IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 27, 2019, accepted October 29, 2019, date of publication November 7, 2019,
date of current version December 3, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2952140

High Intensity Image Encryption Scheme Based on Quantum Logistic Chaotic Map and Complex Hyperchaotic System

JI XU, PENG LI, FEIFEI YANG, AND HUIZHEN YAN
School of Information Science and Engineering, Dalian Polytechnic University, Dalian 116034, China

Corresponding author: Peng Li (lipeng@dlpu.edu.cn)

This work was supported by the Basic Scientific Research Projects of Colleges and Universities of Liaoning Province under Grant 2017J046.

ABSTRACT In this paper, a novel encryption algorithm based on quantum chaotic map and four-wing complex system is proposed. Dynamical performances of the two system are revealed by phase portraits, Lyapunov exponent spectrum, bifurcation diagram analyses and complexity entropy. Based on these analyses, an encryption algorithm is designed by the two chaotic system and DNA coding. Firstly, in process of permutation operation, quantum logistic map is utilized to generate chaotic sequences for disrupting the position of each pixel point combine with Arnold transformation. Then, using the complex hyperchaotic system, the value of each pixel is diffused through mathematical operation and DNA encoding. Finally, security performance is analyzed. Simulation results demonstrate that the algorithm has good robustness and high-quality performance, and it can effectively protect the subject image and resist conventional attack. This encryption scheme can provide a new realization method for security transmission and protection of image information.

INDEX TERMS Quantum logistic chaotic map, complex hyperchaotic system, arnold matrix, image encryption.

I. INTRODUCTION

With fast development of information technology and the scale of the communication network, digital information is generated, transmitted and stored frequently. Among them, digital images including a large amount of private information, if this information is stolen or unauthorized access, which may cause a lot of damage. The digital image has significant characteristics such as large data capacity, high redundancy and strong correlation among adjacent pixel. Thus, traditional encryption scheme such as DES algorithm isn't suitable to protect the digital image information. Therefore, search for high performance encryption algorithm has become a hot research field [1]–[4].

Chaotic systems have many noteworthy features, including the highly sensitive of initial value, pseudo randomness and ergodicity, low cost in the computer operation system and microprocessor [5]–[7]. Hence chaotic system is quite matching for cryptography. In recent years, some image encryption algorithms based on the chaotic system have proposed. Such as Arnold matrix or zigzag transformation is used to calculate new pixel point position for scrambling image matrix by using chaotic system [8]–[11]. Chaotic sequence was used to shift the order of the image matrix [12]–[14]. Because of DNA theory and chaotic sequence, some encryption scheme is designed [13]–[24]. Chai and her research team used DNA theory and SHA256 hash function to encrypt digital image [20], [21]. Yang et al. employed discrete chaotic map combines with DNA theory to obtain encrypted image [14]. In the optical image processing area, Ref. [25]–[27] proposed the image encryption scheme based on the discrete chaotic system and nonlinear transform. Such as Ref. [25] is adopted the RSA public-key cryptographic algorithm in encryption flow. Ref. [26] is proposed the method of image encryption by phase truncation and phase reservation in the two-dimensional linear canonical transform (2D LCT) domain. In Ref. [27], Phase-truncated short-time fractional Fourier transform (PTSTFrFT) and wave-based permutation

The associate editor coordinating the review of this manuscript and approving it for publication was Md. Asikuzzaman.

is combined for encoding the plaintext image. Meanwhile, neural network theory and compressive sensing are adopted for enhancing the security performance [28]–[31].

However, currently chaos-based encryption schemes still have weakness in different aspect need to overcome. Firstly, most encryption algorithm is still used single chaotic system for encrypt operation. These schemes may can't resist brute-force attack efficiently as their key space is small. Moreover, single chaotic system only has few chaotic sequences can be applied. Conversely, Double chaotic system has multi chaotic sequence as secret key can select and combine. Hence, attacker can't knowledge which sequence is adapted to scramble or diffusion. Besides, double chaotic system can expand the key space and enhance the performance of resist brute-force attack. In addition, double chaotic system isn't widely used for encryption algorithm.

Secondly, as seed system in encryption algorithm, Discrete chaotic systems are often adopted [14], [18], [19], [22], [24], [32]–[37]. However, these systems not have complex dynamical behaviors, making their sequence can be easily predicted. Moreover, discrete system has simple structure, so the system parameter can be easily estimated. Compare with discrete chaotic map, some chaos-based encryption algorithm is applied real variable continuous chaotic system as seed system [21], [31], [38], [39]. These systems have more complex structure and more highly dimension than discrete chaotic map. However, it is a significant weakness that the variables space is small. These systems don't have complex dynamical behaviors either. Hence, complex variables chaotic system is applied in encryption algorithm for improving the security performance. As a result of complex chaotic system has real number domain and complex number domain [40]–[42]. It can expand the variable space of the system and improve dynamics characteristics. Moreover, it can effectively add the key space and improve the ability of resist brute-force attack. In encryption algorithm, complex chaotic system can provide different sequence for select and combine. It will increase the difficult of malicious encoding. Therefore, the complex chaotic system can enhance the security performance of different attack.

Quantum chaotic systems are the quantized of classical chaotic system. Such as quantum logistic system is constructed by classical logistic system. This system has high-dimension and more complex dynamic behavior [43]–[45]. Moreover, quantum chaotic system has high sensitivity with parameters. This property is very important for the cryptography. Hence, quantum logistic system is suitable as seed system in encryption algorithm. There are numerous research papers based on the quantum logistic system [33], [46], [47].

Based on the above this analysis, this work proposes a novel encryption algorithm combining the double chaotic system and complex chaotic system. The architecture of this algorithm is scrambling and diffusion is adopted. Firstly, the secret sequence generated by quantum logistic system in scrambling operation. Moreover, in different scrambling round, the elements of Arnold matrix are different. Therefore, the position of pixel can become more random and uncertain. Secondly, according to the advantage of complex chaotic system, a novel complex chaotic system is applied in diffusion operation. Because of the complex chaotic system has high dimension compared with real domain variables chaotic system. Hence, many combinations of chaotic sequence can be applied.

The rest sections of this paper are organized as follows. In Sec. 2, dynamic character analyses of quantum logistic system and complex chaotic system are carried out respectively, and display the corresponding analysis results. Then, the encryption algorithm and decryption algorithm workflow are described respectively in Sec. 3. The encryption and decryption image are shown in the end of this section. Sec. 4 illustrates the results of security performance and relevant technical indexes. The important conclusion is drawn in Sec. 5.

II. BASIC BACKGROUND OF THE PROPOSED CRYPTOSYSTEM

A. QUANTUM CHAOTIC MAP

Based on the classical logistic map and the effect of quantum correlations on the a dissipative system [45], a new quantum chaotic map could be described as Eq. (1)

$$\begin{cases} x_{n+1} = r^*(x_n - |x_n|^2) - r^* y_n \\ y_{n+1} = -y_n{}^* e^{-2\beta} + e^{-\beta} r[(2 - 2x_n)y_n - 2x_n z_n] \\ z_{n+1} = -z_n{}^* e^{-2\beta} + e^{-\beta} r[(2(1 - x_n)z_n - 2x_n y_n - x_n] \end{cases} \tag{1}$$

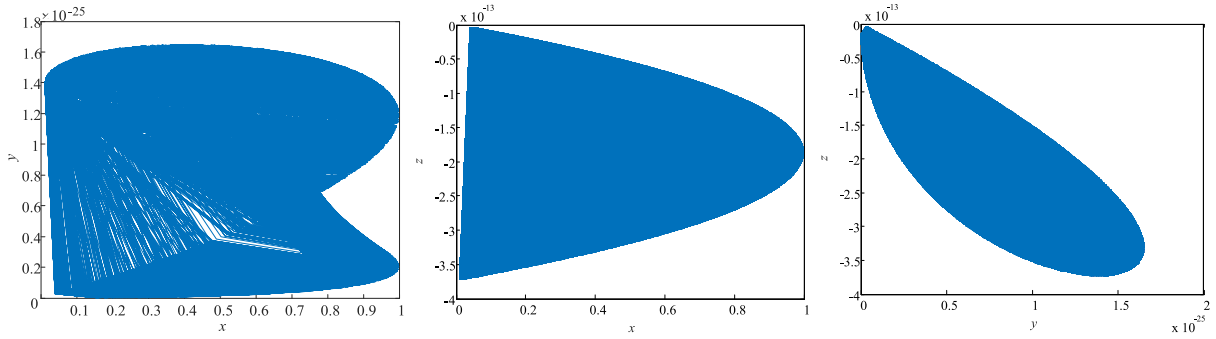
where system parameter β represent dissipation parameter and γ is control parameter.

B. DYNAMICS PROPERTIES OF QUANTUM LOGISTIC SYSTEM

The phase diagram of quantum logistic map is demonstrated in Fig. 1. Setting system parameters $\gamma = 3.99, \beta = 30$, the initial value $(x_0, y_0, z_0) = (0.463442265, 0.04532285, 0.002136285)$. Where the step size is 0.01, the corresponding Lyapunov exponents are LE1 $= 0.63516$, LE2 $= -5.234$, LE3 $= -6.3083$, and the Lyapunov dimension is 1.1214. It can illustrate that the quantum logistic system is chaotic state.

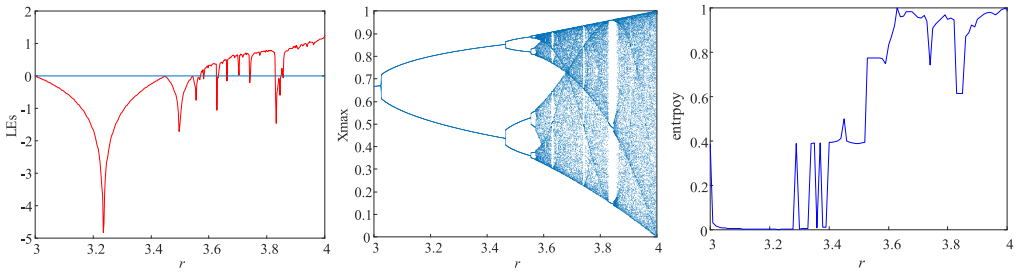
Fixed the initial value and system parameter β, set system parameter $\gamma \in [3,4]$. the max Lyapunov exponent spectrum is shown in Fig 2 (a). Fig 2 (b) is demonstrate the bifurcation diagram of system variable x.

Obviously, quantum logistic system is chaotic when $\gamma \in [3.57, 3.99]$. However, in the region $\gamma \in [3.627, 3.633] \cup [3.739, 3.744] \cup [3.829, 3.844]$, quantum logistic system shows periodic behavior. The system enters chaos by period doubling bifurcation. In order to better reflect the random performance of chaotic sequence better, the permutation entropy (PE) of quantum logistic system is shown in Fig. 2(c). Theoretically, the closer the value of PE is to 1, the better randomness of chaotic sequence.



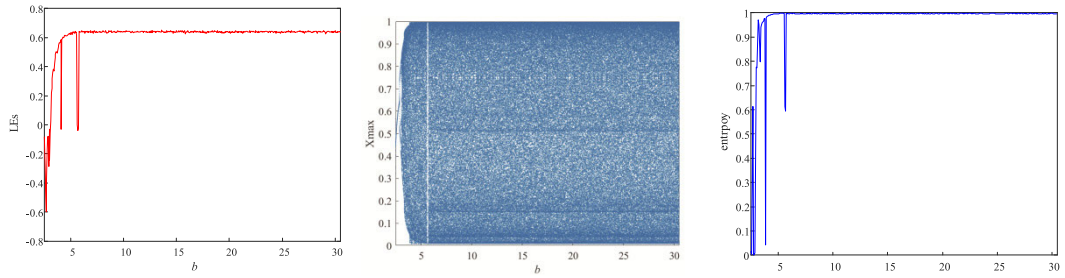
(a) (b) (c)

FIGURE 1. The Phase diagram of quantum logistic map (a) x-y (b) x-z (c) y-z.



(a) (b) (c)

FIGURE 2. Dynamical properties analysis of quantum logistic system ($\gamma \in [3, 4]$, $\beta = 30$) (a) Lyapunov exponent spectrum (b) The bifurcation diagram (c) Permutation entropy complexity.



(a) (b) (c)

FIGURE 3. Dynamical properties analysis of quantum logistic system ($\gamma = 3.99$, $\beta \in [2.5,7.5]$) (a) Lyapunov exponent spectrum (b) The bifurcation diagram (c) Permutation entropy complexity.

When system parameter $\beta \in [2.5, 7.5]$, $\gamma = 3.99$. The corresponding Lyapunov exponent spectrum, bifurcation diagram and complexity entropy are shown in Fig. 3.

It clears that in the Fig. 3(a) and (b), chaotic state of quantum logistic system can be observed when $\beta \in (3.1,30)$. Fig. 3(c) is shown that the value of PE is very high when the $\beta \in (3.1,30)$. It can prove that quantum logistic system can generate more random sequence.

As the seed system in the proposed algorithm, quantum logistic system must satisfy some requirements such as long period and a high degree of complexity. Therefore, for testing the randomness of chaotic sequence, the NIST SP 800-22 test software package is utilized.

The NIST test has two methods for measuring randomness of sequence. The first method is the pass proportion of the statistical test. Given the result of a statistical test, compute the pass proportion of test sample. For instance, if 1000 binary sequences were tested, the significance level $\alpha = 0.01$, and 998 binary sequences had P-value$\geq$0.1. The pass proportion is 0.9960. The range of acceptable proportions is determined using the confidence interval defined as

$$\hat{P} = \sqrt{\frac{\hat{P}(1-\hat{P})}{m}}. \tag{2}$$

where $\hat{P} = 1\text{-}\alpha$, and m is the sample size. If the proportion fall outside of this interval, it can illustrate this sample is nonrandom.

The second method is the P-value of statistical test. It is obtained according to the Eq. (3)

$$\chi^2 = \sum_{i=1}^{10} \frac{(F_i - 0.1s)^2}{0.1s}. \tag{3}$$

where F_i is the value of P-value in subinterval i. If the P-value $\geq$ 0.001, then the sequence can be considered to randomness.

To carry on this test, NIST test suit evaluates around the 200 million of random numbers, 228MByte of data. The result of NIST test is shown in the TABLE 1 to 2.

The analysis results can prove that the quantum logistic system has good dynamical properties and randomness. which means this chaotic system is suitable to apply in encryption algorithm. Also, quantum logistic system has big parameter space. However, the phenomenon of quantum logistic system should be noticed, when system parameter $\beta \to \infty$, the quantum logistic system will reduce to the classical one-dimension logistic system. Therefore, the value of parameter β has a certain range of keeping dynamical properties.

C. FOUR-WING HYPERCHAOTIC COMPLEX SYSTEM

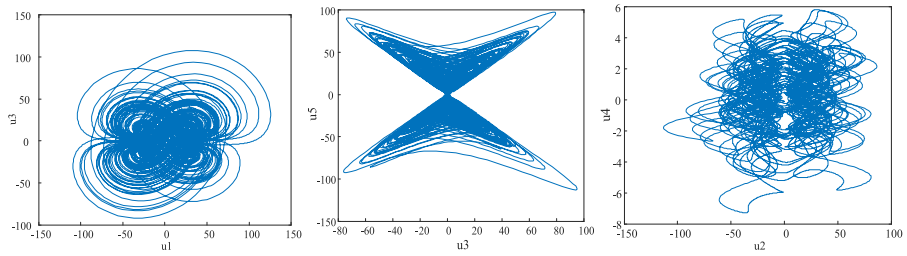
A novel Complex Hyperchaotic System[42] will be adopt as the core element of image processing algorithm, which is

TABLE 1. Result of the NIST SP800-22 test suit for quantum logistic chaotic sequence.

Test name		*x*		*y*		*z*	
		P-value	Result	*P*-value	Result	*P*-value	Result
Frequency		0.7598	Pass	0.9114	Pass	0.8165	Pass
Runs		0.8165	Pass	0.5141	Pass	0.0329	Pass
Block frequency		0.5544	Pass	0.7598	Pass	0.5341	Pass
Long runs		0.0102	Pass	0.4012	Pass	0.0712	Pass
Rank		0.7399	Pass	0.6371	Pass	0.2248	Pass
FFT		0.1223	Pass	0.5542	Pass	0.8832	Pass
Non-Overlapping Template		0.4487	Pass	0.5159	Pass	0.4639	Pass
Overlapping Template		0.1718	Pass	0.9978	Pass	0.3669	Pass
Universal		0.1816	Pass	0.8978	Pass	0.0966	Pass
Approximate Entropy		0.6371	Pass	0.6163	Pass	0.3669	Pass
Cumulative Sums	Forward	0.3190	Pass	0.4012	Pass	0.4012	Pass
	Reverse	0.0668	Pass	0.6163	Pass	0.3505	Pass
Serial	*P* value-1	0.4011	Pass	0.0712	Pass	0.9114	Pass
	P value-2	0.7792	Pass	0.9915	Pass	0.5141	Pass
Random Excursions	x=-4	0.7399	Pass	0.3505	Pass	0.8755	Pass
	x=-3	0.9850	Pass	0.5341	Pass	0.7887	Pass
	x=-2	0.7061	Pass	0.0351	Pass	0.2873	Pass
	x=-1	0.9761	Pass	0.0401	Pass	0.9411	Pass
	x=1	0.6717	Pass	0.3190	Pass	0.2229	Pass
	x=2	0.7728	Pass	0.2133	Pass	0.8195	Pass
	x=3	0.0909	Pass	0.1719	Pass	0.9705	Pass
	x=4	0.3505	Pass	0.0519	Pass	0.1056	Pass

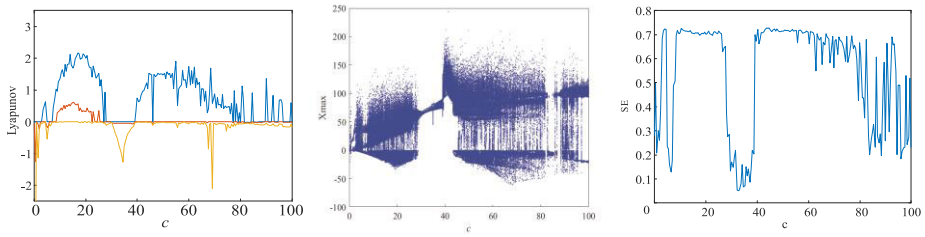
TABLE 2. Result of the NIST SP800-22 test suit for generated keystreams.

Test name		*x*		*y*		*z*	
		P-value	Result	*P*-value	Result	*P*-value	Result
Random Excursions Variant	x=-9	0.5681	Pass	0.7792	Pass	0.9573	Pass
	x=-8	0.2993	Pass	0.5749	Pass	0.7887	Pass
	x=-7	0.9114	Pass	0.7399	Pass	0.4846	Pass
	x=-6	0.7728	Pass	0.5341	Pass	0.4846	Pass
	x=-5	0.8623	Pass	0.1718	Pass	0.1413	Pass
	x=-4	0.8344	Pass	0.5341	Pass	0.1165	Pass
	x=-3	0.0821	Pass	0.0308	Pass	0.7231	Pass
	x=-2	0.1481	Pass	0.3505	Pass	0.9001	Pass
	x=-1	0.7399	Pass	0.0308	Pass	0.5852	Pass
	x=1	0.0012	Pass	0.6993	Pass	0.9885	Pass
	x=2	0.3781	Pass	0.4559	Pass	0.4528	Pass
	x=3	0.1626	Pass	0.0966	Pass	0.2645	Pass
	x=4	0.6371	Pass	0.0590	Pass	0.3115	Pass
	x=5	0.3504	Pass	0.0308	Pass	0.0046	Pass
	x=6	0.8343	Pass	0.1372	Pass	0.9220	Pass
	x=7	0.2133	Pass	0.2622	Pass	0.2645	Pass
	x=8	0.9915	Pass	0.5341	Pass	0.2430	Pass
	x=9	0.2757	Pass	0.2897	Pass	0.0865	Pass



(a) (b) (c)

FIGURE 4. The Phase diagram of Complex hyperchaotic system (a) u1-u3 (b) u3-u5 (c) u2-u4.



(a) (b) (c)

FIGURE 5. Lyapunov Exponent and Bifurcation diagram of Four-Wing Complex System (a) The Lyapunov exponent (b) The bifurcation diagram (c) The complex rate.

expressed as Eq. (2)

$$\begin{cases} \dot{x} = ax - yz + w \\ \dot{y} = xz - by \\ \dot{z} = \frac{1}{2}[\bar{x}(y + w) + x(\bar{y} + \bar{w})] - cz \\ \dot{w} = -\frac{1}{2}(y + \bar{y}). \end{cases} \tag{4}$$

where $x = u_1 + i^* u_2$, y= $u_3 + i^* u_4$ are complex state variables, $z = u_5$, $w = u_6$ are real variables, the system parameter a, b and c are real variables. According to mathematical calculation, the four-wing complex system can be expressed as Eq. (3)

$$\begin{cases} \dot{u}_1 = au_1 - u_3u_5 + u_6 \\ \dot{u}_2 = au_2 - u_4u_5 \\ \dot{u}_3 = u_1u_5 - bu_3 \\ \dot{u}_4 = u_2u_5 - bu_4 \\ \dot{u}_5 = u_1(u_3 + u_5) + u_2u_4 - cu_5 \\ \dot{u}_6 = -u_3. \end{cases} \tag{5}$$

D. DYNAMIC PROPERTIES OF COMPLEX CHAOTIC SYSTEM

The system phase diagram is shown in Fig. 4. It obtained by setting $a = 10, b = 40, c = 14.9$, initial value $(u_1, u_2, u_3, u_4, u_5, u_6) = [10, 1, 10, 1, 10, 1]$. The Lyapunov exponent distribution LE = (2.97791, 0.709212, 0, −0.0838536, −29.9592, −48.5238), and the Lyapunov dimension is 4.1158, which means that the complex chaotic system is hyperchaotic.

Fix the initial value and system parameters $a\,b$. The system parameter c is varied. The dynamic characteristics of the complex chaotic system are studied through Lyapunov exponent spectrum and the bifurcation diagram shown in Fig. 5(a) and (b), respectively. When c is belongs to in region [7], [28], this system in hyperchaotic state. In addition, the randomness of chaotic sequence can be expressed by SE complexity in Fig 5(c).

Therefore, the complex hyperchaotic system has complex dynamics behavior, and this system can adopt in encryption algorithm for enhance the security performance.

III. ENCRYPTION SCHEME DESIGN

A. ENCRYPTION ALGORITHM ARCHITECTURE

In this work, the quantum logistic system combines with Arnold matrix to disorder the image matrix for decreasing the correlation, complex hyperchaotic system used to change the value of pixel point with XOR operation and DNA coding operation. The specific encryption process is shown in Fig 6. The detail encryption steps are as follows.

1) PIXEL POSITION SCRAMBLING

Step 1: Assume the size of plain image I is $H \times W$, where H and W are represent the number of rows and columns. Then, inputting the plain image, nd set s as disturbance variable calculated by Eq. (4)

$$s = \frac{\sum_{i=1}^{H} \sum_{j=1}^{W} I(i, j)}{10^{10}}. \tag{6}$$

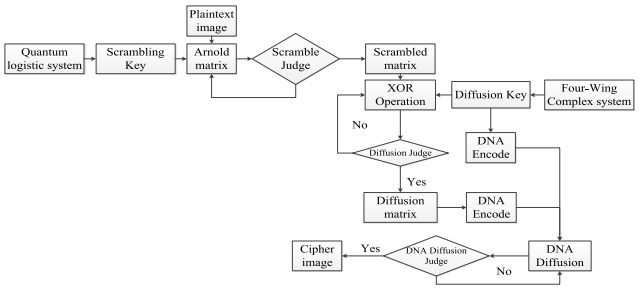


FIGURE 6. The architecture of encryption algorithm.

Hence, the initial value of the quantum logistic chaotic system is obtained from Eq. (5)

$$\begin{cases} x_0' = x_0 + s \\ y_0' = y_0 + s \\ z_0' = z_0 + s. \end{cases} \tag{7}$$

In encryption algorithm, variable s has two functions. Firstly, variable s could change the original initial value for generated a new chaotic sequence. Secondly, variable s is obtained by the plaintext image. When plaintext image is changed, the value of s is different, the chaotic sequence is different.

Step 2: When $N = H^*W$, using s to change the initial value of quantum logistic system. The changed value is used to iterative Eq. (1) $(m + N)$ times in order to get the chaotic sequence. Then, throw out the first m values for enhance the sensitivity of the initial value.

Step 3: According to chaotic sequence, the pseudo-number matrix S obtained as follow

$$\begin{cases} Cx = \mathrm{mod}(\lfloor Cx^*H^*W^*10^5 \rfloor, 256) \\ Cy = \mathrm{mod}(\lfloor Cy^*H^*W^*10^{30} \rfloor, 256) \\ Cz = \mathrm{mod}(\lfloor Cz^*H^*W^*10^{20} \rfloor, 256). \end{cases} \tag{8}$$

In addition, the values of Cx, Cy and Cz are used to scramble position of pixels.

Step 4: Here consider S as parameter of Arnold matrix used to generate new coordinate of pixel point. It has three different format Arnold matrixes as follow in Eq. (7) to Eq. (9)

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ S & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \mathrm{mod}\ (N) \tag{9}$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 254 \\ S & (254^*S) + 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \mathrm{mod}\ (N) \tag{10}$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 254 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \mathrm{mod}\ (N). \tag{11}$$

where S can be obtained from

$$S = [Cx, Cy, Cz]. \tag{12}$$

On the first round, the scrambling matrix is subject to Eq. (9), and each round f the Arnold matrix is different. When iteration time is 6, the permutation is finish. The image scrambling matrix TR is obtained.

2) PIXEL VALUE DIFFUSION

Step 5: Set $N = H^*W$, updating chaotic sequence generator as complex hyperchaotic system. Firstly, inputting the initial value and system parameter, and iterative Eq. (3) is iterated for N times to get the chaotic sequence u. Then, the pseudo-random number sequence is obtained as follow

$$v = \mathrm{mod}(u(i)^*2^{16}, 256) \tag{13}$$

Step 6: the bit-level manipulation diffusion is defined

$$\begin{cases} B(i,j) = TR(i,j) \oplus v(i,j) \\ D(i,j) = B(i,j) \oplus v(i,j) \end{cases} \tag{14}$$

B is the diffusion image matrix. D represents the new diffusion image matrix in Eq. (12).

Step 7: Repeating the step 4 to step 6 again, and the new diffusion image matrix is obtained.

3) DNA LEVEL DIFFUSION

In this section, the DNA coding rules based on the DNA calculation theory is described briefly. According to DNA theory, each DNA sequence consists of four nucleic acid bases. All nuclear acid is subject to the principle of base complementary pairing, the specific content as follows: Adenine (A) is associated with Thymine (T). Cytosine (C) pairs with Guanine (G). Corresponding to a digital image, the pixel point can be encoded by four nucleic acid bases. Therefore, the coding rule has $4! = 24$ kinds. However, only eight encode rule can satisfy the Watson-Crick complementary rule as shown in the TABLE.3.

TABLE 3. Table of DNA encode rule.

Rule	1	2	3	4	5	6	7	8
00	A	A	T	T	G	G	C	C
01	C	G	C	G	T	A	T	A
10	G	C	G	C	A	T	A	T
11	T	T	A	A	C	C	G	G

The law of addition and subtraction of the four basic elements of DNA are shown in the following TABLE.4.

TABLE 4. Table of DNA addition and subtraction rule.

+	A	C	G	T	-	A	C	G	T
A	A	C	G	T	A	A	T	G	C
C	C	G	T	A	C	C	A	T	G
G	G	T	A	C	G	G	C	A	T
T	T	A	C	G	T	T	G	C	A

There DNA diffusion encryption flow is decreased as follows.

Step 8: The numerical matrix is changed into binary matrix before DNA encryption operation. Then, the binary matrix is converted to the DNA matrix $S1$ and the matrix size is $H \times 4 \times W$. At same time, the sequence v is transformed into DNA sequence K_1.

Step 9: In DNA encryption operation, principle of base complementary pairing is performed for scrambling the combination of original DNA matrix. After scrambling operation, a new DNA matrix D is obtained.

Step 10: The diffusion matrix C_1 is generated by DNA level diffusion used the matrix D and the DNA sequence.

Step 11: the final matrix C_2 is obtained by repeating the step 10.

Step 12: The matrix C_2 is decode and then recovering the binary format.

Step 13: Output the encryption results and the cipher image is obtained.

B. DECRYPTION ALGORITHM FLOW

The decryption algorithm is the inverse process of the encryption algorithm. Firstly, receiver gets the encrypted image. Then, the secret key sequence is used to reconstruct plain image and the final decrypted image can be obtained. The specific decryption process is shown in Fig 7.

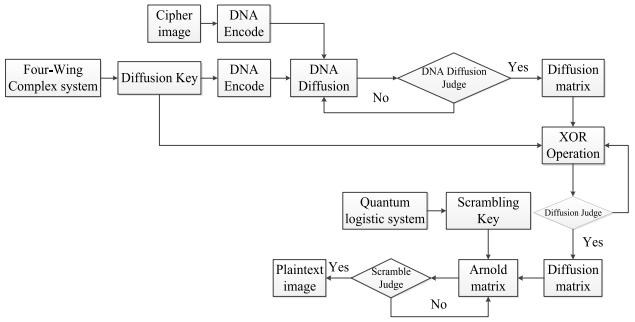


FIGURE 7. The architecture chart of decryption algorithm.

Step 1: Before decryption operation is start, the size of cipher image is measured as $H \times W$. Then, the image matrix is encoded through the DNA encoding rule to obtain DNA matrix with size is $H \times 4 \times W$.

Step 2: Restore the diffusion matrix. At first, Eq. (3) is used to generate decryption key for restore the DNA matrix. In the process of reconstruction, the flow of rebuild the diffusion matrix is inverse compare with DNA level diffusion. After step 2, the diffusion matrix is obtained.

Step 3: In this stage, other pseudo random number sequence generated by Eq. (3) are used to recover the value of diffusion matrix. The bit manipulation diffusion is defined as follow

$$\begin{cases} TR(i,j) = B(i,j) \oplus U_r(i,j) & r = 1 \\ B(i,j) = D(i,j) \oplus U_r(i,j) & r \neq 1, \end{cases} \tag{15}$$

According to Eq. (13), the diffusion operation in decryption process is inverse operation compare with encryption algorithm. When iteration time is 6, the scrambling matrix is obtained.

Step 4: on the basic of step 3, the scrambling operation through Arnold matrix to calculate the original position of pixel point. Where, S is pseudo random number sequence generated by quantum logistic map. The transformation matrix has three formats as follow in Eq. (14) to Eq. (16)

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 254 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod (N) \tag{16}$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 254 \\ S & (254^{*}S)+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod (N) \tag{17}$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ S & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod (N). \tag{18}$$

Compare with encryption algorithm, the scrambling operation is reverse process. When iteration time is 6, the scrambling operation is finish. The incomplete decrypted image matrix is obtained.

Step 5: the decrypted image matrix is obtained by repeating the step 4 and step 5.

C. ALGORITHM SIMULATION

Take the digital image Lena, pepper and baboon as the encryption image, Set quantum logistic map system parameters $\gamma = 1$, $\beta = 2\pi$, initial value $(x_0, y_0, z_0) = [0.3, 0.5, 0.6]$. The Complex chaotic system parameters $a = 8$, $b = 40$, $c = 14.9$ and initial value $(u_1, u_2, u_3, u_4, u_5, u_6) = [10, 1, 10, 1, 10, 1]$. The encryption and decryption results are shown in Fig 8.

IV. ENCRYPTION PERFORMANCE ANALYSIS

A. KEY SPACE ANALYSIS

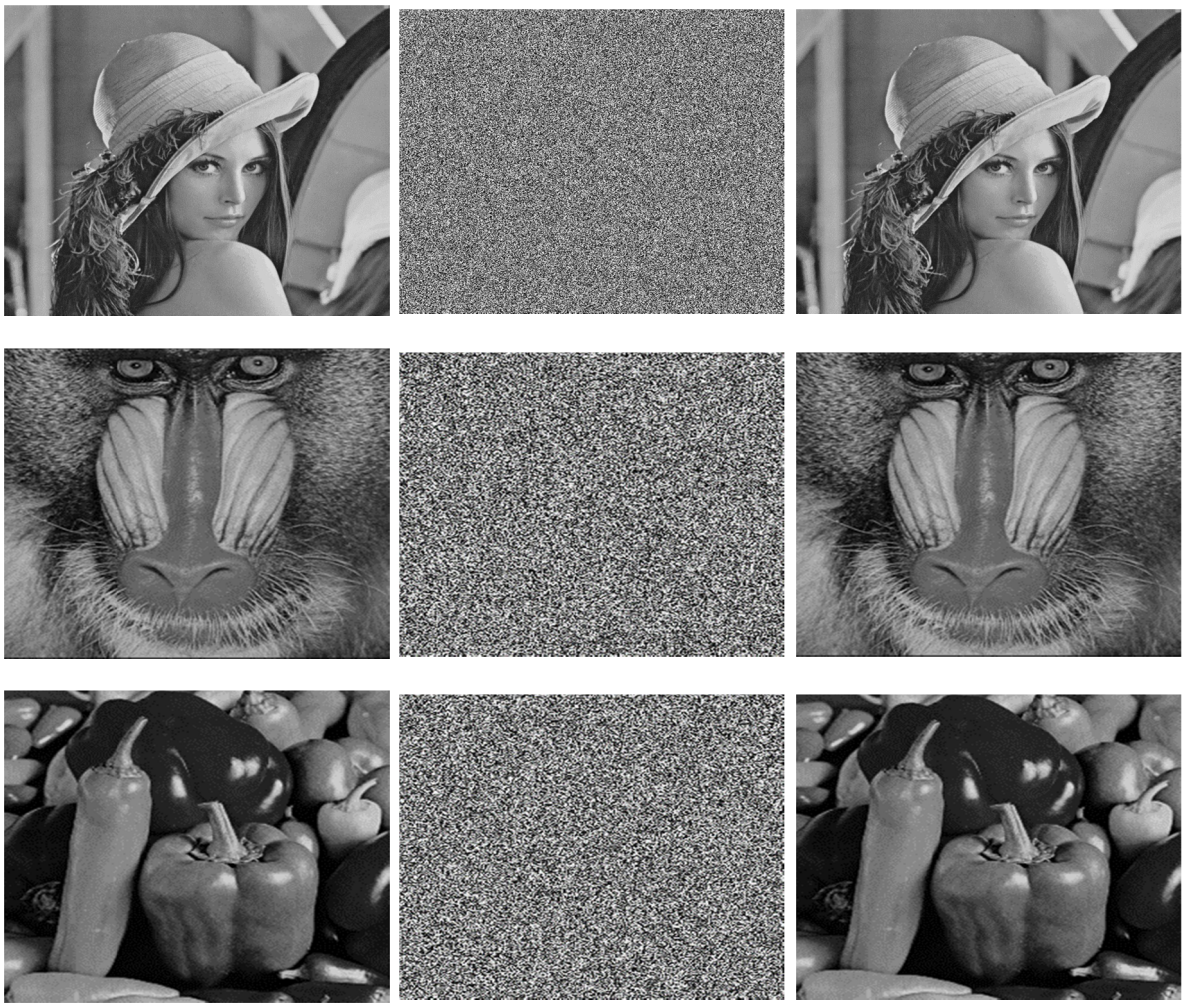
The key space of image encryption algorithm should be large enough for resisting brute force attack. According to the algorithm structure, the secret key format should consist of: (1) the quantum logistic map parameter: γ, β, and initial value: x_0, y_0, z_0. (2) The parameters of complex hyperchaotic system: a, b, c, and original variables: $[u_1\, u_2\, u_3\, u_4\, u_5\, u_6]$. (3) The DNA encoding part include of initial deoxynucleotide c_0, calculation rule α and β, and DNA coding rules L_i. When the computer computational accuracy is 10^{-15}, the key space of this algorithm can approach 2^{685}, it can be illustrated that the algorithm can resist brute-force attack.

TABLE.5 compare with nother encryption algorithm. Obviously, the encryption algorithm proposed in this study has larger key

B. KEY SENSITIVITY ANALYSIS

In a cryptosystem, the secret key should be very sensitivity to slight change for resisting brute-force attack. In order to test the key sensitivity, decrypt the encrypted image with new secret key obtained by changing the initial value of chaotic system. The decryption results are presented in Fig 9. It shown that the hacker cannot get the correct plaintext image when the secret key has slight change. Meanwhile, differences between error decryption image and original image are shown in TABLE.6.

Obviously, the plaintext image can't be recovered by using the slightly changed secret key. We can get form



(a) (b) (c)

FIGURE 8. Encryption Simulation test results (a) Original image (b) Encryption image (c) Decryption image.

TABLE 5. Table of key space.

Encryption scheme	Proposed algorithm	Ref. [13]	Ref. [14]	Ref. [17]	Ref. [19]	Ref. [24]	Ref. [33]	Ref. [39]	Ref. [48]
Key space	2^{685}	2^{576}	2^{327}	2^{453}	2^{159}	2^{373}	2^{256}	2^{186}	2^{279}

TABLE 6. Different of error decrypted image and plain image.

variables	$x+10^{-15}$	$y+10^{-15}$	$z+10^{-5}$	u_1+10^{-15}	u_2+10^{-15}	u_3+10^{-15}	u_4+10^{-15}	u_5+10^{-15}	u_6+10^{-15}
Comparison with plain image	99.62%	99.61%	99.61%	99.63%	99.62%	99.66%	99.65%	99.62%	99.60%

the TABLE.6 that more than 99% of the pixel values are different between error decryption image and original image. Therefore, the secret key of algorithm is highly sensitivity to slight changed.

C. STATISTICAL PERFORMANCE ANALYSIS

In this section, the statistical performance of the encryption algorithm is analyzed for measure the degree of confidentiality of the image information.

1) PIXEL DISTRIBUTION ANALYSIS

The histogram chart reflects the distribution of pixel values in the image. It can illustrate that the statistical information in image. The histogram of plaintext image and encrypted image is shown in Fig 10.

Where, the abscissa reflects pixel value, and the ordinate reflects distribution of pixel point in the image. As shown in Fig. 10(a), the distribution of the plaintext image is relatively concentrated in some areas. By comparing with Fig. 10(b),

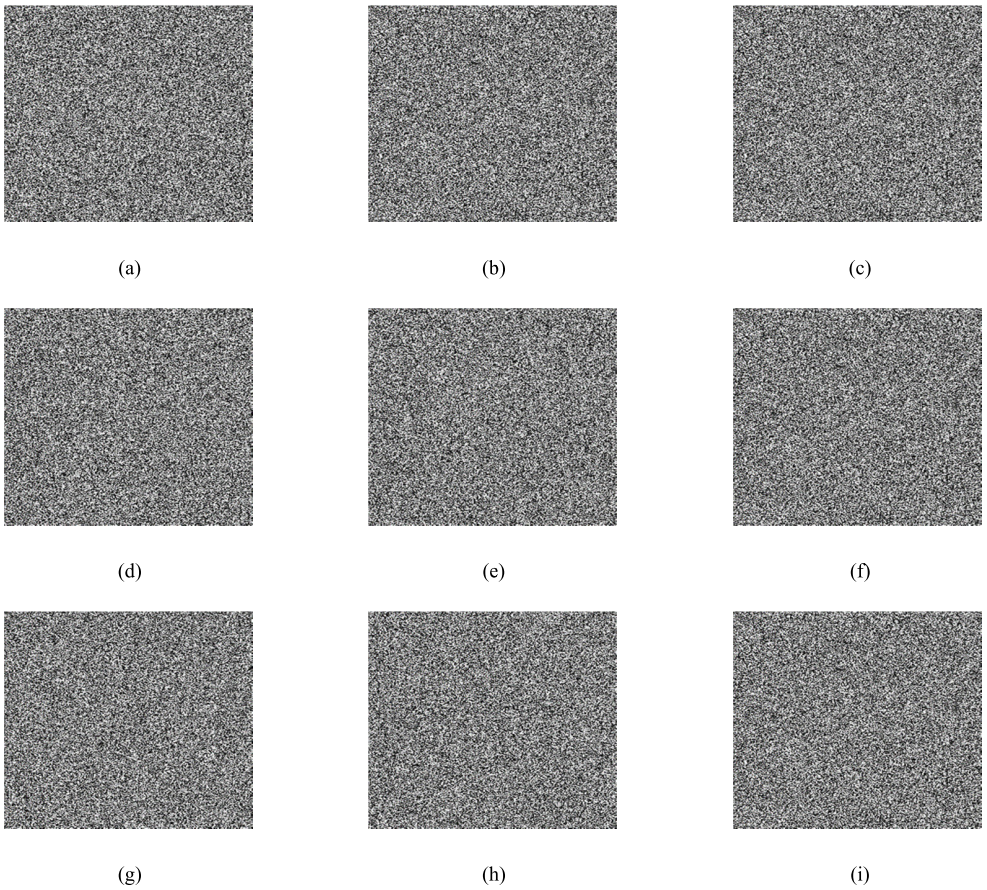


FIGURE 9. Simulation test results (a) Error decryption image ($x + 10^{-15}$) (b) Error decryption image ($y + 10^{-15}$) (c) Error decryption image ($z + 10^{-5}$) (d) Error decryption image ($u_1 + 10^{-15}$) (e) Error decryption image ($u_2 + 10^{-15}$) (f) Error decryption image ($u_3 + 10^{-14}$) (g) Error decryption image ($u_4 + 10^{-15}$) (h) Error decryption image ($u_5 + 10^{-14}$) (i) Error decryption image ($u_6 + 10^{-15}$).

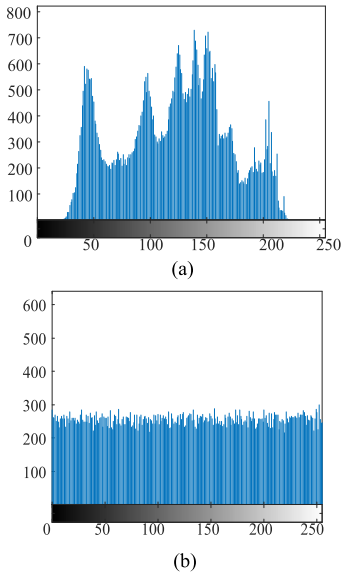


FIGURE 10. Histogram analysis results (a) Original picture histogram (b) encryption picture histogram.

it can be considered that the cipher image is uniformly distributed. The chi-square test is another method for measuring the uniformity. The critical value of freedom with 10%, 5% and 1% probability is 284.3360, 293.2478 and 310.4574 respectively. TABLE.7 shows that the chi-square value of different plaintext images. The results of χ^2 -values are smaller than the critical value of different probability. Therefore, the hypothesis is correct about the histogram of cipher image is uniform distribution Consequently, the proposed image encryption scheme could resist the statistical analysis attack.

2) ADJACENT PIXEL POINT CORRELATION ANALYSIS

For verify the correlation between the encrypted image and the original image. The image correlation coefficient is obtained as following.

$$r_{xy} = \frac{cov(x, y)}{\sqrt{D(X)D(Y)}}, \tag{19}$$

$$cov(x, y) = E\left\{[x - E(x)][y - E(y)]\right\}, \tag{20}$$

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

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

where, $E(x)$ and $D(x)$ are the expectation and variance of variable x respectively, and cov (x, y) is represent covariance.

TABLE 7. Chi-square result of different plaintext image.

Image name	χ^2-value (Plaintext Image)	χ^2-value (Cipher Image)	Critical Value		
			$\chi^2_{0.1}(255)$	$\chi^2_{0.05}(255)$	$\chi^2_{0.01}(255)$
Lena (256*256)	$4.2127*10^4$	227.3086	Pass	Pass	Pass
Pepper (256*256)	$5.3887*10^4$	237.3164	Pass	Pass	Pass
Plane (256*256)	$1.7950*10^5$	216.0586	Pass	Pass	Pass
Baboon (256*256)	$5.1009*10^4$	213.1328	Pass	Pass	Pass
Camera (256*256)	$1.1071*10^5$	215.0078	Pass	Pass	Pass

TABLE 8. Table of correlation coefficient.

Name	Plain image			Cipher image		
	Horizontal	Vertical	diagonal	Horizontal	Vertical	diagonal
Lena (256*256)	0.9460	0.9725	0.9321	-0.0022	-0.0073	0.0032
Pepper (256*256)	0.9677	0.9734	0.9479	-0.0053	-0.0034	0.0027
Plane (256*256)	0.9194	0.9012	0.8526	-0.0021	-0.0045	-0.0009
Baboon (256*256)	0.8827	0.8386	0.7945	-0.0057	-0.0077	0.0012
Camera (256*256)	0.9355	0.9592	0.9130	-0.0037	0.0087	0.0003

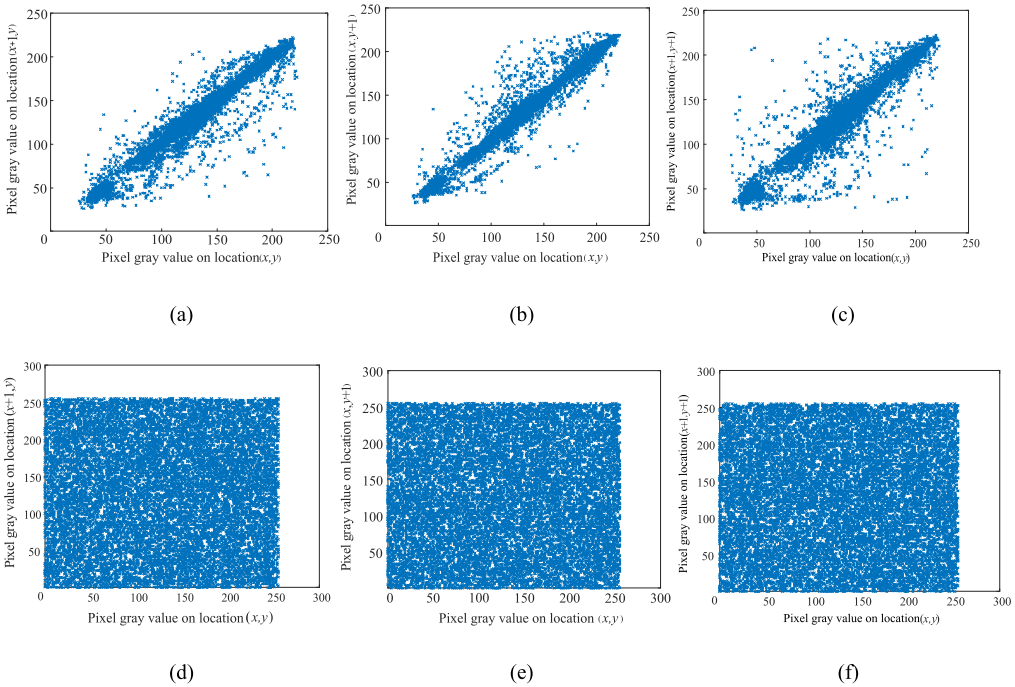


FIGURE 11. The correlation coefficient analysis results (a) the adjacent pixel distribution of a plaintext in horizontal direction, (b) the adjacent pixel distribution of a plaintext in vertical direction (c) the adjacent pixel distribution of a plaintext in diagonal direction (d) the adjacent pixel distribution of a ciphertext in horizontal direction (e) the adjacent pixel distribution of a ciphertext in vertical direction (f) the adjacent pixel distribution of a ciphertext in diagonal direction.

The correlation of two adjacent positions between the plaintext image and the encrypted image are illustrated in Fig 11.

TABLE.8 shows the correlation coefficient of cipher image. As can be seen from TABLE.8, the original image has strong correlation in different direction. Fig. 11(a-c) demonstrated that the distributed of pixel point is intensive. Conversely, the encryption image has low correlation, almost close to 0. Therefore, each pixel point of the encryption image does not have correlation.

TABLE.9 shows the compare results with another encryption scheme. Comparing with other encryption algorithm, the proposed algorithm can reduce the correlation in adjacent position effective.

TABLE 9. Table of compare with another scheme.

Algorithm	Direction		
	Horizontal	vertical	diagonal
Original image	0.9460	0.9725	0.9321
Proposed algorithm	-0.0022	-0.0073	0.0032
Ref. [15]	0.0036	0.0023	0.0039
Ref. [18]	-0.0048	-0.0112	-0.0045
Ref. [21]	0.0095	-0.0062	-0.0052
Ref. [34]	-0.0066	-0.0089	0.0424

D. ANTI-NOISE ATTACK PERFORMANCE ANALYSIS

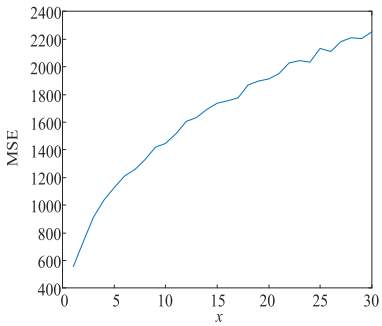
In this work, mean squared error (MSE) and peak signal-to-noise ratio are adopted to calculate the data when the cipher

image has interfered by noise signal. Those data are related to the quality of decrypted image. The formula of MSE and PSNR is as follows:

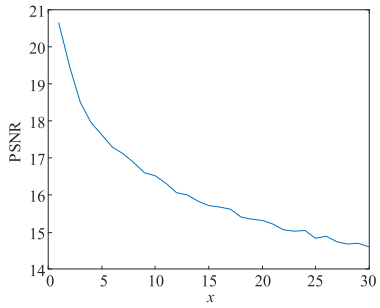
$$MSE = \frac{\sum_{i=1}^{n} (y_i - x_i)^2}{H*W}, \tag{23}$$

$$PSNR = 10 \lg \frac{255^2}{MSE}. \tag{24}$$

where x_i and y_i are the pixel value of plaintext image and cipher respectively. After simulation test, the spectrum of MSE and PSNR are shown in the Fig 12.



(a)



(b)

FIGURE 12. The spectrum of MSE and PSNR (a) MSE (b) PSNR.

Obviously, when the encrypted image is attacked by Gaussian white noise with an average value of 0 and a variance within the range of (0, 30), the value of MSE is grown and the value of PSNR decrease. The distribution of MSE and PSNR display that noise signal could affect the decryption progress and the quality of decrypted image is decline.

The other mathematical measure about image quality is cosine similarity, it used to calculate the similarity between the decrypted image which interfered by noise signal and original image. The equation of cosine similarity as follows.

$$\cos\theta = \frac{\sum_{i=1}^{n} (x_i, y_i)}{\sqrt{\sum_{i=1}^{n} x_i^2} \sqrt{\sum_{i=1}^{n} y_i^2}}, \tag{25}$$

where x_i is the decrypted image without any noise signal, and y_i is decrypted image with Gaussian noise signal. In ideal condition, the result of cosine similarity should be 1. The value of cosine similarity decrease is show that the noise signal influenced the cipher image. The quality of decrypted image is reduced.

The cosine similarity is demonstrated in the Fig 13, when cipher image affects by Gaussian white noise signal, the quality of decrypted image is broken. However, in simulation test, the decrypted image is obtained by proposed algorithm still can recognize the characteristic of plain image as show in the Fig 14.

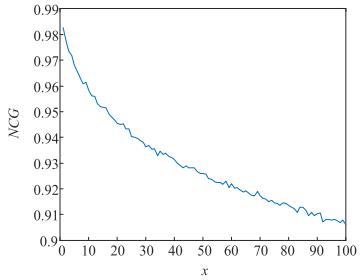


FIGURE 13. The spectrum of cosine similarity.

The decrypted image is obtained by cipher image which influence by 4% salt and pepper noise ignal, MSE is 1105.4708, PSNR is 17.6953, and the value of cosine similarity is 0.96796. The decrypted image is shown in the Fig 15.

E. INFORMATION ENTROPY ANALYSIS

Information entropy as a quantum of randomness is reflects the uncertainty of image information. Theoretically, the higher value of the entropy can prove the higher randomness for cipher image. The calculation of information entropy is

$$H(m) = \sum_{i=1}^{L-1} p(m) \log_2 \frac{1}{p(m_i)}. \tag{26}$$

where L represents the gray level. The $p(m)$ is the probability of gray value is appearing in the image matrix. For 8-bit gray image, denote $L = 256$, the theoretical value of information entropy should be close to 8. TABLE.10 is illustrated the value of information entropy in different image.

According to the TABLE.10 the information entropy of all encrypted image is close to the theoretical value 8. In order to measure the randomness more accurately, Wu et al. have proposed the modified Shannon entropy measure named local Shannon entropy and another research work is adopted [49]–[51]. It is obtained by computing non-overlapping blocks by randomly selected. The test results of local entropy are listed in TABLE.10. Based on the result of TABLE.10, the global entropy is close to theorical value and local entropy is acceptable in different significant level. TABLE.11 shows the comparison analyzes of proposed algorithm with other proposed algorithms.

TABLE 10. Table of information entropy.

Image name	Information entropy (Global)	Local entropy No. of Block=30 Block size=44*44	Critical Value		
			$h^{*-}_{0.05}$=7.9019 $h^{*+}_{0.05}$=7.9030	$h^{*-}_{0.01}$=7.9017 $h^{*+}_{0.01}$=7.9032	$h^{*-}_{0.001}$=7.9015 $h^{*+}_{0.001}$=7.9034
Lena (256*256)	7.9975	7.9023	Pass	Pass	Pass
Camera (256*256)	7.9976	7.9024	Pass	Pass	Pass
Pepper (256*256)	7.9974	7.9024	Pass	Pass	Pass
Baboon (256*256)	7.9977	7.9030	Pass	Pass	Pass
Airplane (256*256)	7.9976	7.9020	Pass	Pass	Pass

(a)

(b)

(c)

FIGURE 14. The decrypted image influence by white noise.

As shown in the TABLE.11, the proposed algorithm has great performance between other algorithms in cover information of plaintext image. It is means that the encrypted image obtained through proposed algorithm can't be decoded by attacker.

FIGURE 15. The decrypted image influence by salt & pepper noise.

TABLE 11. Table of information entropy.

Encryption scheme	Information entropy
Proposed algorithm	7.9975
Ref. [16]	7.9971
Ref. [17]	7.9972
Ref. [19]	7.9972
Ref. [24]	7.9973
Ref. [38]	7.9964
Ref. [52]	7.9954

TABLE 12. The plain image in different position.

	position				
	(138,180)	(147,76)	(163,50)	(138,180)	(89,113)
NPCR	99.60%	99.61%	99.62%	99.60%	99.66%
UACI	33.39%	33.30%	33.55%	33.39%	33.43%

TABLE 13. NPCR Values of different plaintext images.

Image name	NPCR (mean)	Pass rate		
		$NPCR^{*}_{0.05}$ =99.5693%	$NPCR^{*}_{0.01}$ =99.5527%	$NPCR^{*}_{0.001}$ =99.5341%
Lena (256*256)	99.61%	100.00%	100.00%	100.00%
Camera (256*256)	99.61%	95.00%	100.00%	100.00%
Pepper (256*256)	99.60%	95.00%	100.00%	100.00%
Baboon (256*256)	99.59%	85.00%	90.00%	100.00%
Airplane (256*256)	99.62%	95.00%	100.00%	100.00%

F. QUANTITATIVE ANALYSIS OF ANTI DIFFERENTIAL ATTACK

NPCR and UACI always are used to measure the performance for resisting the differential attack of this algorithm. The specific calculation method is shown as follows

$$NPCR = \frac{\sum_{i,j} D(i,j)}{L} \times 100\%, \tag{27}$$

$$UACI = \frac{1}{L}\sum_{i,j}\frac{|C(i,j) - C_1(i,j)|}{256} \times 100\%. \tag{28}$$

TABLE 14. Table of anti-difference attack analyze.

Image name	UACI (mean)	Pass rate		
		$UACI^{*-}_{0.05}$=33.2824 $UACI^{*+}_{0.05}$=33.6447	$UACI^{*-}_{0.01}$=33.2255 $UACI^{*+}_{0.01}$=33.7016	$UACI^{*-}_{0.001}$=33.1594 $UACI^{*+}_{0.001}$=33.7677
Lena (256*256)	33.43%	75.00%	90.00%	95.00%
Camera (256*256)	33.48%	100.00%	100.00%	100.00%
Pepper (256*256)	33.40%	80.00%	85.00%	100.00%
Baboon (256*256)	33.41%	100.00%	100.00%	100.00%
Airplane (256*256)	33.50%	100.00%	100.00%	100.00%

where $C(i, j)$ and $C_1(i, j)$ are the cipher images before and after one pixel of the plain image is changed, and W and H are the number of pixel point of row and column in image matrix respectively. $D(i, j)$ is symbolic function, the value of $D(i, j)$ is determined by equation (27)

$$D(i,j) = \begin{cases} 1 & C(i,j) \neq C_1(i,j) \\ 0 & C(i,j) = C_1(i,j). \end{cases} \tag{29}$$

The theoretical values of NPCR and UACI are 99.61% and 33.43%. For a plain image, the mean value of NCPR and UACI can be calculated by repeated calculation for 20 times, the value of pixel of plain image is changed randomly each time. The analysis results are given in TABLE.12 and TABLE.14 respectively.

According to the Ref. [25]–[27], [53], strictly critical NPCR and UACI score were adopted. Given a significance level a, the critical NPCR score is obtained as follows:

$$N_a^* = \frac{G - \Phi^1(\alpha)\sqrt{\frac{G}{L}}}{G+1}. \tag{30}$$

where G is the number of pixels in an image, L indicates the largest allowed pixel value. If NPCR value is greater than N^* a. This result can prove encryption scheme has ability to resist difference attack. The critical value of UACI with given a can be obtained from

$$\begin{cases} u_a^{*-} = \mu_u - \Phi^{-1}(\frac{\alpha}{2})\sigma_u \\ u_a^{*+} = \mu_u + \Phi^{-1}(\frac{\alpha}{2})\sigma_u, \end{cases} \tag{31}$$

where

$$\mu_u = \frac{G+2}{3G+3}, \tag{32}$$

And

$$\sigma_u = \frac{(G+2)(G^2+2G+3)}{18(G+1)^2GL}. \tag{33}$$

Theoretically, encryption algorithm can pass the test if the calculated UACI value is with the range (u^{*-}_a, u^{*+}_a). Based on TABLE.13 and 14, for the Lena (256*256), the mean value of NPCR is 99.61% and UACI is 33.43%. The results demonstrated that the algorithm can resist different-attack effectively.

TABLE.15 reveals the result compare with other encryption algorithms. In contrast, the encryption algorithm proposed in this study has better anti-differential attack performance than other encryption schemes, which means that the algorithm has higher security.

TABLE 15. Table of anti-difference attack analyze.

Encryption scheme	NPCR	UACI
Proposed algorithm	99.61%	33.43%
Ref. [12]	99.61%	33.53%
Ref. [16]	99.65%	33.38%
Ref. [21]	99.62%	33.49%
Ref. [35]	99.61%	33.46%
Ref. [36]	99.61%	33.42%
Ref. [37]	99.61%	33.46%
Ref. [54]	99.58%	33.56%

G. COMPUTATIONAL AND COMPLEXITY ANALYSIS

The computational cost of encryption algorithm depends on the scrambling and mutation operations. The analysis is performed in comparison with Ref. [50], [51], [55]. The time-consuming of the proposed algorithm mainly includes the cost time of the scrambling operation, the pixel diffusion operation and the DNA level diffusion.

The average execution time encryption of one round operation is 0.16s. It is smaller than 0.33s in Ref. [55]. TABLE.16 is illustrated the comparison of the average execution time of different image.

TABLE 16. Table of average execution time in one round.

Image name	Proposed algorithm	Ref. [55]
Lena (256*256)	0.16s	0.33s
Pepper (256*256)	0.18s	0.35s

Experiments are carried out in MATLAB R2018a in system with Intel Core i7 2.20GHz and 16GB RAM. The throughput of the proposed encryption scheme is 2.33Mb/s, which means the proposed scheme need 2.28 sec for encrypting 8bit depth 256 × 256 Lena image. Hence, the proposed algorithm is well suited for security application.

V. CONCLUSION

In this paper, a novel encryption algorithm for gray image has designed. To begin, the dynamical characterize analysis result show that the two different chaotic systems have good

dynamic characteristics including big parameter space and more complex dynamical behavior. Then, the encryption algorithm used Arnold matrix to scramble the order of plain matrix. DNA theory is used to change the value of pixel combine with complex chaotic system. The simulation experiment and security analysis show that the algorithm has a large key space and sensitivity to the secret key. Furthermore, the algorithm can resist common attacks, such as statistical, brute-force and anti-differential attack. Moreover, this algorithm has good characteristics of robustness, it can effectively resist the interference of noise signal and protect the image information. Therefore, this encryption scheme is convenient for implementation and large-scale application in private information protection.

AUTHOR CONTRIBUTIONS

Ji Xu designed and carried out experiments, data analyzed and manuscript wrote. Peng Li made the theoretical guidance for this paper. Feifei Yang and Huizhen Yan designed and improved the algorithm.

CONFLICTS OF INTEREST

No conflicts of interests about the publication by all authors.

REFERENCES

[1] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *J. Cryptol.*, vol. 4, no. 1, pp. 3–72, Jan. 1991.

[2] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 765. 1994, pp. 386–397.

[3] F. Sun, Z. Lü, and S. Liu, "A new cryptosystem based on spatial chaotic system," *Opt. Commun.*, vol. 283, no. 10, pp. 2066–2073, May 2010.

[4] C. Gentry, S. Halevi, and N. P. Smart, "Homomorphic evaluation of the AES circuit," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 7417, R. Safavi-Naini and R. Canetti, Eds. Berlin, Germany: Springer-Verlag, 2012, pp. 850–867.

[5] R. Matthews, "On the derivation of a 'chaotic' encryption algorithm," *Cryptologia*, vol. 8, no. 8, pp. 29–41, 1989.

[6] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006.

[7] G. Millerioux, J. M. Amigo, and J. Daafouz, "A connection between chaotic and conventional cryptography," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 55, no. 6, pp. 1695–1703, Jul. 2008.

[8] X. Xu and J. Feng, "Research and implementation of image encryption algorithm based on zigzag transformation and inner product polarization vector," in *Proc. IEEE Int. Conf. Granular Comput.*, Aug. 2010, pp. 556–561.

[9] G. Ye and K.-W. Wong, "An efficient chaotic image encryption algorithm based on a generalized Arnold map," *Nonlinear Dyn.*, vol. 69, no. 4, pp. 2079–2087, Sep. 2012.

[10] X.-Y. Ji, S. Bai, Y. Guo, and H. Guo, "A new security solution to JPEG using hyper-chaotic system and modified zigzag scan coding," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 22, no. 1, pp. 321–333, May 2015.

[11] D. Zhang and J. Zhang, "An improved algorithm of watermark preprocessing based on Arnold transformation and chaotic map," in *Proc. Int. Symp. Intell. Comput. Appl.*, 2015, pp. 241–247.

[12] X. Wang, Q. Wang, and Y. Zhang, "A fast image algorithm based on rows and columns switch," *Nonlinear Dyn.*, vol. 79, no. 2, pp. 1141–1149, 2015.

[13] P. Li, J. Xu, J. Mou, and F. Yang, "Fractional-order 4D hyperchaotic memristive system and application in color image encryption," *EURASIP J. Image Video Process., Jan*, vol. 2019, p. 22, Dec. 2019.

[14] F. Yang, J. Mou, C. Luo, and Y. Cao, "An improved color image encryption scheme and cryptanalysis based on a hyperchaotic sequence," *Phys. Scripta*, vol. 94, no. 8, Apr. 2019, Art. no. 085206.

[15] Q. Zhang, L. Guo, and X. P. Wei, "Image encryption using DNA addition combining with chaotic maps," *Math. Comput. Model.*, vol. 52, nos. 11–12, pp. 2028–2035, Dec. 2010.

[16] X.-Y. Wang, Y.-Q. Zhang, and Y.-Y. Zhao, "A novel image encryption scheme based on 2-D logistic map and DNA sequence operations," *Nonlinear Dyn.*, vol. 82, no. 3, pp. 1269–1280, Nov. 2015.

[17] Aqeel-ur-Rehman, X. Liao, A. Kulsoom, and S. Ullah, "A modified (Dual) fusion technique for image encryption using SHA-256 hash and multiple chaotic maps," *Multimedia Tools Appl.*, vol. 75, no. 18, pp. 11241–11266, Sep. 2016.

[18] A. Belazi, A. A. A. El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Process.*, vol. 128, pp. 155–170, Nov. 2016.

[19] A. Kulsoom, D. Xiao, Aqeel-Ur-Rehman, and S. A. Abbas, "An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules," *Multimedia Tools Appl.*, vol. 75, no. 1, pp. 1–23, Jan. 2016.

[20] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using dna sequence operations," *Opt. Lasers Eng.*, vol. 88, pp. 197–213, Jan. 2017.

[21] X. Chai, Z. Gan, Y. Lu, Y. Chen, and D. Han, "A novel image encryption algorithm based on the chaotic system and DNA computing," *Int. J. Mod. Phys. C*, vol. 28, no. 5, May 2017, Art. no. 1750069.

[22] W. Liu, K. Sun, Y. He, and M. Yu, "Color image encryption using three-dimensional sine ICMIC modulation map and DNA sequence operations," *Int. J. Bifurcation Chaos*, vol. 27, no. 11, 2017, Art. no. 1750171.

[23] L.-M. Zhang, K.-H. Sun, W.-H. Liu, and S.-B. He, "A novel color image encryption scheme using fractional-order hyperchaotic system and DNA sequence operations," *Chin. Phys. B*, vol. 26, no. 10, 2017, Art. no. 100504.

[24] Aqeel-ur-Rehman, X. Liao, M. A. Hahsmi, and R. Haider, "An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using DNA and chaos," *Optik*, vol. 153, pp. 117–134, Jan. 2018.

[25] L. Gong, K. Qiu, C. Deng, and N. Zhou, "An optical image compression and encryption scheme based on compressive sensing and RSA algorithm," *Opt. Laser Eng.*, vol. 121, pp. 169–180, Oct. 2019.

[26] Z.-J. Huang, S. Cheng, L.-H. Gong, and N.-R. Zhou, "Nonlinear optical multi-image encryption scheme with two-dimensional linear canonical transform," *Opt. Lasers Eng.*, vol. 124, Jan. 2020, Art. no. 105821.

[27] S.-S. Yu, N.-R. Zhou, L.-H. Gong, and Z. Nie, "Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system," *Opt. Lasers Eng.*, vol. 124, Jan. 2020, Art. no. 105816.

[28] S. Su, A. Lin, and J.-C. Yen, "Design and realization of a new chaotic neural encryption/decryption network," in *Proc. IEEE Asia–Pacific Conf. Circuits Syst. (APCCAS)*, Dec. 2000, pp. 335–338.

[29] C. Li, S. Li, D. Zhang, and G. Chen, "Cryptanalysis of a chaotic neural network based multimedia encryption scheme," in *Advances in Multimedia Information Processing* (Lecture Notes in Computer Science), vol. 3333. 2004, pp. 418–425.

[30] S. Lian, G. Chen, A. Cheung, and Z. Wang, "A chaotic-neural-network-based encryption algorithm for JPEG2000 encoded images," in *Proc. Int. Symp. Neural Netw.*, 2004, pp. 627–632.

[31] X. Chai, X. Zheng, Z. Gan, D. Han, and Y. Chen, "An image encryption algorithm based on chaotic system and compressive sensing," *Signal Process.*, vol. 148, pp. 124–144, Jul. 2018.

[32] S. E. Borujeni and M. Eshghi, "Chaotic image encryption design using Tompkins-Paige algorithm," *Math. Problems Eng.*, vol. 2009, Jul. 2009, Art. no. 762652.

[33] A. Akhshani, A. Akhavan, S. C. Lim, and Z. Hassan, "An image encryption scheme based on quantum logistic map," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 17, no. 12, pp. 4653–4661, 2012.

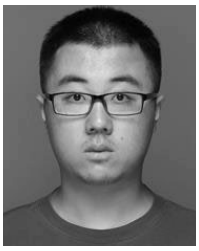
[34] Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, "2D Sine Logistic modulation map for image encryption," *Inf. Sci.*, vol. 297, pp. 80–94, Mar. 2015.

[35] W. Liu, K. Sun, and C. Zhu, "A fast image encryption algorithm based on chaotic map," *Opt. Lasers Eng.*, vol. 84, pp. 26–36, Sep. 2016.

[36] C. Cao, K. Sun, and W. Liu, "A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map," *Signal Process.*, vol. 143, pp. 122–133, Feb. 2018.

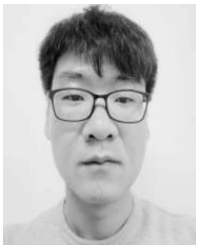
[37] Q. Xu, K. Sun, C. Cao, and C. Zhu, "A fast image encryption algorithm based on compressive sensing and hyperchaotic map," *Opt. Lasers Eng.*, vol. 121, pp. 203–214, Oct. 2019.

[38] X.-Y. Wang, L. Yang, R. Liu, and A. Kadir, "A chaotic image encryption algorithm based on perceptron model," *Nonlinear Dyn.*, vol. 62, no. 3, pp. 615–621, 2010.
[39] C. Zhu, "A novel image encryption scheme based on improved hyperchaotic sequences," *Opt. Commun.*, vol. 285, no. 1, pp. 29–37, 2012.
[40] A. C. Fowler, J. D. Gibbon, and M. J. McGuinness, "The complex Lorenz equations," *Phys. D, Nonlinear Phenomena*, vol. 4, no. 2, pp. 139–163, 1982.
[41] A. Rauh, L. Hannibal, and N. Abraham, "Global stability properties of the complex Lorenz model," *Phys. D, Nonlinear Phenomena*, vol. 99, no. 1, pp. 45–58, Dec. 1996.
[42] J. Liu, S. Liu, and F. Zhang, "A novel four-wing hyperchaotic complex system and its complex modified hybrid projective synchronization with different dimensions," *Abstract Appl. Anal.*, vol. 2014, Jun. 2014, Art. no. 257327.
[43] M. V. Berry, N. L. Balazs, M. Tabor, and A. Voros, "Quantum maps," *Ann. Phys.*, vol. 122, no. 1, pp. 26–63, Sep. 1979.
[44] M. Goggin, B. Sundaram, and P. Milonni, "Quantum logistic map," *Phys. Rev. A, Gen. Phys.*, vol. 41, no. 10, May 1990, Art. no. 5705.
[45] A. Akhshani, A. Akhavan, A. Mobaraki, S.-C. Lim, and Z. Hassan, "Pseudo random number generator based on quantum chaotic map," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, no. 1, pp. 101–111, Jan. 2014.
[46] A. Zaghloul, T. Zhang, M. Amin, and A. A. A. El-Latif, "Color encryption scheme based on adapted quantum logistic map," *Proc. SPIE*, vol. 9159, Apr. 2014, Art. no. 915922.
[47] S. M. Seyedzadeh, B. Norouzi, M. R. Mosavi, and S. Mirzakuchaki, "A novel color image encryption algorithm based on spatial permutation and quantum chaotic map," *Nonlinear Dyn.*, vol. 81, nos. 1–2, pp. 511–529, 2015.
[48] G. Bhatnagar and Q. J. Wu, "Chaos-based security solution for fingerprint data during communication and transmission," *IEEE Trans. Instrum. Meas.*, vol. 61, no. 4, pp. 876–887, Apr. 2012.
[49] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan, and P. Natarajan, "Local Shannon entropy measure with statistical tests for image randomness," *Inf. Sci.*, vol. 222, pp. 323–342, Feb. 2013.
[50] D. Ravichandran, P. Praveenkumar, J. B. Balaguru Rayappan, and R. Amirtharajan, "Chaos based crossover and mutation for securing DICOM image," *Comput. Biol. Med.*, vol. 72, pp. 84–170, May 2016.
[51] D. Ravichandran, P. Praveenkumar, and J. B. B. Rayappan, "DNA chaos blend to secure medical privacy," *IEEE Trans. Nanobiosci.*, vol. 16, no. 8, pp. 850–858, Dec. 2017.
[52] X. Wang, L. Liu, and Y. Zhang, "A novel chaotic block image encryption algorithm based on dynamic random growth technique," *Opt. Lasers Eng.*, vol. 66, pp. 10–18, Mar. 2015.
[53] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Inf. Sci.*, vol. 480, no. 1, pp. 403–419, Apr. 2019.
[54] L. Yaru and W. Jianhua, "Image encryption based on compressive sensing and variable parameter chaotic mapping," *J. Optoelectron. Laser Tianjin*, vol. 26, no. 3, pp. 605–610, Mar. 2015.
[55] H. Natiq, N. M. G. Al-Saidi, M. R. M. Said, and A. Kilicman, "A new hyperchaotic map and its application for image encryption," *Eur. Phys. J. Plus*, vol. 133, no. 1, p. 6, Jan. 2018.



JI XU received the B.E degree from the Shengli College China University of Petroleum, China, in 2017. He is currently pursuing the Ph.D. degree with Dalian Polytechnic University, Dalian, China. His mainly research interests include chaos theory and chaotic digital image cryptosystem.

PENG LI received the B.S., M.S., and Ph.D. degrees in information and communication engineering from the Harbin Institute of Technology, Harbin, China. He is currently an Associate Professor with the School of Information Science and Engineering, Dalian Polytechnic University, Dalian, China. His mainly research interests include multihop networks, image processing, and complex networks.



FEIFEI YANG received the B.E. degree from Longdong University, Qingyang, China, in 2016. He is currently pursuing the Ph.D. degree in control science and engineering with Dalian Polytechnic University, Dalian, China. His mainly research interest includes chaos theory and application.

HUIZHEN YAN received B.S. and M.S. degrees from Xi'an Jiaotong University (XJTU), Xi'an, China, and the Ph.D. degree in applied mathematics from Northeastern University (NEU), Shenyang, China, in 2000. She is currently a Professor with the School of Information Science and Engineering, Dalian Polytechnic University. Her research interests include game theory and its application and ecological mathematics.