A gray image encryption algorithm based on 3D chaotic map and DNA operations

Yuwen Sha[1] , Yinghong Cao[2] , Huizhen Yan[3]

{dlpusyw@sina.com[1], caoyinghong@dlpu.edu.cn[2], yanhz@dlpu.edu.cn[3]}

School of Information Science and Engineering, Dalian polytechnic University,

Dalian, 116034, China

Abstract. In this paper, a new gray image encryption system based on 3D chaotic map and deoxyribonucleic acid (DNA) sequence operations is presented. SHA is designed to give the initial value of the encryption system. The whole algorithm is designed based on permutation and diffusion framework. First, modify the chaotic sequence generated by the chaotic system, and the Arnold function is permuted the plane image. Secondly, DNA level diffusion is introduced, we start by performing a DNA XOR on the DNA coding image. Lastly, decoding is performed on the diffused DNA matrix. The results of experiment and analyses indicate that our encryption algorithm can pass the attack tests and has a certain application prospect.

Keywords: Image encryption, 3D chaotic map, DNA XOR.

1 Introduction

With the advent of the electronic information age, the ways of information exchange have been constantly enriched. In the process of communication, a large amount of information comes along, and the security of transmission and storage of the information on the Internet is threatened. Compared with the encryption of digital images, text images already have classical encryption algorithms, such as RSA, DES, IDEA [1]. Due to the digital image information not only has the characteristics of huge amount of data, but also has strong correlation and redundancy. This makes the encryption technology based on text image difficult to meet the needs of image encryption. Therefore, how to ensure that these private images are not attacked and stolen in the transmission process has become a research hotspot [2, 3]. This makes more and more cryptographers keen on designing a secure and effective image encryption method. Recently, after the study of scholars in the image encryption field of many novel technologies, including optical transform, chaotic systems, DNA computing, compressive sensing Fourier transform, cellular automata, wavelet transform.

Encryption and decryption of digital images require a large number of passwords that are the same size as the plaintext. How to produce pseudo random numbers with good statistical characteristics has become an urgent demand for digital image encryption. Chaotics complex structure, difficult to analyze and predict, can produce a large number of passwords, so it is used in the field of digital data encryption. In 1978, R.Matthews put forward a generalized

EAI GreeNets 2021, June 06-07, Dalian, People's Republic of China

DOI 10.4108/eai.6-6-2021.2307857

Logistic mapping based on the study of Logistic, and applied this permutation [4]. In 1998, J. Friedrich applied the state values of chaotic systems directly to the pixel method of permutation images. He found that permutation, which simply changed the position of pixels in an image, was not resistant to statistical analysis. This makes what appears to be a successful encryption operation still insecure. Permutation can flatten the encrypted histogram and change the statistical characteristics of the original histogram by changing the value of pixels. However, the visual effect after encryption is not good, so he proposed the classic permutation and diffusion frame structure. This is also the structure adopted by the vast majority of encryption schemes [5-12]. But encryption algorithms of security level are too low. Pareeket al. [5] used pseudo-random sequences produced chaotic logistic map for an image encryption algorithm. However, due to the one-dimensional mapping, the small key space once leads to poor security performance. Later, some high-dimensional chaotic maps were proposed for image encryption. Wang al. [6] use the mixed chaotic sequence to design an encryption algorithm. The pseudo-random sequences are generated by mixing Logistic map, Henon map and Lorenz system. Although the mixing of multiple systems can increase the size of the key space, the security of the encryption strategy is insufficient. Wei al. [13] introduced hyper-chaotic system for RGB image encryption algorithm. Although it can generate more complex chaotic sequences than low-dimensional chaotic systems, but the encryption and decryption speeds are not ideal because the system is too complex. One-time password is currently the most secure encryption algorithm [14-17], but the one-time password has become a new problem, so DNA encryption technology has been incorporated into the encryption system.

In 1994, Adleman published his famous DNA computing research article [18]. With the deepening of DNA computing research, many advantages of DNA computing have been gradually discovered, such as large amounts of parallelism, low power consumption, and large storage. Therefore, a new area of DNA image encryption has emerged. With the application of DNA addition, subtraction, XOR, and complementation in the field of image encryption, researchers found that an encryption system based on chaotic systems and DNA computing is easier to implement while ensuring image security [19-26]. For example, Chai al. [25] presented encryption algorithm in which SHA 256 hash function, a new there-dimensional chaotic system and DNA XOR operation are to enforce system security. NIU al. [26] presented Josephus traversing and pixel permutation for image encryption scheme. However some algorithms also have some security drawbacks [27-29], for example, Zhang al. [28] introduced DNA addition and two Logistic chaotic maps to encrypt image encryption. Liu al. [27] presented combining DNA complementary rule and chaotic maps to encrypt mage. But these two systems have a common disadvantage of small key space. Zhang al. [29] used encoding and chaos map to improve an RGB image encryption algorithm. After Liu al. [30] analyzed its security, it was found that this encryption system has two security risks. First, through experimental analysis of known plane images and ciphertext images, the key is not difficult to obtain process, the encryption system is less sensitive to the plane. In order to solve the shortcomings of chaotic encryption and DNA encryption, such as small key space, strong correlation, weak anti-attack ability, and poor sensitivity to encrypted images. In this paper, the gray-scale image design method improves the above a new chaotic system.

The following content will be divided into 5 sections and introduced in turn. Firstly, section 2 gives Preliminary works. Section 3 gives our encryption scheme by the architecture of permutation and diffusion. In Section 4, input experimental parameters to test performance. In Section 5, we give Security analyses. Finally, Section 6 puts conclusion at last.

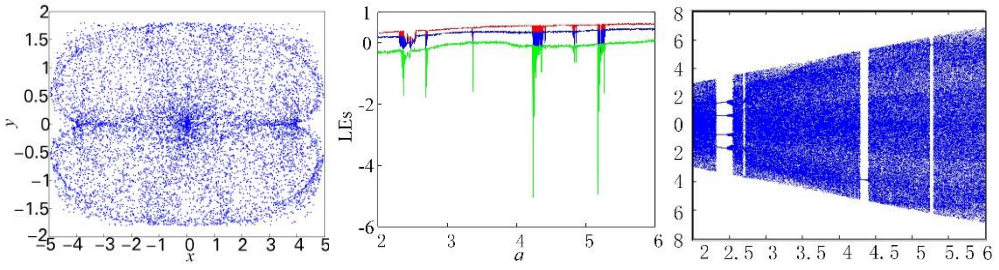
2 Preliminary Works

2.1 The model of system

The three-dimensional discrete chaotic map will be used in the encryption system of this paper and is obtained in Ref [31]. Its mathematical formula is given below:

$$\begin{cases} x_{n+1} = \sin x_n \sin y_n - a \sin z_n \\ y_{n+1} = b \sin x_n \cos y_n \\ z_{n+1} = c y_n \end{cases}, \quad (1)$$

where a, b, c are control parameters, when $(a, b, c) = (4, 4, 2)$ and the initial value $(x_0, y_0, z_0) = (0.5,0.2,0.1)$. The phase diagram is given in Fig.1 (a). Fixed the system parameter $b \in [1,5]$, the LEs (Lyapunov exponent spectrum) is shown in Fig.1 (b). The BDs (bifurcation diagram) is plotted in the Fig.1 (c).



(a) (b) (c)

Fig.1 Phase diagram, LES and BDs of 3D discrete chaotic map: (a) Phase diagram in x-y plane, (b) LES with b=4, c=2, $a \in [2,6]$, (c) BD with b=4, c=2 , $a \in [2,6]$.

2.2 DNA information

2.2.1 Convert image to DNA code

In DNA computing, the bases A, T, C, and G are used to represent information. Therefore, the image pixels are converted to 8-bit binary and use 00, 01, 10, 11 to represent A, T, C, and G respectively, corresponding to a total of 24 encoding rules, but Binary encoding and DNA encoding to produce structural and characteristics of the link. So, you can get eight rules for DNA coding from Table.1. This will also be used as the decoding rule in the decryption process.

In this paper, pixel is the basic unit of image. The gray value of pixel point is expressed as 8-bit binary sequence in computer. According to the rule of binary pair and DNA coding, it can be expressed as 4 nucleic acid bases. For example, A, T, C, and G are represented as 00, 11, 10, and 01 respectively. For pixel points is 121 using encoding rule 1 in Table.1, the binary sequence is represented as [01111001], and the corresponding DNA sequence is represented as [C T G C]. Similarly, if the DNA sequence given is ATCG, follow coding rule 1 in Table.1. We can get a decoded binary sequence of 00110110, the decimal number is “54”. This is how the DNA sequence is decoded.

Table.1 DNA encoding rules

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

2.2.2 DNA operations

When binary pixels are encoded as DNA, the corresponding binary operation rules are inherited by DNA operations as shown in Table.2 and Table.3.

Table.2 XOR operation

XOR	A	G	C	T
A	A	G	C	T
G	G	A	T	C
C	C	T	A	G
T	T	C	G	A

Table.3 Addition and Subtraction operation

+	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

2.3 Optimized Arnold transformation

The following is the optimization of Arnold matrix transformation method: assume the plaintext image is *P*, expand *P* into *A* one-dimensional row vector, and denote it as *A*. Arnold transformation is performed on the position (1, *j*) of coordinates of any point of vector *A*, and the new coordinate position (*p*, *q*) is obtained through the following formula.

$$\begin{cases} p = 1 + aj \\ q = b + (ab + 1) j \end{cases}. \tag{2}$$

Considering only the above equation, the exchange between pixel points (1, *j*) and (1, *q*) can be realized through pseudo-random variables *a* and *b*. At the same time, *ab*+1 is regarded as a new random number denoted by *a*, then Equation (2) becomes as shown in Equation (3).

$$q = b + aj\ . \tag{3}$$

3 Encryption Scheme

3.1 The Secret Sequence Generator

SHA 256 is a hash function. For messages of any length, SHA 256 will generate a 256-bit hash value, called a message digest. Therefore, using the SHA 256 function to encrypt the image can generate a 256-bit hash value, which will be used to calculate the initial value of the chaotic system.

Firstly, the plane image is entered as a parameter to SHA 256 function, then the key K with 256 bits is generated, and K is divided into 32 groups, each consists of 8-bital numbers. K can be derived as follows:

$$K = k_1, k_2, \ldots, k_{32}, \quad \text{subject to: } k_i = \left\{ k_{i,0}, k_{i,1} \cdots, k_{i,7} \right\}, \tag{4}$$

where $1 \leq i \leq 32$ and $0 \leq j \leq 7$.

The new stream key can be obtained through the following formula:

$$\begin{cases} k_a = \mathrm{mod}(10^{-15} \, mean(K(1:8) \oplus K(9:16), 2^6) \\ k_b = \mathrm{mod}(10^{-15} \, mean(K(17:24) \oplus K(25:32), 2^6) \\ k_c = \mathrm{mod}(10^{-15} \, sum(K(1:8) \oplus K(9:16) \oplus K(17:24), 2^6) \end{cases}, \tag{5}$$

where k_a, k_b, k_c and k_d are the disturbance parameters of the chaotic system, mean (□) is to find the mean operator, mod denotes the modular operator and $K_{2i} \oplus K_{2i+1}$ is the XOR operation.

In this encryption algorithm, the initial value is given as the key, and the initial value of the new chaotic system can be calculated from the following formula:

$$\begin{cases} x_1 = x_0 + k_a \\ y_1 = y_0 + k_b \\ z_1 = z_0 + k_c \end{cases}. \tag{6}$$

3.2 Image encryption flows

First, the encryption flow chart is given in Fig.2, specific details are described in the following two chapters.

3.2.1 Permutation steps

Arnold can generate a lot of pseudo-random sequences, so it can be used in scrambling with the help of sequences generated by 3D discrete chaotic map. The permutation process can be represented in follows.

***Step* 1.** Input grayscale plain image P of size $M \times N$ where M and N are lengths and widths.

***Step* 2.** Use the initial values x_1, y_1, z_1 and u_1 produced by Sec. 3.1, then initial values are taken into 3D discrete chaotic map and iterate the chaotic map for $r+l$ ($r=M \times N$, $l \geqq 500$) times. discarding former l times values of iteration result, key sequence X, Y and Z can be generated by Eq. (1), the four integer sequences $X1$, $Y1$ and $Z1$ are obtained from the following formulas:

$$\begin{cases} X = \{x_1, x_2, \cdots, x_r\} \\ Y = \{y_1, y_2, \cdots, y_r\} \\ Z = \{z_1, z_2, \cdots, z_r\} \end{cases}, \tag{7}$$

$$\begin{cases} X1 = \mathrm{mod}(\, floor((X + 100) \times 10^{10}), 10 \times \max(M, N)) + 1 \\ Y1 = \mathrm{mod}(\, floor((Y + 100) \times 10^{10}), 10 \times \max(M, N)) + 1 \\ Z1 = \mathrm{mod}(\, floor((Z + 100) \times 10^{10}), 10 \times \max(M, N)) + 1 \end{cases}, \tag{8}$$

where floor function is a downward rounding of the results, max (M, N) is the maximum number of M, N.

***Step* 3.** Divide the key sequence $X1$, $Y1$ and $Z1$ into the three groups that can be expressed as: $G(1)=[X1, Y1]$, $G(2)=[X1, Z1]$, $G(3)=[Y1, Z1]$. The first value of the plane pixel will participate in the selection of the chaotic sequence. when $((P(1) \times 1000) \bmod 6)+1=x$, we get key sequence $G(x)$ that is used to permute gray image.

***Step* 4.** In this step, permutation method used is Arnold. Firstly, the image P is expanded into a row vector, assume chaotic sequence array $G(1)$ is obtained in Step 3 then get the random variable $a = X1$, $b = Y1$ as setting in Eq. (3). After the permutation operation can be completed, the image P' is obtained.

3.2.2 Diffusion steps

In the diffusion process, we use DNA XOR operation, which may need to be help of a key matrix produced by 3D discrete chaotic system, to diffuse the image P'. The detailed diffusion steps are given in follows.

***Step* 1.** Transform P' into a binary matrix D ($M \times N \times 8$). Then, DNA matrix W ($M \times N \times 4$) can be obtained after performing matrix D with DNA encoding l_1 rule ($1 \le l_1 \le 8$) operation.

***Step* 2.** Further manipulation of the chaotic sequences X, Y and Z obtained from Eq. (7), then $X1$, $Y1$ and $Z1$ can be calculated in follow:

$$\begin{cases} X1 = \dfrac{sum(abs(X) + floor(Y))}{r} \\ YI = \dfrac{sum(abs(Y) + floor(Z))}{r} \\ Z1 = \dfrac{sum(abs(X) + floor(Z))}{r} \end{cases}. \tag{9}$$

***Step* 3.** The final key matrix can be obtained by the following formula:

$$K2 = \mathrm{mod}(round(\frac{3 \times 10^8 \times T}{F}), 256), \tag{10}$$

$$\begin{cases} T(i, j) = (X1 + i)^2 + (Y1 + i)^2 + Z1^2 \\ F(i, j) = (X1 + i)^2 + j^3 + Y1 \times i \times j \end{cases}, \tag{11}$$

where T and F represent modified chaotic sequence, which used to calculate the key matrix $K2$.

***Step* 4.** Convert $K2$ to a DNA matrix $K3$ with encoding l_1 rule ($1 \le l_1 \le 8$), the encrypted S matrix is shown in follow:

$$S(i) = D(i) \oplus K3(i) \oplus D(i-1), \tag{12}$$

where $\oplus$is DNA XOR operator, $K3(i)$ is the ith (i = 1, 2, …., MN) element of matrix $K1$, $S(i)$ is the output DNA data. When i=1, $S(0) = D$(end).

***Step* 5.** Input the decoding rule l_2, then decode DNA matrix S after diffusion and the ciphertext image S' is generated.

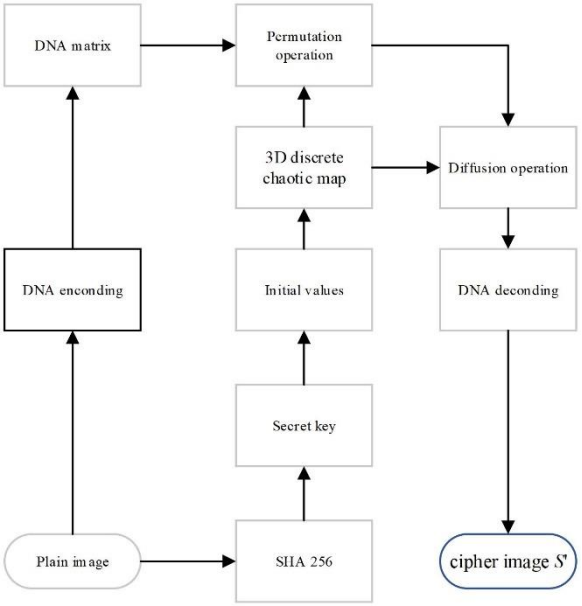
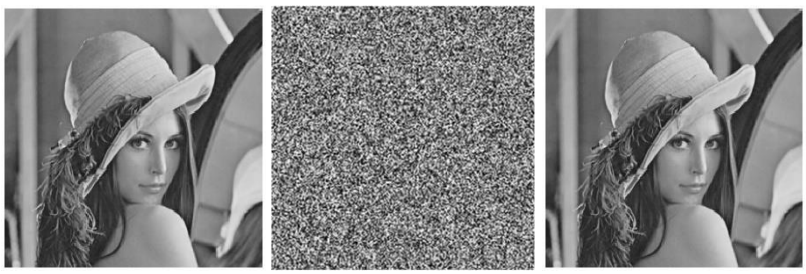


Fig.2 Flow chart of encryption scheme.

4 Simulation tests

Firstly, the initial values and parameters of 3D discrete chaotic system are set as: (x_0, y_0, z_0) = (0.5, 0.2, 0.1), (a, b, c) = (4, 4, 2). Secondly, DNA encoding rules l_1=1 and l_2=3 and iteration numbers l=500; Lena (256 256) as a grayscale image to be encrypted. Lastly, the experimental results are presented in Fig.3 (a)–(f).



(a) (b) (c)

Fig.3 Encryption and decryption test: (a) Original image Lena, (b) encrypted image, (c) decrypted image.

It can be seen from Fig.3 (a)–(b) that, the plane image is encrypted by the encryption algorithm in this paper, it becomes a picture similar to noise, the plaintext information has been successfully hidden. Then after observe the Lena image and decryption as show in Fig.3 (a)–(c), the decrypted image is found to be the same as the original image, it shows that the encryption algorithm with this paper is feasible.

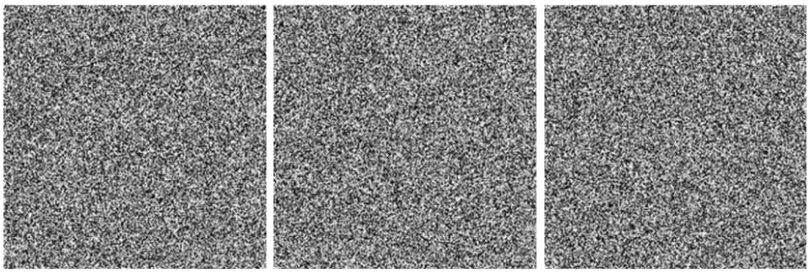
5 Security analyses

5.1. Analysis of key space

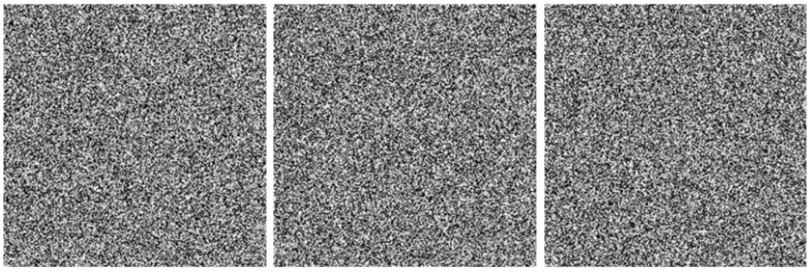
Key space is a collection of all legal keys. The cryptosystem's key space should be large enough so that can effectively combat exhaustive attacks, especially encryption and decryption of very fast cryptographic systems, the length of the password should be at least 100 bit [32]. In the proposed algorithm, key space collection consist of:
(1) The 256-bit external secret key which generated by the plan image are used to give initial values encryptin system.
(2) The chaotic system parameter (x_0, y_0, z_0, a, b, c).
(3) Iterating parameter l in order to obtain chaotic sequences.
(4) The first pixel of the original image ($P(1)$).
(5) Encoding rule l_1 and decoding rule l_2.
Since the calculation of the key space is related to the 10^{-15} of the computer, it is assumed here that accuracy is 10^{-15}, only the key of 3D discrete chaotic system x_0, y_0, z_0, a, b, c and the external key generated by SHA 256 hash function space will be $10^{208} \approx 2^{691}$. When the encryption system has such a large encryption space, only brute force attacks are invalid for the system.

5.2. Analysis of key sensitivity

The analysis of key sensitivity is to make a key change slightly while the other keys remain unchanged, and then decrypt the encrypted image with it. In experiments, the test of key sensitivity scheme uses (x_0, y_0, z_0, a, b, c), which belongs 3D discrete chaotic map, as secret key. Fig.4 shows the decrypted image of the encrypted image after slightly changing the value of parameter, x_0+10^{-16}, y_0+10^{-16}, z_0+10^{-16}, $a+10^{-15}$, $b+10^{-15}$, $c+10^{-15}$ and keeping remaining parameters same. Key sensitivity experiment shows in Fig.5 that the small change of the key will seriously affect the decryption effect of the image, nothing information about the original image to be found due to the image becomes chaotic. Therefore, the algorithm has good security.



(a) (b) (c)

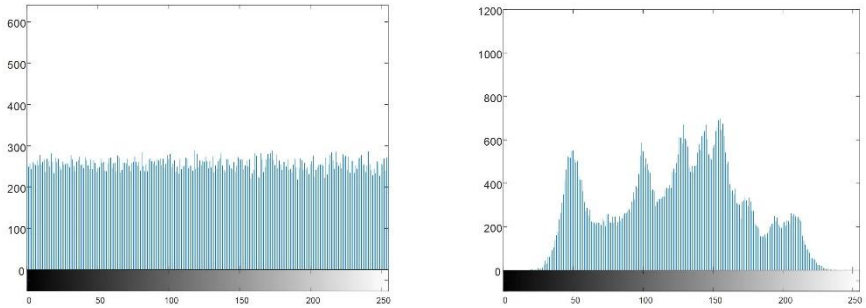


(d) (e) (f)

Fig.4 Key sensitivity tests: (a) Changed key with x_0+10^{-16}, (b) Changed key with y_0+10^{-16}, (c) Changed key with z_0+10^{-16}, (d) Changed key with $a+10^{-15}$, (e) Changed key with $b+10^{-15}$, (f) $c+10^{-15}$.

5.3 Histogram analysis

The histogram of the image is often used to analyze image information, which can be considered as an approximation of the gray density function, Although the histogram cannot directly reflect the image content, it can analyze the performance of an encryption scheme. For example, the histogram of an ideal encrypted image should look like a flat image, if it is not enough, image information can obtained by information statistical analysis. The gray histograms of Lena image before and after encryption are showed in Fig. 5.



(a) (b)

Fig.5 Histogram experimental analysis: (a) Histogram of the original image Lena, (b) histogram of encrypted image.

It can be seen from Fig.5 (b) that the images have almost the same gray value and the statistical Therefore, the encryption algorithm has better performance against statistical analysis.

5.4 Correlation analysis

The correlation coefficient r_{xy} is calculated as follows:

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)D(y)}}, \tag{13}$$

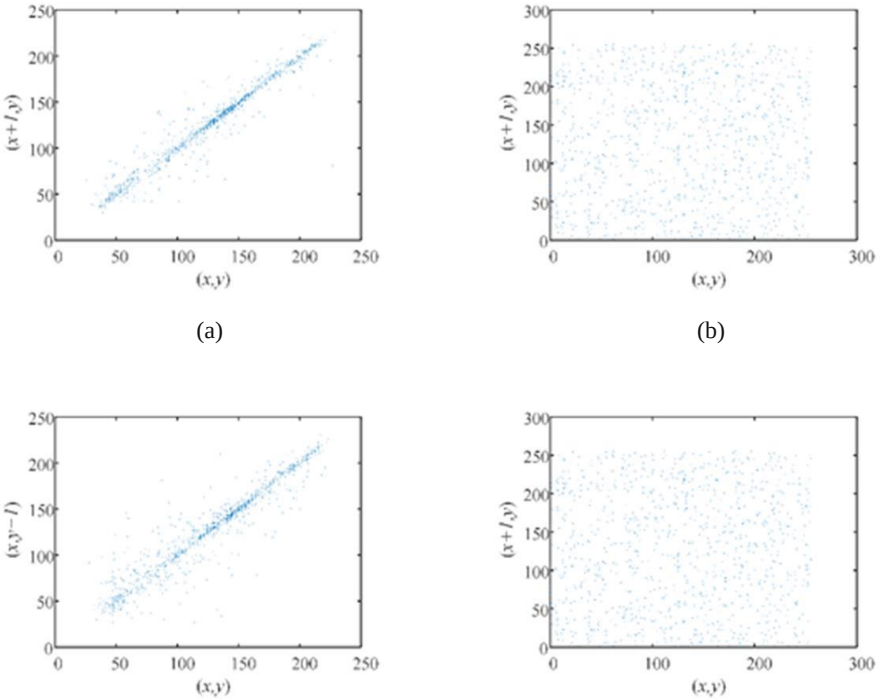
$$\mathrm{cov}(x,y) = E\left\{\left[x - E(x)\right]\left[y - E(y)\right]\right\}, \tag{14}$$

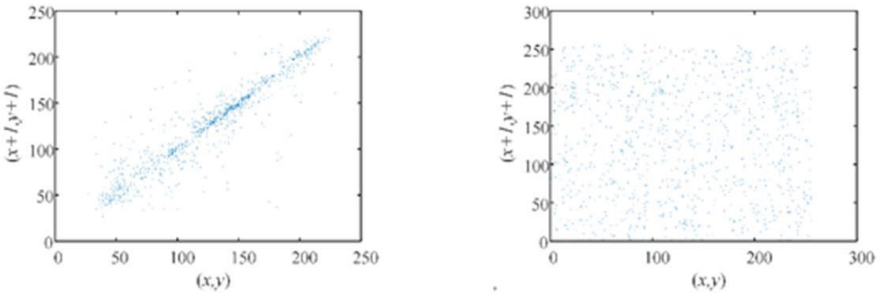
$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, \tag{15}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\left[x_i - E(x)\right]^2, \tag{16}$$

where x and y are the gray value of adjacent pixels, N is the total number of pixels, cov(x, y) is the covariance, $E(x)$ is the average value of pixels and $D(x)$ is the variance. The greater the absolute value of r_{xy}, the stronger the correlation.

In order to visually observe the correlation changes of images before and after encryption, Fig.6 give the 2000 pairs correlation adjacent pixels of the plain image Lena (256 256) and its cipher image in three directions, and the results are compared with the image encryption literatures in recent years, as shown in Table.4.





(e) (f)

Fig.6 Correlation experimental analysis (a) Horizontal correlation of the original image Lena (b) Horizontal correlation of the encrypted image Lena (c) Vertical correlation of the original image Lena (d) Vertical correlation of the encrypted image Lena (e) Diagonal correlation of the original image Lena (f) Vertical correlation of the encrypted image Lena

Table.4 Correlation value table

Direction	Lena image	Our algorithm	Ref [33]	Ref [34]	Ref [35]
Horizontal	0.9692	0.0018	-0.0065	0.0058	0.0198
Vertical	0.9423	0.0016	0.0672	0.0094	0.0141
Diagonal	0.9160	-0.0008	0.0047	0.0214	0.0025

It can be seen from Table.4 that the correlation coefficients of plaintext are all above 0.9, but the correlation coefficients of adjacent elements of ciphertext are all approximately 0. The correlation index of this algorithm is better than that of other algorithms.

5.5 Information entropy analysis

Information entropy is an important indicator reflecting the randomness of information. The more random the pixel value distribution, the higher the information entropy of the image. When the occurrence probability of each gray value is equal, the information entropy of the image is the Ideal value. the information entropy can be derived from the following formula:

$$H(m)=\sum_{i=0}^{L-1} p(m_i)\log\frac{1}{p(m_i)}, \tag{17}$$

where $P(m_i)$ represents the probability of the standard state m_i and L total number of state variables m_i. Suppose there are 28 state values for information m and the probability of their occurrence. According to Eq. (17), if the information entropy of ciphertext close to the ideal value of $H(m)$=8 which represents encryption algorithm can fight against entropy attacks. It can be concluded from Table.5 that the information leakage of ciphertext is very small and the algorithm is safe.

Table.5 Information entropy comparison with other algorithms.

Images	Our algorithm	Ref [36]	Ref [37]	Ref [38]
Camera	7.9972	7.9953	7.4101	7.9937
Couple	7.9972	7.9948	7.4740	7.9938

6.Conclusion

Through a series of experiment and safety analysis, this encryption system in this paper has the following two advantages. First, the hybrid system used for encryption is a new 3D chaotic system. It has a fast iteration speed, which can speed up the running speed of the system. At the same time, due to the large number of parameters, which solves the key space security problem to a certain extent. and by analyzing phase diagram, LEs and BDs illustration, this proves that this encryption system can be applied to chaotic image encryption. Secondly, the plaintext image is closely related to the chaotic sequence by using the SHA 256 hash function, which improved the sensitivity of the encryption system to flat images. in other words, once the plaintext changes slightly, the encryption system will be extremely sensitive to this change. Simulation results show that the algorithm has large key space, high key sensitivity, reduced correlation, enhanced pseudo-randomness, higher security, and stronger ability to resist various attacks.

References

[1] G. Ye, "A block image encryption algorithm based on wave transmission and chaotic systems," *Nonlinear Dynamics,* vol. 75, no. 3, pp. 417-427, 2014.

[2] S. Wang, C. Wang, and C. Xu, "An image encryption algorithm based on a hidden attractor chaos system and the Knuth-Durstenfeld algorithm," *Optics & Lasers in Engineering,* vol. 128, 2020.

[3] H. Dong, E. Bai, X. Q. Jiang, and Y. Wu, "Color Image Compression-Encryption Using Fractional-Order Hyperchaotic System and DNA Coding," *IEEE Access,* vol. 8, pp. 163524-163540, 2020.

[4] R. A. J. Matthews, "On the derivation of a Chaotic encryption algorithm," *Cryptologia,* 1984.

[5] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image and Vision Computing,* vol. 24, no. 9, pp. 926-934, 2006.

[6] W. Mei-Lin, L. Qing, and L. I. Ya, "An image encryption algorithm based on the mixed chaotic sequence," *Optoelectronics Letters,* vol. 6, no. 004, pp. 310-313, 2010.

[7] L. Huang, S. Cai, X. Xiong, and M. Xiao, "On symmetric color image encryption system with permutation-diffusion simultaneous operation," *Optics & Lasers in Engineering,* vol. 115, no. APR., pp. 7-20, 2018.

[8] Y. He, F. Wang, S. Wang, and B. Chen, "Diffusion Adaptation Framework for Compressive Sensing Reconstruction," 2017.

[9] E. Borowski, Y. Chen, and H. Mahmassani, "Social media effects on sustainable mobility opinion diffusion: Model framework and implications for behavior change," *Travel Behaviour & Society,* vol. 19, 2020.

[10] 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 & Applications,* vol. 75, no. 1, pp. 1-23, 2016.

[11] Wang *et al.*, "Concerted Ion-Exchange Mechanism for Sodium Diffusion and Its Promotion in Na3V2(PO4)(3) Framework," *Journal of Physical Chemistry C Nanomaterials & Interfaces,* 2018.

[12] J. Chang, S. Karra, and K. B. Nakshatrala, "Large-Scale Optimization-Based Non-negative Computational Framework for Diffusion Equations: Parallel Implementation and Performance Studies," 2017.

[13] X. Wei, L. Guo, Q. Zhang, J. Zhang, and S. Lian, "A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system," *Journal of Systems & Software,* vol. 85, no. 2, pp. 290-299, 2014.

[14] A. Argyris, E. Pikasis, and D. Syvridis, "Gb/s One-Time-Pad Data Encryption With Synchronized Chaos-Based True Random Bit Generators," *Journal of Lightwave Technology,* vol. 34, no. 22, pp. 5325-5331, 2016.
[15] S. M. H. Alwahbani and E. B. M. Bashier, *Speech scrambling based on chaotic maps and one time pad*. 2013.
[16] A. Shakiba, "A Randomized CPA-Secure Asymmetric-Key Chaotic Color Image Encryption Scheme based on the Chebyshev Mappings and One-Time Pad," *Journal of King Saud University Computer & Information Sciences,* 2019.
[17] W. X. a, W. S. a, Z. Y. b, and L. C. c, "A one-time pad color image cryptosystem based on SHA-3 and multiple chaotic systems - ScienceDirect," *Optics & Lasers in Engineering,* vol. 103, pp. 1-8, 2018.
[18] Adleman and L., "Molecular Computation Of Solutions To Combinatorial Problems," *Science,* vol. 266, no. 5187, pp. 1021-1024, 1994.
[19] X. L. a, L. W. b, Y. Y. b, and P. L. b. a. c, "An improvement color image encryption algorithm based on DNA operations and real and complex chaotic systems," *Optik,* vol. 127, no. 5, pp. 2558-2565, 2016.
[20] X. Wei, G. Ling, Z. Qiang, J. Zhang, and S. Lian, "A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system," *Journal of Systems & Software,* vol. 85, no. 2, pp. 290-299, 2014.
[21] X. Y. Wang, H. L. Zhang, and X. M. Bao, "Color image encryption scheme using CML and DNA sequence operations," *Bio Systems,* pp. 18-26, 2016.
[22] X. Zhang and R. Ye, "A novel RGB image encryption algorithm based on DNA sequences and chaos," *Multimedia Tools & Applications,* pp. 1-25, 2020.
[23] H. R. Shakir, "A Color-Image Encryption Scheme Using a 2D Chaotic System and DNA Coding," *Advances in Multimedia,* vol. 2019, pp. 1-13, 2019.
[24] Xiaopeng *et al.*, "A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system," *Journal of Systems & Software,* 2012.
[25] Chai *et al.*, "A novel image encryption algorithm based on the chaotic system and DNA computing," *International Journal of Modern Physics C Physics & Computers,* 2017.
[26] Y. Niu and X. Zhang, "A Novel Plaintext-Related Image Encryption Scheme Based on Chaotic System and Pixel Permutation," *IEEE Access,* vol. PP, no. 99, pp. 1-1, 2020.
[27] Q. Wang, Q. Zhang, X. Wei, X. Xue, and L. Guo, "Image Encryption Based on Chaotic Map and DNA Coding," *Journal of Computational and Theoretical Nanoscience,* vol. 7, no. 2, pp. 388-393, 2010.
[28] Q. Zhang, L. Guo, and X. Wei, "Image encryption using DNA addition combining with chaotic maps," *Mathematical & Computer Modelling,* vol. 52, no. 11-12, pp. 2028-2035, 2010.
[29] L. Liu, Z. Qiang, and X. Wei, *A RGB image encryption algorithm based on DNA encoding and chaos map*. Pergamon Press, Inc., 2012.
[30] Y. Zhang, Y. Li, W. Wen, Y. Wu, and J. X. Chen, "Deciphering an image cipher based on 3-cell chaotic map and biological operations," *Nonlinear Dynamics,* 2015.
[31] F. Yang, J. Mou, C. Luo, and Y. Cao, "An improved color image encryption scheme and cryptanalysis based on hyperchaotic sequence," *Physica Scripta,* 2019.
[32] 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 Dynamics,* vol. 81, no. 1-2, pp. 511-529, 2015.
[33] X. Wang, Q. Wang, and Y. Zhang, "A fast image algorithm based on rows and columns switch," *Nonlinear Dynamics,* vol. 79, no. 2, pp. 1141-1149, 2015.
[34] N. Zhou, A. Zhang, J. Wu, D. Pei, and Y. Yang, "Novel hybrid image compression–encryption algorithm based on compressive sensing," *Optik - International Journal for Light and Electron Optics,* vol. 125, no. 18, pp. 5075-5080, 2014.
[35] Y. Zhang, B. Xu, and N. Zhou, "A novel image compression–encryption hybrid algorithm based on the analysis sparse representation," *Optics Communications,* 2017.
[36] Zhou *et al.*, "Image compression-encryption scheme based on hyper-chaotic system and 2D

compressive sensing," *Optics & Laser Technology,* 2016.

[37] X. Liu, Y. Cao, P. Lu, X. Lu, and Y. Li, "Optical image encryption technique based on compressed sensing and Arnold transformation," *Optik - International Journal for Light and Electron Optics,* vol. 124, no. 24, pp. 6590-6593, 2013.

[38] Ponuma, R., and Amutha, "Compressive sensing based image compression-encryption using Novel 1D-Chaotic map," *Multimedia Tools & Applications,* 2018.