Research on image encryption algorithm based on a class of three-dimensional quadratic polynomial chaotic system

Zhongtang Chen[1], Yu Zhu[1,2], Shuang Chen,Yandan Wang

1. Shenyang jainzhu university, Shenyang 110168
E-mail: chen630609@163.com

2. Shenyang jainzhu university,Shenyang 1110168
E-mail: zhuyuit@163.com

Abstract: In this paper, a novel three-dimensional quadratic polynomial chaotic system without equilibrium point is constructed, and a new image encryption algorithm is proposed based on this chaotic system. With the help of the randomness of chaotic system, the algorithm can only complete the encryption process by diffusion processing based on XOR operation. Security analysis is carried out from three aspects: key space, statistical analysis and sensitivity analysis. The results show that the encryption algorithm can effectively resist exhaustive key attacks because of a large key space, which means higher security and certain application value.

Key Words: Polynomial System, Image Encryption, Safety Analysis

1 INTRODUCTION

In 1917, Mauborgne and Vernam invented the technique of one-Time pads[1]. The idea of this technique is that for any plaintext message, a cipher with the same volume as the plaintext message should be generated, and the cipher with the same volume can be obtained through xor operation. In 1949, Shannon, the great founder of information theory, pointed out that the core of a secure communication system is information encryption. Only the key is private and protected, and the communication channel, communication content and even encryption algorithm and decryption algorithm are all public. In 1989, Matthews proposed the method of generating a large number of pseudorandom Numbers by using the chaotic system to determine the parameters and initial values of the chaotic system as the key of the cryptographic system, thus greatly reducing the length of the key. The application of chaotic system in cryptosystem has solved the difficult problem of how to generate a large number of random Numbers with good statistical properties left by one -time encryption technology. From then on, chaotic system began to combine with encryption system, and created a new method of generating pseudo-random Numbers in chaotic system. In 1998, Baptista proposed the ergodic encryption character algorithm based on chaotic system, where one-dimensional Logistic mapping was used. In 2008, Massoudi et al. reviewed the selective encryption algorithm of image encryption system[3]. Behnia et al. proposed an algorithm to generate cryptographic sequences by means of chaotic coupled mapping and single chaotic mapping. Tong et al. further proposed an algorithm for generating cipher sequences by means of composite chaotic maps. In 2009, Wang et al. proposed a method of generating cipher sequences by combining four one-dimensional chaotic maps[4]. In 2010, Wang et al. proposed an image encryption algorithm combined with the neuron model. Tong et al. studied a new combined chaotic system and confirmed that the maximum Lyapunov exponent of the chaotic system was higher than that of Logistic. Liao et al. proposed a method to transform the gray value of pixels with the discrete value of sinusoidal waveform. Yuan et al. Proposed a new five dimensional hyperchaotic parallel image encryption system. After image pixel classification, the same level pixels can perform encryption operation at the same time, which improves the encryption speed and security performance.

There are still a lot of researches on image cryptosystem focusing on chaotic cryptosystem. It can be seen that cryptosystem sequence plays an important role in image cryptosystem. Research idea of this paper focus on the excavation of the new chaotic system, based on no balance is constructed of three dimensional quadratic polynomial chaotic systems[2], chaos characteristic show that the system has a good applied to image encryption, after the simulation experimental results show that the system can effectively resist exhaustive key attacks, produce a large key space and gain a good encryption effect.

2 A THREE-DIMENSIONAL QUADRATIC POLYNOMIAL CHAOTIC SYSTEM

In this paper, a three-dimensional quadratic polynomial system with five nonlinear terms and two constant terms is constructed and the polynomial (1) is shown in the equation with seven parameters, a , b , c , d , m , p and q .

$$\begin{cases} \dot{x} = axy + byz \\ \dot{y} = cxz + dyz + p \\ \dot{z} = mxy + q \end{cases} \tag{1}$$

This work is supported by Nature Science Foundation of Liaoning Province of China under Grant No.20180550060

978-1-6654-4089-9/21/$31.00 ©2021 IEEE

The system has seven terms, including five quadratic terms and two constant terms which all satisfy the following four conditions simultaneously.

$$abcdmpq \neq 0 \tag{2}$$

$$abc > 0 \tag{3}$$

$$bm < 0 \tag{4}$$

$$adq + pbm > 0 \tag{5}$$

While $a=-1$, $b=-8$, $c=1$, $d=0.1$, $m=1$, $p=-20$, $q=38$ and the initial condition is $(x_0, y_0, z_0)=(1,1,1)$,the system can generate a new chaotic attractor shown in Figure 1,the projection on the $x-y$ is shown in Figure 2,the projection on the $x-z$ is shown in Figure 3 and on the $y-z$ is shown in Figure 4.

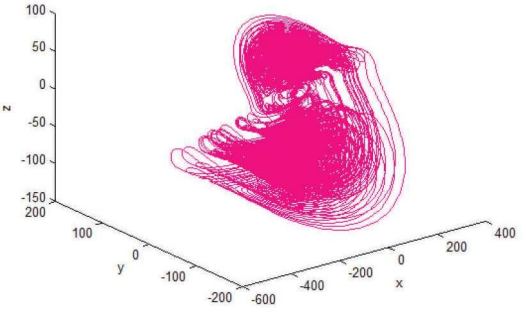


Fig 1. A new chaotic attractor

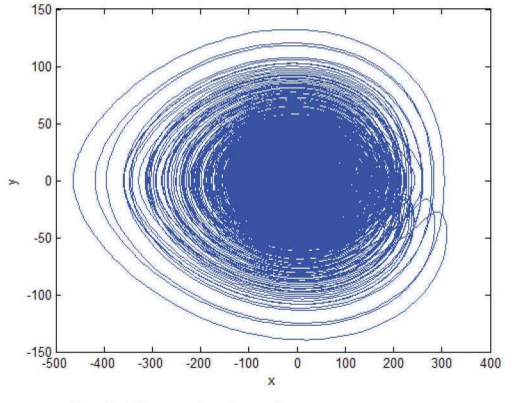


Fig 2. The projection of attractor on $x-y$

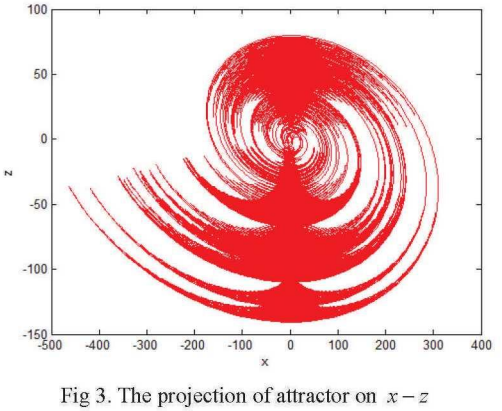


Fig 3. The projection of attractor on $x-z$

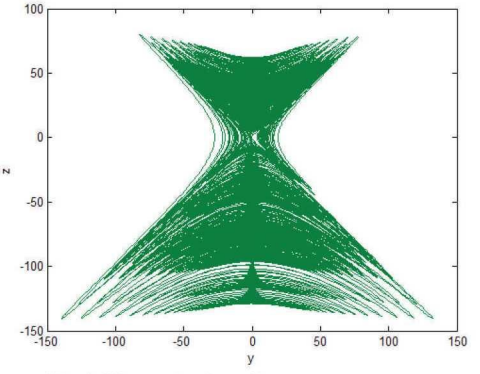


Fig 4. The projection of attractor on $y-z$

Lyapunov exponent is an important tool to determine whether the chaos in dynamical systems is exist.In order to verify the existence of chaos in the system, three Lyapunov exponents are calculated , $LE_1 = 0.7816$, $LE_2 = -0.0453$ and $LE_3 = -1.944$ .It turns out that the system is chaotic because the LE_1 is positive.

3 ENCRYPTION AND DECRYPTION

3.1 Diffusion Algorithm

The purpose of diffusion processing is to hide the information of any plaintext pixel in the ciphertext pixel as much as possible without changing the pixel position[7]. The diffusion algorithm used in the encryption process in this paper is shown in the equation (6):

$$C_i = C_{i-1} \oplus S_i \oplus P_i \tag{6}$$

Where P is one-dimensional vector of plaintext expansion, S denotes the key vector, C is the ciphertext vector, C_0 comes from the key and $i=1,2,\cdots,M*N$.

The following relation can be obtained from the equation (6):

$$C_1 = C_0 \oplus S_1 \oplus P_1 \tag{7}$$

$$C_2 = C_0 \oplus S_1 \oplus S_2 \oplus P_1 \oplus P_2 \tag{8}$$

$$C_3 = C_0 \oplus S_1 \oplus S_2 \oplus S_3 \oplus P_1 \oplus P_2 \oplus P_3 \tag{9}$$

$$C_n = C_0 \oplus S_1 \oplus \cdots \oplus S_n \oplus P_1 \oplus \cdots \oplus P_n \tag{10}$$

It can be shown clearly that the plaintext pixel P_1 is diffused into $C_1, C_2, \cdots, C_{M*N}$,which is diffused into all the pixels of ciphertext, P_2 is diffused into $C_2, \cdots, C_{M*N}$,and so on, P_{M*N} is only hidden in C_{M*N} ,which also means the diffusion is limited.To solve the problem,the diffusion method of the equation (6) is used twice in this paper.The intermediate ciphertext vector C ,firstly,is obtained by forward diffusion and assigned to P ,secondly,backward diffusing P which is lately assigned.The pixel P_{M*N} is hidden in $C_{M*N}, C_{M*N-1}, \cdots, C_1$,the pixel P_{M*N-1} is hidden in $C_{M*N-1}, C_{M*N-2}, \cdots, C_1$,likewise,the pixel P_1 is hidden only in C_1 during the backward diffusion. In this way,the

information of each plaintext pixel is diffused to each ciphertext pixel in theory after twice diffusion.

The encryption algorithm is shown in equation (11) and (12). Where, C_i obtained in equation (11) is assigned to P_i in equation (12).

$$C_i = C_{i-1} \oplus S_i \oplus P_i \tag{11}$$

$$C_i = C_{i+1} \oplus S_i \oplus P_i \tag{12}$$

The decryption algorithm is shown in equation (13) and (14). Among them, equation (13) is the inverse process of (11), and equation (14) is the inverse process of (12).

$$P_i = C_{i-1} \oplus C_i \oplus S_i \tag{13}$$

$$P_i = C_{i+1} \oplus C_i \oplus S_i \tag{14}$$

3.2 Encryption Scheme

In this section, an encryption scheme based on the polynomial system is designed in detail by the diffusion algorithm in section 3.1. In this case, the chaotic sequences in x direction and y direction generated by the chaotic system, which are defined as sequence S_1 and sequence S_2 respectively.The sequence S_1 is used to forward diffusion and S_2 is used to backward diffusion , C_1 denotes the intermediate result after the forward diffusion, C stores the information of ciphertext and P denotes the plaintext.The encryption process is shown in Figure 5.

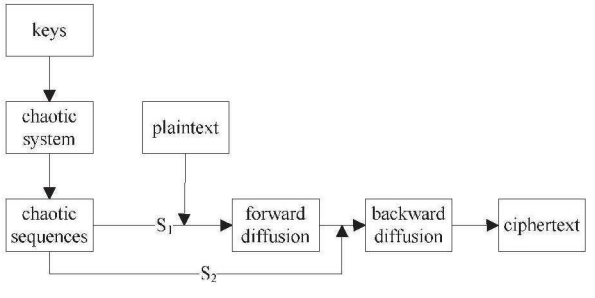


Fig 5.encryption process

Step1: Fetch the plaintext data, save it in the matrix, get the size of the matrix as $[M, N]$ and expand the matrix by column and write it as P .

Step 2:The chaotic system is used to iteratively generate the sequences with length $M * N$ in x direction and y direction, which are denoted as S_1 and S_2 .

Step 3:Let $C_0' = 0$,then $C_1' = C_0' \oplus S_1 \oplus P_1$,do the forward diffusion according to the equation (11),assign C' to P and let $C_0 = 0$,then $C_{M*N} = C_0 \oplus S_{2_{M*N}} \oplus P_{M*N}$,finally get the ciphertext vector C after the backward diffusion according to the equation (12) and the encryption is totally completed.

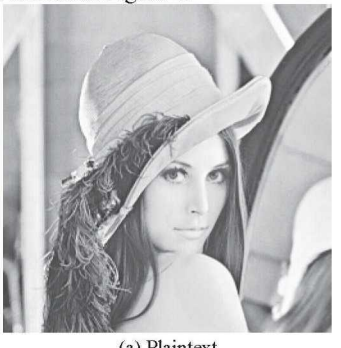
Step 4:While decrypting vector D saves the intermediate result,vector E saves the restored image. Let $D_0 = 0$ and $E_0 = 0$,then $D_{M*N} = D_0 \oplus S_{1_{M*N}} \oplus C_{M*N}$,the decryption is done according to (15) and (16), $E_1 = E_0 \oplus S_{11} \oplus D_1$, the decryption is totally completed., and, decrypt according to equations (15) and (16), respectively, until decryption is completed.

$$D_i = C_{i+1} \oplus S_{2_y} \oplus C_i \tag{15}$$

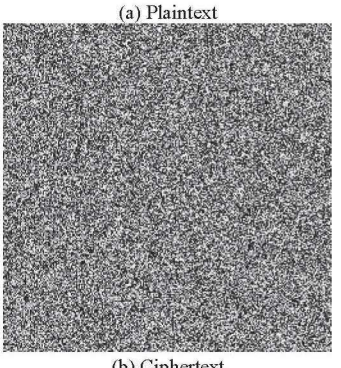
$$E_i = D_{i-1} \oplus S_i \oplus D_i \tag{16}$$

4 SIMULATION RESULT

In this paper, Lena gray-scale image (256 × 256) is used for experimental verification. The effect of encryption and decryption is shown in Figure 6.



(a) Plaintext



(b) Ciphertext

(c) Restore image

Fig 6. image encryption effect

5 SAFETY ANALYSIS

In this paper, key space analysis, statistical analysis and sensitivity analysis are used to detect the security of encryption scheme. The statistical analysis includes histogram analysis, ciphertext information entropy analysis, correlation analysis of adjacent pixels.

5.1. Key Space Analysis

The key space is the collection of all keys in image cryptography system. If the key space is small, the number

of keys will be less, and the corresponding image cryptography system can not resist the exhaustive key attack. The parameter precision of the system is set to 10^{-14}, and the key space is $10^{14} \times 10^{14} \times 10^{14} \approx 2^{138}$. Such a large key space is enough to resist exhaustive key attack.

5.2. Information Entropy

For a random variable x, its entropy is denoted as $H(x)$, indicating the uncertainty or information quantity of the variable. The calculation formula of entropy of random variable is shown in (17).

$$H(x) = -\sum_{i=1}^{n} p_i \log_2 p_i \tag{17}$$

In this equation, we take the base 2 Logarithm, and the unit of entropy is the bit. The probability that the random variable x has a value of x_i is $p_i, i = 1,2,\cdots,n, 0 < p_i < 1$, $p_1 + p_2 + \cdots + p_n = 1$.

The maximum entropy of gray image is 8 bits, and only when the gray values obey uniform distribution, the entropy of gray image reaches the maximum value. The ratio of entropy of random variable x to the maximum value of entropy of random variable x becomes the relative entropy of random variable x. the difference between 1 and relative entropy is called redundancy of the sequence.

The information entropy, relative entropy and redundancy information of the encrypted image compared to others are shown in Table 1.

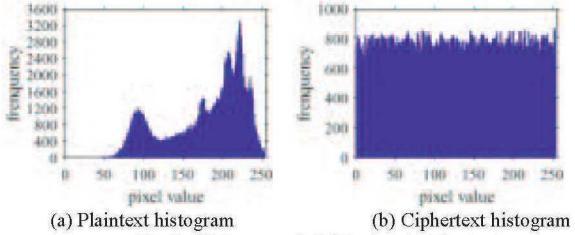
Table 1. Information entropy of ciphertext compared to others

	Proposed Algorithm	Reference11	Reference14
entropy	7.9976	7.9964	7.9896

It can be seen from Table 1 that the information entropy of ciphertext is very close to the ideal value, which indicates that the grayscale distribution of ciphertext image is uniform, and that the image information is not easy to be stolen and the encryption effect is good.

5.3. Histogram Analysis

Histogram can reflect the pixel distribution of the image. The more uniform the pixel distribution is, the better the encryption effect is. In this paper, the intensity distribution of Lena and the intensity distribution of the encrypted image are plotted, as shown in Figure 7.



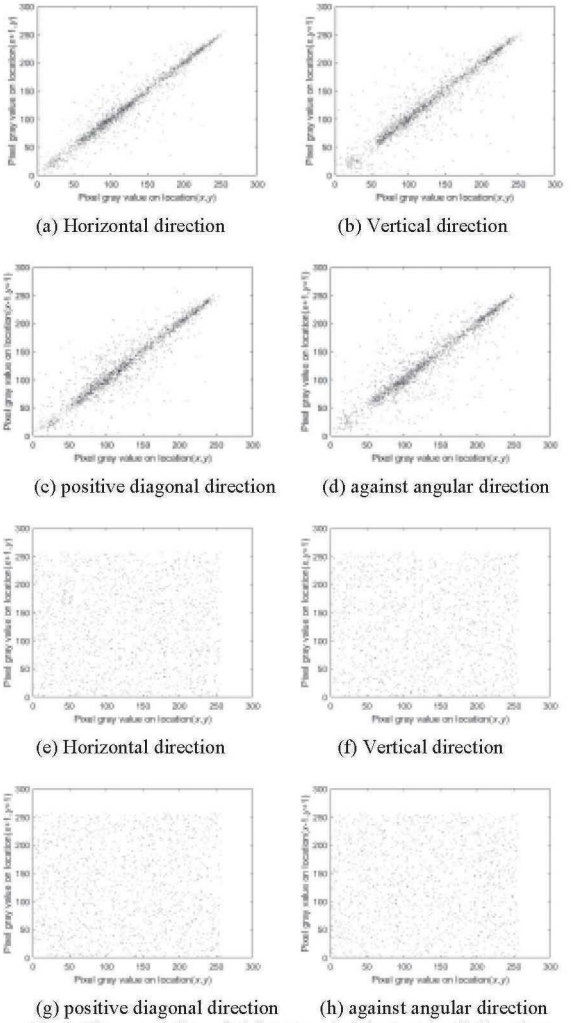
(a) Plaintext histogram (b) Ciphertext histogram

Fig 7. .Histogram of plaintext and ciphertext

It can be seen that the histogram of the plaintext image is right-biased and has obvious statistical characteristics, while the frequency of each pixel in the histogram of the cipher image is basically equal to that of each gray level, and the histogram has no obvious statistical characteristics, so it can withstand a statistical attack.

5.4. Correlation Analysis of Adjacent Pixels

Generally, there is a strong correlation between the adjacent pixels in the horizontal, vertical, positive diagonal and anti angle directions of plaintext image, but there should be no correlation between the adjacent pixels in the ciphertext image. Figure 8 shows the correlation of plaintext and ciphertext in all directions.



(a) Horizontal direction (b) Vertical direction

(c) positive diagonal direction (d) against angular direction

(e) Horizontal direction (f) Vertical direction

(g) positive diagonal direction (h) against angular direction

Fig 8. The correlation of plaintext and ciphertext in all directions

As can be seen in figure 8, pairs of adjacent Pixel pairs in each direction of the plaintext image are clustered on the $y = x$ line, however, the pairs of adjacent pixels in each direction are scattered in the rectangle (the lower-left coordinate is (0,0), the upper-right coordinate is (255,255)), which shows that the plaintext images have strong correlation in each direction, the correlation coefficient of the adjacent pixels of the encrypted image is close to 0, which indicates that the encryption algorithm based on the chaotic system conceals the original information of the plaintext image, it has good performance of uniform distribution.

5.5. Key Sensitivity Analysis

Quantifying the difference between two images of the same size can be accomplished by calculating NPCR and UACI values. If two images of the same size are recorded as P_1 and P_2, and the Pixel values at the midpoint (i,j) of the image are $P_1(i,j)$ and $P_2(i,j)$, respectively, and the image size is $M \times N$, then the formulas for NPCR and UACI are shown in formulas (18) and (19).

$$NPCR = \frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N} \left| Sign(P_1(i,j) - P_2(i,j)) \right| \times 100\%$$

$$Sign(x) = \begin{cases} 1, & x > 0 \\ 0, & x = 0 \\ -1, & x < 0 \end{cases} \quad (18)$$

$$UACI = \frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{\left| P_1(i,j) - P_2(i,j) \right|}{255} \times 100\% \quad (19)$$

If both images are random, the ideal expectation of NPCR is 99.6094% and the ideal expectation of UACI is 33.4635%.

The key sensitivity analysis aims to analyze the difference between two ciphertext images obtained by encrypting the same plaintext image when the key changes slightly. If the difference between the two ciphertext images is significant, it is said that the key sensitivity of the image cryptography system is strong, otherwise, the key sensitivity is poor.

In this paper, the sensitivity of x_0, y_0, z_0 in the key set is very high, and the precision can reach 10^{-14} .it takes the key set as $\{1+10^{-14}, 1, 1\}$, $\{1, 1+10^{-14}, 1\}$, $\{1, 1, 1+10^{-14}\}$ to encrypt the same plaintext image, and the calculated NPCR value and UACI value are shown in Table 2. It can be seen from Table 2 that the NPCR and UACI values are in line with the expected values in the near future, indicating that the key sensitivity of the encryption algorithm system is strong.

Table 2. Measurement results of NPCR and UACI when the key changes slightly

$x_0, y_0 z_0$	NPCR	UACI
$1+10^{-14}, 1, 1$	99.55895	33.59785
$1, 1+10^{-14}, 1$	99.64599	26.76270
$1, 1, 1+10^{-14}$	99.58343	26.80466

6 CONCLUSION

In this paper, a new 3-d quadratic polynomial chaotic system without equilibrium point is constructed and the attractor of the system in this case is usually called hidden attractor, which is more complex than 1-d and 2-d chaotic systems. Based on the chaotic system, the image is encrypted by xor operation, and the implementation of the encryption algorithm is verified by simulation, and the related performance indexes show the validity and security of the encryption system, in the future image encryption field has the application value.

REFERENCES

[1] X. Y. Wang. Chaos in complex nonlinear systems [M]. Beijing: Electronic Industry Press, 2003:1-46.

[2] Z. T. Chen,Z. Li, C. C. Sun. Analysis and Control of a Three-Dimensional Quadratic Polynomial System with No Equilibrium Point and No Linear Term,2020 Chinese Control And Decision Conference (CCDC), 2020.

[3] Y. Wang. Research on chaotic encryption algorithm and hash function construction [M]. Beijing: Electronic Industry Press, 2011.

[4] J. Q. Li. Data security and application based on chaos [M]. Beijing: National Defense Industry Press, 2017.

[5] Y. Zhang. Detailed explanation of digital image cipher algorithm: Based on C, c#T and MATLAB [M]. Beijing: Tsinghua University Press, 2019.

[6] H. J. Liu. Chaos synchronization and its application in image encryption [M]. Shenyang: Liaoning science and Technology Press, 2017.

[7] Y. Zhang. Chaotic digital image encryption [M]. Beijing: Tsinghua University Press, 2016.

[8] L. Huang. Image encryption algorithm based on chaotic mapping and continuous symmetric diffusion [J]. Journal of Heilongjiang Institute of Technology (Comprehensive Edition), 2019,19 (03): 58-63.

[9] S. Q. Zhu,J. Q. Li. A clear text attack and improvement of a chaotic image encryption algorithm [j]. Computer engineering and application, 2017 (24): 118-126.

[10] L. Tu,C. Zhang,L. Y. Jia. Image encryption algorithm based on two-dimensional generalized logistic mapping [J]. Control engineering, 2014 (2): 279-282.

[11] P. Liu. Image encryption algorithm based on Chaos Theory and des [J]. Computer and modernization, 2013 (8): 184-191.

[12] C. X. Zhu. Cryptanalysis and improvement of a kind of Hyperchaotic image encryption algorithm [J]. Acta physica Sinica, 2012,61 (12): 76-87.

[13] H. J. Tian,P. Lei,Y. Wang. Image encryption algorithm based on chaos and DNA dynamic coding [J]. Journal of Jilin University (Engineering Edition), 2014,44 (3): 801-806.

[14] C. J. Hu,X. Chen,Y. Guo. Optical image encryption algorithm based on multi chaotic mapping. Journal of laser, 2017,38 (1): 110-114.

[15] Zhu Xiaosheng, Liao Xiaofeng. Scrambling algorithm based on image partition. Computer technology and development, 2015,25 (12): 52-55,59.

[16] J. Wang, G. P. Jiang. Security analysis and improvement of a hyperchaotic image encryption algorithm. Acta physica Sinica, 2011,60 (6): 83-93.

[17] Kanso A, Gheblen M. A novel image encryption algorithm based on a 3D chaotic map. Communications in Nonlinear Science and Numerical Simulation, 2012,17(7):2943-2959.

[18] T. G. Pan,G. Y. Li. Bit transform image encryption algorithm based on chaos theory [J]. Journal of electrical machinery and control, 2013, 17 (10): 97-100.