of Bifurcation and Chaos 28(4):1850047
34. Zhang S, Gao T (2016) An image encryption scheme based on DNA coding and permutation of hyper-image. Multimed Tools Appl 75:17157–17170
35. Zhang X, Nie W, Ma Y, Tian Q (2017) Cryptanalysis and improvement of an image encryption algorithm based on hyper-chaotic system and dynamic S-box. Multimed Tools Appl 76:15641–15659
36. Zhang X, Wang C (2019) A novel multi-attractor period multi-scroll chaotic integrated circuit based on CMOS wide adjustable CCCII. IEEE Access 7:16336–16350
37. Zhang W, Yu H, Zhao Y, Zhu ZL (2016) Image encryption based on three-dimensional bit matrix permutation. Signal Process 118:36–50
38. Zhao Q, Wang C, Zhang X (2019) A universal emulator for memristor, memcapacitor, and meminductor and its chaotic circuit. Chaos. 29:13141
39. Zhou M, Wang C (2020) A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks. Signal Process 171:107484
40. Zhou N, Yang J, Tan C, Pan S, Zhou Z (2015) Double-image encryption scheme combining DWT-based compressive sensing with discrete fractional random transform. Opt Commun 354:112–121
41. Zhu C, Wang G, Sun K (2018) Cryptanalysis and improvement on an image encryption algorithm design using a novel chaos based S-box. Symmetry. 10:399

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.