IMAGE ENCRYPTION ALGORITHM OF CHAOS SYSTEM ADDING COSINE EXCITATION FUNCTION

Zhenzhou GUO[1] and Xintong LI[2]

[1]School of Artificial Intelligence,
Shenyang Aerospace University, Shenyang, China
[2]School of Computer, Shenyang Aerospace University, Shenyang, China

ABSTRACT

In order to increase the chaotic performance of the chaotic system, the chaotic system A-S proposed by Sprott is improved by adding a cosine excitation function to a controller. A series of new chaotic systems are obtained, and the chaotic performance of the improved system is verified. The image is encrypted by the chaotic sequence generated by the improved A chaotic system. In the scrambling part of the image encryption algorithm, the zigzag transformation is improved, and different directions are selected to start the traversal, so that the scrambling process is not easy to be restored. The diffusion part draws on the traditional IDEA algorithm to perform diffusion operations on the image. Finally, the encryption algorithm is analyzed and tested, and the results show that the algorithm has fast encryption and decryption speed, sufficient key space, and can resist statistical analysis attacks well. The algorithm can provide better guarantee for the security of images.

KEYWORDS

Cosine Excitation Function, Three-dimensional Chaotic System, Digital Image Encryption.

1. INTRODUCTION

In today's increasingly prosperous Internet era, to ensure the security of people using the Internet to transmit information, many encryption algorithms have been proposed to ensure the security of the transmission process. However, in the field of image encryption, it has never been a recognized algorithm that can encrypt images according to their own characteristics. The chaotic system is favoured by many scholars because of its good uncertainty, unpredictability and non-repeatability. Among the chaotic systems, low-dimensional chaotic systems like [1], [2], [3], [4] are simple and efficient. But their chaotic range is small, the parameters are few, and they are easier to predict [5], [6], [7], [8]. Therefore, on the basis of the original one-dimensional chaotic system, Zhou et al. proposed to connect two one-dimensional chaotic systems in series to iteratively generate a cascaded chaotic system in [9]. First, the output value of the first chaotic system is used as the input value of the second chaotic system, and then the output value of the second chaotic system is fed back to the first chaotic system as its input value. Compared with ordinary low-dimensional chaotic systems, cascade mapping has more obvious chaotic characteristics, and the chaotic trajectory is more difficult to predict. Taking this as a theoretical basis, WU and HUA et al. proposed some cascaded maps: 2D-HSM, 2D-LSCM, 2D-LASM and 2D-SLMM in [10], [11], [12], [13].

David C. Wyld et al. (Eds): DMML, SEAS, ADCO, NLPI, SP, BDBS, CMCA, CSITEC - 2022
pp. 173-186, 2022. CS & IT - CSCP 2022 DOI: 10.5121/csit.2022.120715

Even so, low-dimensional maps can no longer meet people's security requirements for chaotic algorithms. On this basis, the high-dimensional chaotic map stands out, it has a larger number of parameters and chaotic range, and also has higher security. To make high-dimensional chaotic maps as efficient as possible while having strong encryption performance, many proposals and improvements for high-dimensional chaotic systems have emerged. [14] improved the traditional Baptista algorithm, combined with the hash algorithm and the cyclic shift function, and proposed a one-time encryption algorithm. [15] proposed a new Logistic dynamic linear and nonlinear hybrid coupled mapping lattice. The image encryption algorithm obtained by random encryption has high sensitivity. A new CGCML custom global coupling map is proposed to encrypt color images in [16]. In addition to improving the chaotic system itself, it is also possible to combine the chaotic system with other technologies, and often get good encryption effects, such as DNA technology, quantum technology and Fourier transform. In 2000, Gehani et al first proposed an algorithm to combine DNA coding with chaotic systems in [17]. The color image is encrypted with DNA technology. Dynamic DNA coding is used to improve the security of the encryption algorithm in [18]. Since three-dimensional and lower-dimensional chaotic systems only have a positive Lyapunov exponent, hyperchaotic systems are proposed to improve the performance of chaotic systems in [19]. Hyperchaotic systems have two or more positive Lyapunov exponents. Therefore, hyperchaotic systems have more complex dynamics and are difficulty to be deciphered. However it has higher time complexity. Therefore, in the field of chaos research, how to design a chaotic system with both high efficiency and security is still a research hotspot.

In this paper, a series of three-dimensional chaotic systems are improved, and a cosine excitation function is added to one of the controllers, and a series of new three-dimensional chaotic systems are obtained. Comparing the Lyapunov exponents before and after improvement, and analyze the dynamic characteristics of one of the chaotic systems. The chaotic sequence is generated by the improved chaotic system, and the encryption key is obtained after passing through. This paper uses an improved zigzag transform combined with line shifting to scramble the plain image. Then use the traditional IDEA algorithm to diffuse the image. Finally, the performance of the proposed encryption algorithm is analyzed, and the algorithm is simulated and tested through different performance indicators.

The section 2 of the full text introduces the improved method of 3D chaotic system. And analyzing its chaotic performance analysis. The section 3 applies the image encryption algorithm designed for 3D chaotic system. The section 4 analyzes the performance of the image encryption algorithm through simulation experiments. The section 5 summarizes the full text.

2. INTRODUCTION TO CHAOS SYSTEM

In [20], Sprott summarized some chaotic systems in 1994. In this paper, the A-S system is improved. The cosine excitation function is introduced and the system control parameters are added, so that the output result of the chaotic system has wide-area convergence. In the new chaotic system, the cosine excitation function plays a role in influencing the transition process, and the characteristics of the original three-dimensional chaotic system still play a major role in the influence of the new chaotic system. Table 1 shows the comparison of the Lyapunov exponents of the better performing systems before and after improvement with the same coefficients. It can be seen from Table 1 that the improved method proposed in this paper has a good enhancement effect on chaotic systems. Therefore, the improved method is feasible.

Table 1. Comparison of chaotic systems

Case	Equation	Improved equation	Lyapunov exponent	New Lyapunov exponent
A	$\begin{cases}\dot{x}=ay\\ \dot{y}=-bx+cyz\\ \dot{z}=d-ey^2\end{cases}$	$\begin{cases}\dot{x}=ay+r\cos(\omega t)\\ \dot{y}=-bx+cyz\\ \dot{z}=d-ey^2\end{cases}$	0.020 0 -0.012	0.044 0 -0.010
B	$\begin{cases}\dot{x}=ayz\\ \dot{y}=bx-cy\\ \dot{z}=d-exy\end{cases}$	$\begin{cases}\dot{x}=ayz+r\cos(\omega t)\\ \dot{y}=bx-cy\\ \dot{z}=d-exy\end{cases}$	0.442 0 -1.019	0.471 0 -0.432
C	$\begin{cases}\dot{x}=ayz\\ \dot{y}=bx-cy\\ \dot{z}=d-ex^2\end{cases}$	$\begin{cases}\dot{x}=ayz+r\cos(\omega t)\\ \dot{y}=bx-cy\\ \dot{z}=d-ex^2\end{cases}$	0.051 0 -0.426	0.240 0 -0.640
D	$\begin{cases}\dot{x}=-ay\\ \dot{y}=bx+cz\\ \dot{z}=dxz+3y^2\end{cases}$	$\begin{cases}\dot{x}=-ay+r\cos(\omega t)\\ \dot{y}=bx+cz\\ \dot{z}=dxz+3y^2\end{cases}$	2.744 0 -8.579	3.422 0 -14.145
E	$\begin{cases}\dot{x}=ayz\\ \dot{y}=bx^2-cy\\ \dot{z}=d-4x\end{cases}$	$\begin{cases}\dot{x}=ayz+r\cos(\omega t)\\ \dot{y}=bx^2-cy\\ \dot{z}=d-4x\end{cases}$	0.076 0 -0.688	0.685 0 -0.455
F	$\begin{cases}\dot{x}=-ay+bz^2\\ \dot{y}=cx+0.5y\\ \dot{z}=dx-ez\end{cases}$	$\begin{cases}\dot{x}=-ay+bz^2+r\cos(\omega t)\\ \dot{y}=cx+0.5y\\ \dot{z}=dx-ez\end{cases}$	0.319 0 -0.828	0.500 0 -0.825
G	$\begin{cases}\dot{x}=0.4x+az\\ \dot{y}=bxz-cy\\ \dot{z}=-dx+ey\end{cases}$	$\begin{cases}\dot{x}=0.4x+az+r\cos(\omega t)\\ \dot{y}=bxz-cy\\ \dot{z}=-dx+ey\end{cases}$	0.202 0 -0.939	0.267 0 -0.896
H	$\begin{cases}\dot{x}=-ay+bz^2\\ \dot{y}=cx+0.5y\\ \dot{z}=dx-ez\end{cases}$	$\begin{cases}\dot{x}=-ay+bz^2+r\cos(\omega t)\\ \dot{y}=cx+0.5y\\ \dot{z}=dx-ez\end{cases}$	0.306 0 -0.764	0.828 0 -0.323
K	$\begin{cases}\dot{x}=axy-bz\\ \dot{y}=cx-dy\\ \dot{z}=ex+0.3z\end{cases}$	$\begin{cases}\dot{x}=axy-bz+r\cos(\omega t)\\ \dot{y}=cx-dy\\ \dot{z}=ex+0.3z\end{cases}$	0.079 0 -0.548	0.119 0 -0.515
L	$\begin{cases}\dot{x}=ay+3.9z\\ \dot{y}=0.9x^2-by\\ \dot{z}=c-dx\end{cases}$	$\begin{cases}\dot{x}=ay+3.9z+r\cos(\omega t)\\ \dot{y}=0.9x^2-by\\ \dot{z}=c-dx\end{cases}$	0.243 0 -4.581	0.597 0 -4.498
N	$\begin{cases}\dot{x}=-2y\\ \dot{y}=ax+bz^2\\ \dot{z}=c+dy-2z\end{cases}$	$\begin{cases}\dot{x}=-2y+r\cos(\omega t)\\ \dot{y}=ax+bz^2\\ \dot{z}=c+dy-2z\end{cases}$	0.164 0 -1.912	0.437 0 -1.895
Q	$\begin{cases}\dot{x}=-az\\ \dot{y}=bx-cy\\ \dot{z}=3.1x+dy^2+0.5z\end{cases}$	$\begin{cases}\dot{x}=-az+r\cos(\omega t)\\ \dot{y}=bx-cy\\ \dot{z}=3.1x+dy^2+0.5z\end{cases}$	0.485 0 -0.928	0.487 0 -0.937
R	$\begin{cases}\dot{x}=0.9-ay\\ \dot{y}=0.4+bz\\ \dot{z}=cxy-dz\end{cases}$	$\begin{cases}\dot{x}=0.9-ay+r\cos(\omega t)\\ \dot{y}=0.4+bz\\ \dot{z}=cxy-dz\end{cases}$	0.311 0 -0.988	0.326 0 0.987

2.1. Trajectory diagram of chaotic system and Lyapunov exponent

In this paper, the improved A system is used to analyze and generate encrypted sequences.

$$\begin{cases} \dot{x} = ay + r\cos\omega t \\ \dot{y} = -bx + cyz \\ \dot{z} = d - ey^2 \end{cases} \tag{1}$$

When the initial value of the system (x, y, z) is (1, 1, 1), the system parameters a=5; b=2; c=1; d=10; e=15; r=-1; ω=1 , the chaotic trajectory of the system is shown in Figure 1.

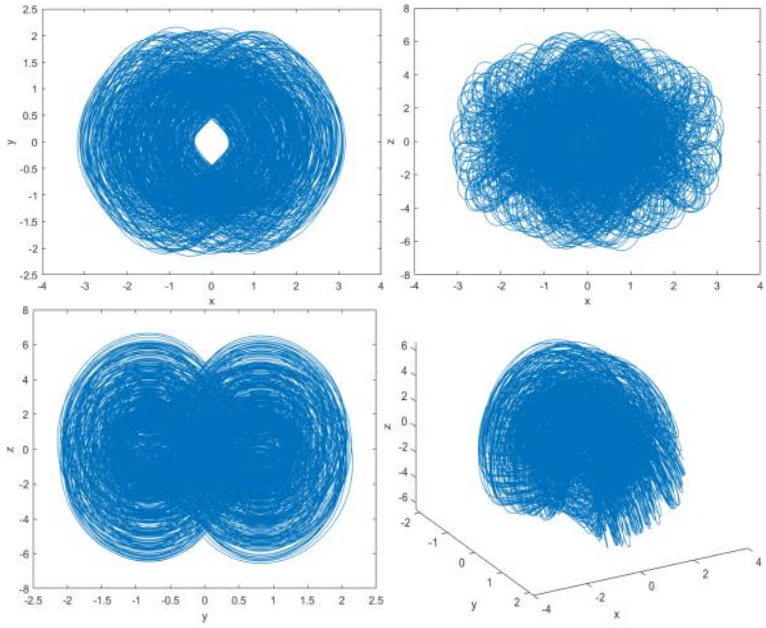

Figure 1. Trajectory diagram of chaotic system

The Lyapunov exponent can be used to analyze the characteristics of the chaotic system. The Lyapunov exponent spectrum of the improved A system is shown in Figure 2. It can be seen from the figure that one of the exponents is always greater than 0. This shows that the chaotic system is chaotic at this time.

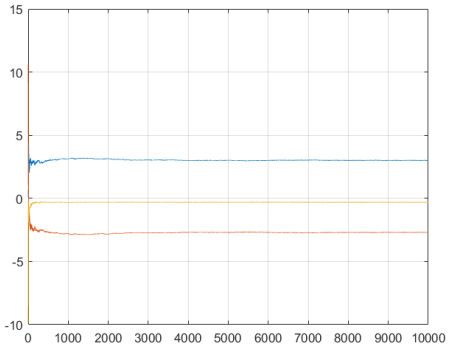

Figure 2. Lyapunov exponent

2.2. Bifurcation diagram

For a chaotic system to exhibit good chaotic dynamics, appropriate system parameters are also required. When the initial values of x, y, and z are (0, 0, 0), draw a bifurcation diagram about parameters a, b, c and d, as shown in Figure 3. It can be seen from the figure that the system has a large parameter range.

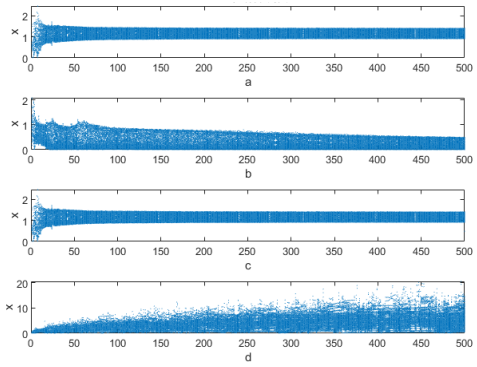

Figure 3. Bifurcation diagram of parameters

2.2. Balance point analysis

Taking system A as an example. Let rcos (ωt)=N and independent of x, y, and z. The system equations are shown below.

$$\begin{cases} \dot{x} = ay + N \\ \dot{y} = -bx + cyz \\ \dot{z} = d - ey^2 \end{cases} \tag{2}$$

Let the right-hand side of the equation be zero:

$$\begin{cases} ay + N = 0 \\ -bx + cyz = 0 \\ d - ey^2 = 0 \end{cases} \tag{3}$$

Solving Eq.3 to get the system equilibrium point (0, -N/a, 0) or (0, $\sqrt{d/e}$, 0), and the Jacobian matrix at the equilibrium point is:

$$J = \begin{bmatrix} 0 & \mathrm{a} & 0 \\ -\mathrm{b} & 0 & \mathrm{c}\sqrt{\mathrm{d}/\mathrm{e}} \\ 0 & -2\sqrt{\mathrm{ed}} & 0 \end{bmatrix} \tag{4}$$

Getting the eigenmatrix of the system:

$$J - \lambda E = \begin{bmatrix} -\lambda & a & 0 \\ -b & -\lambda & c\sqrt{d/e} \\ 0 & -2\sqrt{ed} & -\lambda \end{bmatrix} \tag{5}$$

Let the system characteristic matrix |J-λE|=0. Its expression is shown in Eq.6.

$$-\lambda 3-(2cd+ab)\lambda=0 \tag{6}$$

Solving the characteristic Eq.6 to get three eigenvalues: $\lambda_1=0$, $\lambda_2=\sqrt{2cd+ab}\,i$, $\lambda_3=-\sqrt{2cd+ab}\,i$. All eigenvalues have non-positive real parts. According to the Lyapunov stability method, the system is asymptotically stable at the equilibrium point.

3. IMAGE ENCRYPTION ALGORITHMS

3.1. Generate chaotic sequence

(1) The hash value of the plain image is calculated by the SHA256 algorithm and converted to decimal output. Due to the precision problem of MATLAB, the first 45 bits are selected to obtain three values between 0 and 1, which are used as the initial values x_0, y_0, and z_0 of the chaotic system.

(2) Enter the given system initial values x0, y0, z0, and let the step size l=0.001. Generating three chaotic sequences through the system function ode45, and processing the three chaotic sequences respectively:

$$Xi=\mathrm{mod}(\mathrm{floor}((xi(1001:\mathrm{floor}(M\times N/2)+1000))\times 10\text{^}15),256),\quad i=1,2,3 \tag{7}$$

After processing by Eq.7, we get three integer sequences X1, X2 and X3.

3.2. Image Encryption Algorithm Description

Chaos-based encryption algorithms are generally composed of two ways of permutation and diffusion. In this paper, the image is scrambled by zigzag transformation and line shift, and the whole encryption process is completed through the designed diffusion algorithm.

3.3. Zigzag

The elements in the two-dimensional matrix are traversed from the upper left corner as shown in Figure 4 according to the "zigzag" trajectory, and then the traversed elements are stored in one-dimensional, and then the one-dimensional matrix is converted into a two-dimensional matrix to obtain A transformed new 2D matrix.

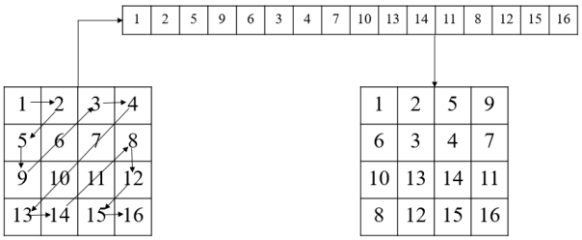

Figure 4. Zigzag transform

However, it can be seen from the above figure that no matter how many times this transformation is repeated, the positions of the first two digits and the last two digits of the matrix have not changed. In the actual encryption, it may leave an opportunity for attackers. Therefore, we

change the starting position of the zigzag, so that the positions of all elements in the matrix change as much as possible.

Figure 5 shows the traversal order of the improved Zigzag. The steps of the scrambling algorithm using Zigzag are as follows:

(1) Read the grayscale image P and the number of iterations n.
(2) From the lower left corner of the two-dimensional image matrix, traverse the entire two-dimensional matrix in the order marked in the figure, and place the traversed elements in a one-dimensional matrix in turn.
(3) Reshape the obtained one-dimensional matrix into a two-dimensional matrix P′, let P=P′.
(4) Repeat steps (2) and (3) until n times are completed.
(5) The image P after the disturbance is output.

In the end, each element in the new matrix P we get is completely different from its position in the original matrix.

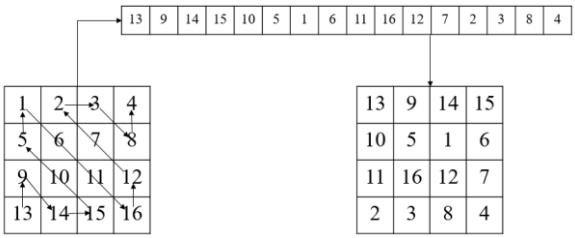

Figure 5. Improved Zigzag transform

We call the matrix to be zigzag transformed as P=a(i, j)M×N, where a(i, j) is the value of the matrix at row i and column j, and M and N are the number of rows and columns of the matrix, respectively number. z is the position of the element in the two-dimensional matrix in the one-dimensional matrix obtained after the transformation.

After comparison, the period of zigzag transformation is much larger than that of traditional Arnold scrambling, and at most four zigzag transformations, its scrambling effect will be better than Arnold scrambling. Meanwhile, the time complexity of the zigzag transformation is $\theta(n^2)$. It can be seen that the improved zigzag transformation algorithm is simple to implement, faster and of better quality.

3.4. row shift

To enhance the scrambling effect of the image, a set of line shifts is added after the zigzag transformation. The first line of the image does not move, and from the second line, the elements of each line are shifted to the right by i-1 bits, where i is the number of lines.

3.5. Diffusion algorithm

The diffusion algorithm proposed in this paper is inspired by the IDEA block encryption algorithm proposed and improved by X.J.Lai and Massey. IDEA algorithm is proposed on the basis of DES algorithm, which is closer to triple DES. This paper simplifies a part of the algorithm, and the execution order of the proposed diffusion encryption algorithm is:

(1) Convert the two-dimensional image matrix P into a one-bit matrix, and divide it into two groups P1 and P2 of equal length.
(2) XOR P1 with the processed chaotic sequence X1.
(3) Add P2 to the processed chaotic sequence X2 and take the modulo.
(4) Add the results of steps (1) and (2) and take the modulo.
(5) XOR the result of step (1) with the processed chaotic sequence X3.
(6) Concatenate the results of steps (4) and (5) to obtain a one-dimensional matrix with a length of M×N, and reshape it into a two-dimensional matrix to obtain the diffused cipher image.

4. PERFORMANCE ANALYSIS

In this section, a series of simulation experiments will be conducted to test the algorithm using several different methods. Three images of Lena, Baboon and Pepper are selected as test images.

4.1. Histogram analysis

Due to the particularity of the image, the pixels of the plain image are unevenly distributed, which makes the image easy to be cracked when subjected to statistical analysis attacks. The histogram can clearly show the distribution of image pixel values. This section analyzes the statistical characteristics of the histograms of plain images and cipher images.
The histograms of Lena's plain and cipher images are shown in Figure 6.

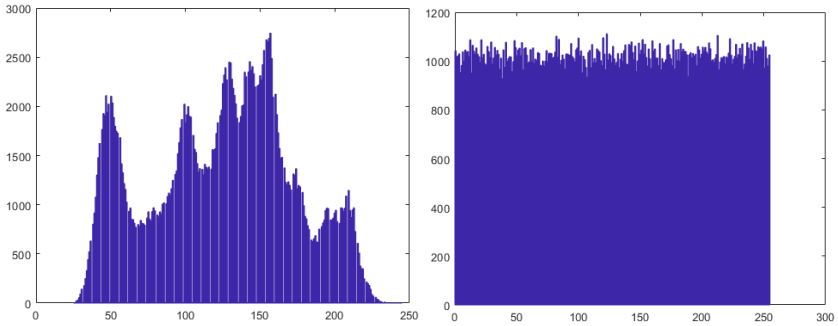

Figure 6. Plain image histogram (left) and cipher image histogram (right) of Lena

4.2. Correlation analysis

Generally speaking, plain images have strong correlations in four directions: horizontal, vertical, positive diagonal, and anti-diagonal, while cipher images have weak correlations in all directions. This paper selects 5000 pixels in Lena image, Baboon image and Pepper image respectively, and calculates the pixel correlation coefficient r in four directions. The closer r is to 1, the higher the correlation between pixels; the closer to 0, the lower the correlation.

The experimental results are shown in Table 2. Figure 11 shows the pixel correlation graphs of Lena plain image and cipher image in horizontal, vertical, positive and anti-diagonal directions.

Table 2. Correlation coefficients

Image		**Horizontal direction**	**vertical direction**	**Diagonal direction**	**Anti-angle direction**
Lena	Plain image	0.9867	0.9734	0.9625	0.9698
	Cipher image	-0.0075	-0.0071	-3.8565×10-4	0.0035

Baboon	Plain image	0.7542	0.8638	0.7050	0.7091
	Cipher image	0.0049	-0.0105	-0.0101	0.0151
Pepper	Plain image	0.9771	0.99781	0.9622	0.9680
	Cipher image	-0.0010	0.0072	-0.0042	0.0164

From the table, we can see that the difference is highly correlated with the pixels of the plain image, and the connection between the adjacent pixels of the cipher image has been reduced to almost non-existent in the encryption process.

4.3. Key space

The key space of the algorithm proposed in this paper is 2^{161}, and the key length of the encryption algorithm with fast encryption speed is at least 2^{128}, hence the key space of the algorithm in this paper can effectively resist the exhaustive attack.

4.4. NPCR and UACI

In image encryption, there are often cases where the difference between two images cannot be observed by the naked eye. The two values NPCR and UACI are generally used to quantify the difference between images. The two images of the same size to be compared are marked as P1 and P2 respectively. The meaning and calculation method of NPCR and UACI are briefly introduced below.

NPCR: Compare whether the values of the pixels at the same position of the two images are the same. The ratio of the number of different pixels to all the pixels is the value of NPCR, and the calculation formula is shown in formula (8) and formula (9).

$$NPCR(P_1, P_2) = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|Sign(P_1(i,j) - P_2(i,j))\right| \times 100\% \tag{8}$$

$$Sign(x) = \begin{cases} 1, & x>0 \\ 0, & x=0 \\ -1, & x<0 \end{cases} \tag{9}$$

For two random images, the probability of the same pixel at any position is 1/256, and the probability of difference is 255/256. Therefore, the theoretical expectation of NPCR is about $255/256 \approx 99.6094\%$.

UACI: NPCR measures the number of different values of pixels in two random images, but does not show the degree of difference in the values of pixels in the two images, so UACI is introduced to supplement. It describes the average value of the difference between the values of all pixel points in the same position of the two images to be compared and the ratio of the maximum difference value (255). Its calculation formula is shown in formula (10).

$$UACI(P_1, P_2) = \frac{1}{MN}\sum_{i}^{M}\sum_{j}^{N}\frac{\left|P_1(i,j) - P_2(i,j)\right|}{255-0} \times 100\% \tag{10}$$

The expected UACI of two random images is calculated to be $257/768 \approx 33.4635\%$.

Through the values of NPCR and UACI, the degree of difference between the two images can be known. The larger the value, the greater the difference between the two images.

4.5. Key sensitivity analysis

Key sensitivity analysis refers to the difference analysis of the cipher image obtained by encrypting the same plain image with two keys with little difference. Since the chaotic system is very sensitive to the change of the initial value, the purpose of testing the sensitivity of the key is achieved by changing only a small initial value of the chaotic system.

To increase the size of an initial value by 10-15 to generate a new set of chaotic sequences. Encrypt the same plain image through two chaotic sequences respectively. Analyzing the difference between the two cipher images obtained, and calculate the value of NPCR and UACI. The three grayscale images of Lena, Baboon and Pepper are tested respectively. The test results are shown in Table 3.

Table 3. NPCR and UACI for key sensitivity

Image		**Lena**	**Baboon**	**Pepper**	**Expectation**
Proposed	NPCR	99.5899%	99.6094%	99.6014%	99.6094%
	UACI	33.4469%	33.3903%	33.4592%	33.4635%
Ref.[21]	NPCR	99.565%	99.572%	/	99.6094%
	UACI	33.450%	33.448%	/	33.4635%
Ref.[22]	NPCR	99.6002%	99.5903%	99.6112%	99.6094%
	UACI	33.5079%	33.5281%	33.5265%	33.4635%

As can be seen from the table, the key sensitivity of the encryption algorithm is very close to the expectation. The performance on Baboon and Pepper are also better than the algorithms in [21] and [22].

4.6. Plaintext sensitivity analysis

Plaintext sensitivity refers to the difference between the contrasting cipher images when two images with very little difference are encrypted with the same key. If the difference between the two images is large, the plaintext sensitivity of the algorithm is high; otherwise, the plaintext sensitivity is poor.

Therefore, change the value of a random pixel point, and analyze the difference of the cipher image after encryption respectively. Table 4 is the NPCR and UACI values of the images tested. It can be concluded from the table that the algorithm has better plaintext sensitivity.

Table 4. NPCR and UACI for plaintext sensitivity

Image	**Lena**	**Baboon**	**Pepper**	**Expectation**
NPCR	99.5823%	99.6086%	99.5949%	99.6094%
UACI	33.5124%	33.5196%	33.3958%	33.4635%

4.7. Noise attack

Noise is manifested as irrelevant and abrupt pixels in the image, and the noise generated by different methods is also different. Figure 7 shows the noise in the simulated channel, and the decrypted image after adding four kinds of noise to the Lena cipher image. After adding Poisson noise with variance of 0.01, multiplicative noise with variance of 0.04, Gaussian noise with variance of 0.01 and variance of 0.1 salt-and-pepper noise to the cipher image, it is decrypted.

Figure 7. Decrypted image of cipher image after adding noise

It can be seen from the four images that after adding different degrees of noise, there is still a good decryption effect. Even if there are errors in the values of some pixel points, the approximate image can still be seen. It shows that the encryption algorithm has a certain anti-interference ability in the face of noise attack, and can restore the original image better in the face of interference, which provides a certain reliability guarantee for transmission in the channel.

4.8. Shear attack

When transmitting in the channel, not only will it face noise attacks, but sometimes part of the image will be lost. At this time, the encryption algorithm needs to decrypt the part of the cipher image that has been transmitted to obtain a clear plain image as much as possible. Figure 8 shows the cipher images and the decrypted images after 1/8 cutting, 1/4 cutting and 1/2 cutting of the Lena cipher image respectively.

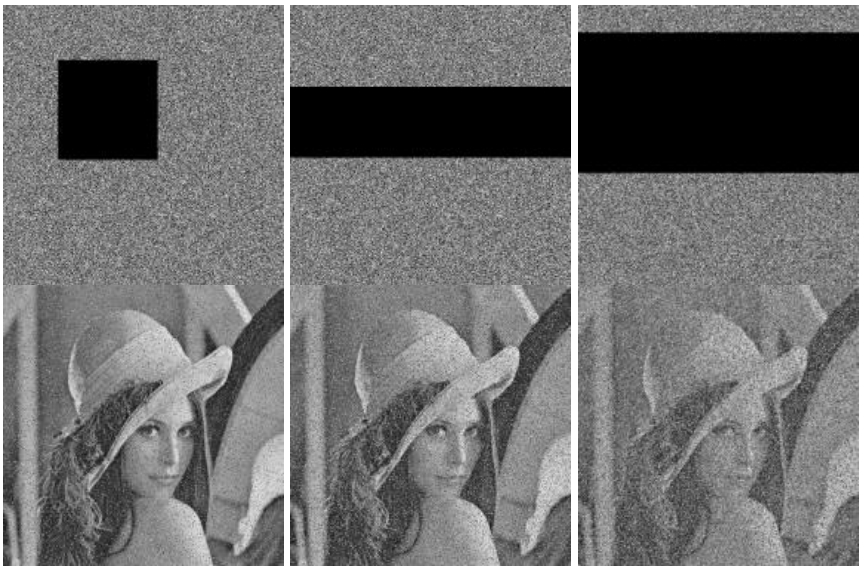

Figure 8. Cut cipher image and its decrypted image

It can be seen from the above figure that as the cut-out part becomes larger and larger, the decrypted image is distorted to a certain extent. Although the decrypted image is not clear enough, the basic outline of the image can still be seen, and sometimes the algorithm proposed in this paper can cope well with the need for real-time transmission. Therefore, the algorithm proposed in this paper can still give a more complete image even if there is data loss.

4.9. Information entropy analysis

The information entropy was drawn and summarized by Shannon in 1948 from the concept of thermal entropy in thermodynamics, which refers to the uncertainty of information and the level of information value. The information entropy of low information degree will be high, and the information entropy of high information degree will be low. The formula of information entropy is shown in Eq.11.

$$H = -\sum_{i=0}^{L} p(i)\log_2 p(i) \tag{11}$$

Among them, L is the number of gray levels of the image (L=256 in this paper). p(i) represents the probability of occurrence of gray value i. In this paper, the theoretical value of information entropy H is 8. Table 4 shows the information entropy of the plain images of Lena, Baboon, and Pepper and their cipher images.

Table 5. Information entropy

Image	**Lena**	**Baboon**	**Pepper**
Plain image	7.4478	7.3579	7.5943
Cipher image	7.9993	7.9994	7.9993
Ref.[21]	7.9993	7.9992	/
Ref.[22]	7.9979	7.9971	7.9974

It can be seen from the table that the information entropy of the image encrypted by the algorithm proposed in this paper is relatively high. The cipher image contains less information, so the algorithm proposed in this paper has better encryption effect.

5. CONCLUSION

In this paper, an improved method for 3D chaotic system by adding cosine excitation function is proposed. The chaotic trajectory diagram, Lyapunov exponent, time series diagram, system bifurcation diagram and equilibrium point analysis of the improved A system all show that the system has obvious dynamic characteristics and good chaos. The proposed scrambling and diffusion algorithm has made some changes on the original basis, which ensures the security and improves the efficiency. The final algorithm test results show that the algorithm can resist some common security attacks, and the value of pixel points is related to more pixels as much as possible, which has better robustness. Therefore, the encryption algorithm proposed in this paper can play a better role in the process of image security communication.

REFERENCES

[1] Zhou Y , Long B , Chen C . A new 1D chaotic sys-tem for image encryption[J]. Signal Processing, 2014, 97(apr.):172-182.

[2] Liu, Wenhao, Sun, et al. A fast image encryption algori-thm based on chaotic map.[J]. Optics & Lasers in Engi-neering, 2016, 84:26-36.
[3] Hui W A , Di X A , Xin C B , et al. Cryptanalysis- and enhancements of image encryption using combinat-ion of the 1D chaotic map - ScienceDirect[J]. Signal P-rocessing, 2018, 144:444-452.
[4] Abd, El-Latif, Ahmed, et al. A novel image encryption scheme based on substitution-permutation network and chaos[J]. Signal Processing: The Official Publication of the European Association for Signal Processing (EURA-SIP), 2016, 128:155-170.
[5] Zhou Y , Bao L , Chen C L P . A new 1D chaotic system for image encryption[J]. Signal Processing, 2014, 97:172–182.
[6] Arroyo D , Rhouma R , Alvarez G , et al. On the security of a new image encryption scheme based on chaotic map lattices[J]. Chaos An Interdisciplinary Jour-nal of Nonlinear Science, 2008, 18(3):033118-113.
[7] Papadopoulos H-E , Wornell G-W . Maximum-likelihoo-d estimation of a class of chaotic signals[J]. IEEE Tran-sactions on Information Theory, 2002, 41(1):312-317.
[8] Wu X , Hu H , Zhang B . Parameter estimation only from the symbolic sequences generated by chaos system[J]. Chaos Solitons & Fractals, 2004, 22(2):359-366.
[9] Zhou Y , Hua Z , Pun C-M , et al. Cascade Chaotic System With Applications[J]. IEEE Transactions on Cyb-ernetics, 2015:2001.
[10] Wu J , Liao X , Bo Y . Image encryption using 2D Hénon-Sine map and DNA approach[J]. Signal Process-ing, 2018, 153:11-23.
[11] Hua Z , Fan J , Xu B , et al. 2D Logistic-Sine-Co-upling Map for Image Encryption[J]. Signal Processing, 2018, 149.
[12] Hua Z , Zhou Y . Image encryption using 2D Logistic-adjusted-Sine map[J]. Information Sciences, 2016, 339.
[13] Hua Z , Zhou Y , Pun C M , et al. 2D Sine Logistic modulation map for image encryption[J]. Information e-nces, 2015, 297:80-94.
[14] Wang X A , Zhu X A , Wu X B , et al. Image encryption algorithm based on multiple mixed hash functions and cyclic shift - ScienceDirect[J]. Optics and Lasers in Engineering, 2018, 107:370-379.
[15] Wang X , Yang J , Guan N . High-sensitivity image encryption algorithm with random cross diffusion based on dynamically random coupled map lattice model[J]. Chaos Solitons & Fractals, 2021, 143(5):110582.
[16] Wang X , Qin X , Liu C . Color image encryption algorithm based on customized globally coupled map lattices[J]. Multimedia tools and applications, 2019.
[17] Gehani A , Labean T , Reif J . DNA-based cryptography[M]. 2000.
[18] Chai X , Fu X , Gan Z , et al. A color image cryptosystem based on dynamic DNA encryption and chaos[J]. Signal Processing, 2019, 155(FEB.):44-62.
[19] Nguyen N T , Bui T Q , Gagnon G , et al. Designing a Pseudo-Random Bit Generator with a Novel 5D-Hyperchaotic System[J]. IEEE Transactions on Industrial Electronics, 2021, PP(99):1-1.
[20] Sprott, J. Some simple chaotic flows[J]. Physical revie-w. E, Statistical physics, plasmas, fluids, and related int-erdisciplinary topics, 1994, 50(2):R647-R650.
[21] Wang X , Zhao H , Feng L , et al. High-sensitivity image encryption algorithm with random diffusion based on dynamic-coupled map lattices[J]. Optics and Lasers in Engineering, 2019, 122(Nov.):225-238.
[22] Wu J , Liao X , Bo Y . Image encryption using 2D Hénon-Sine map and DNA approach[J]. Signal Processing, 2018, 153:11-23.

AUTHORS

Zhenzhou GUO born in 1977, MS, lecturer, his research interest includes Chaos encryption.

Xintong LI, born in 1997, MS candidate, her research interest includes Chaos encryption.