Bit level image encryption algorithm based on hyper-chaotic system*

MAN Zhenlong[1], ZHANG Yue[2], ZHOU Ying[1], LU Xiaoli[1], and WANG Zhaoquan[1]**

1. School of Electronic and Information Engineering, Liaoning Technical University, Huludao 125100, China

2. Advanced Interactive Technology and Application Laboratory, Computer Network Information Center, Chinese Academy of Sciences, Beijing 100190, China

(Received 28 September 2022; Revised 22 December 2022)

Because chaotic systems are unpredictable, ergodic and sensitive to initial values and parameters, they are often used in the field of encryption. To avoid the bad randomness of the random key generated by the low dimensional chaotic map system, a 5-dimensional multi-wing hyperchaotic system is adopted in this paper. The key stream generated by the chaotic system is related to the plaintext image. So it can effectively resist the attacks of selecting plaintext. The plaintext graph is decomposed into binary form by bit plane decomposition technique, and then these bit planes are divided into high and low groups. The designed control matrix is used to identify the specific scrambling mode, and each bit is permuted within and between groups. Finally, bit diffusion is used to change the pixel value of each pixel. Theoretical analysis and numerical simulation show that the algorithm has good encryption performance for image encryption.

Document code: A **Article ID:** 1673-1905(2023)03-0186-7

DOI https://doi.org/10.1007/s11801-023-2161-7

With the rapid development of multimedia computing and communication technique, image has become an important part of information transmission of multimedia technique because it can better reflect the static characteristics of real things[1]. Digital image processing technique has penetrated into many aspects of human life, such as industrial Internet, medical detection, aerospace remote sensing, meteorology, communications, reconnaissance and industry. Because of this, image information has been paid more and more attention. In addition, protecting the security of image data is becoming increasingly important, especially in the military, commercial and medical fields. Different from text information, digital image has the inherent characteristics of large data capacity, strong correlation between adjacent pixels and high redundancy[2]. These characteristics not only greatly reduce the encryption speed, but also lead to traditional encryption algorithms, such as data encryption standard (DES), international data encryption algorithm (IDEA) and advanced encryption standards, are no longer applicable to image encryption[3]. At the same time, to prevent the leakage of image information, many scholars have proposed a variety of new image encryption algorithms, including chaos theory[4-9], optical transformation[10], random grid technique[11], DNA coding[12] and image decomposition technique[13]. However, chaotic systems have attracted extensive attention because of their excellent characteristics, such as periodicity, ergodicity, pseudo-randomness and high sensitivity to control parameters.

In 1963, LORENZ[14] deeply studied the law of atmospheric flow, and abstracted it into a physical model, combined with mathematical theory analysis, and gave the corresponding mathematical equation. The chaotic solution can be obtained by such a mathematical equation, and the chaotic behavior can be displayed by using the chaotic map, and these maps can be parameterized by the initial variables. Since then, many scholars have begun to make in depth research on this basis. In 1989, MATTHEW first proposed an algorithm based on chaos encryption. He made use of logistic map as a cipher generator to complete the encryption of digital image information[4]. In 1998, FRIDRICH[15] proposed a chaotic image encryption structure based on "scrambling diffusion". Since then, excellent chaotic encryption algorithms have emerged in endlessly. The image is scrambling algorithm generally including pixel processing[16], block level data[17] and DNA data[18]. However, the above algorithms only apply the scrambling process to the bit level, while the diffusion operation is still performed at the pixel level, so the diffusion is not complete. At the same time, we note that some algorithms apply low-dimensional chaotic systems (especially one-dimensional chaotic systems). The chaotic orbits of

* This work has been supported by the Scientific Research Fund Project of Liaoning Provincial Department of Education (No.LJKQZ2021152).

** E-mail: 765001821@qq.com

these low-dimensional chaotic systems are expected to be very simple and easy to predict[19]. Therefore, the security performance has to be discussed. For example, Ref.[20] proposed an adaptive algorithm to estimate the system with simple chaotic behavior, and Ref.[21] also showed a scheme to successfully predict the system initial value of low dimensional chaotic system. In view of the above shortcomings, Ref.[22] introduced a series framework, which used the combination of two different one-dimensional chaotic systems to generate a new one-dimensional chaotic system to resist attacks. In Refs.[19] and [22], the authors used two one-dimensional chaotic systems to couple into a two-dimensional chaotic system to increase the complexity and prediction difficulty of the chaotic system. However, none of the above algorithms can solve the common problem that the chaotic orbits of low dimensional chaotic systems are relatively simple.

To overcome the shortcomings of the above algorithms, this paper proposes a novel image encryption algorithm based on hyperchaotic. We solve the problem of simple chaotic behavior by using a 5-dimensional multi-wing hyperchaotic system. At the same time, the chaotic system generated in this paper is related to the characteristics of planar images to enhance the sensitivity of plaintext. For different images, this algorithm can obtain a completely different chaotic sequence. In addition, we choose to use bit plane decomposition to decompose the image into 8-bit plane subgraphs, and then perform "diffusion scrambling" on these bit plane subgraphs to enhance the security of the cryptosystem. In the scrambling process, we use the idea of packet switching to ensure that every bit element has the opportunity to face switching. Experimental results and simulation experiments show that the algorithm not only has superior performance, but also can resist different types of attacks.

In this paper, a chaotic system is introduced into the image encryption algorithm, and the experimental analysis shows good results. The 5-dimensional hyperchaotic system model is defined as follows[23]:

$$\begin{cases} x_1' = -ax_1 + x_2x_3 \\ x_2' = -bx_2 + fx_5 \\ x_3' = -c_3 + gx_4 + x_1x_2 \\ x_4' = dx_4 - hx_1 \\ x_5' = ex_5 - x_2x_1^2 \end{cases}, \tag{1}$$

where x_1, x_2, x_3, x_4, x_5 are the state variables of the chaotic system. a, b, c, d, e, f, g and h are the system parameters. The nonlinear terms in the system are x_1x_2, x_2x_3 and $x_2x_1^2$. In this experiment, we set the parameters as a=10, b=60, c=20, d=15, e=40, f=1, g=50, h=10, and the initial condition is $x_1(0)$=1, $x_2(0)$=1, $x_3(0)$=1, $x_4(0)$=1, $x_5(0)$=1. The Lyapunov exponent is L_1=9.979, L_2=1.96, L_3=0.005 362, L_4=−19.13, L_5=−27.28. Therefore, the chaotic system is hyperchaotic. We can see the chaotic behavior of the system from the attractor in Fig.1.

The encryption process adopted in this paper is shown in Fig.2. First, the chaotic system generates a chaotic sequence related to the original image characteristics by using the characteristics of the plaintext image itself. Then, the plane is decomposed into 8-bit planes by using the bit plane decomposition technique, and then the 8-bit planes are combined into two groups by a certain combination rule. Chaotic sequences are used to complete bit level scrambling to enhance the security of cryptosystems. After that, each bit is diffused by the bit level diffusion principle. Finally, the eight images are reconstructed by the bit plane construction technique to obtain the ciphertext image.

Step 1: First, the plaintext image with pixel size is decomposed into 8 binary bit plane subgraphs by bit plane decomposition technique, and these eight subgraphs are divided into two groups according to certain rules (the grouping rules can also be part of the key). The upper four bits are classified as the first group (g_8, g_7, g_6, g_5), and the lower 4-bit plane subgraphs are classified as the second group (g_4, g_3, g_2, g_1). We make two groups of planes form two sub blocks ***img***1 and ***img***2 respectively. The composition is shown as follows

$$\begin{cases} \boldsymbol{img}1 = \{g_8, g_7, g_6, g_5\} \\ \boldsymbol{img}2 = \{g_4, g_3, g_2, g_1\} \end{cases}. \tag{2}$$

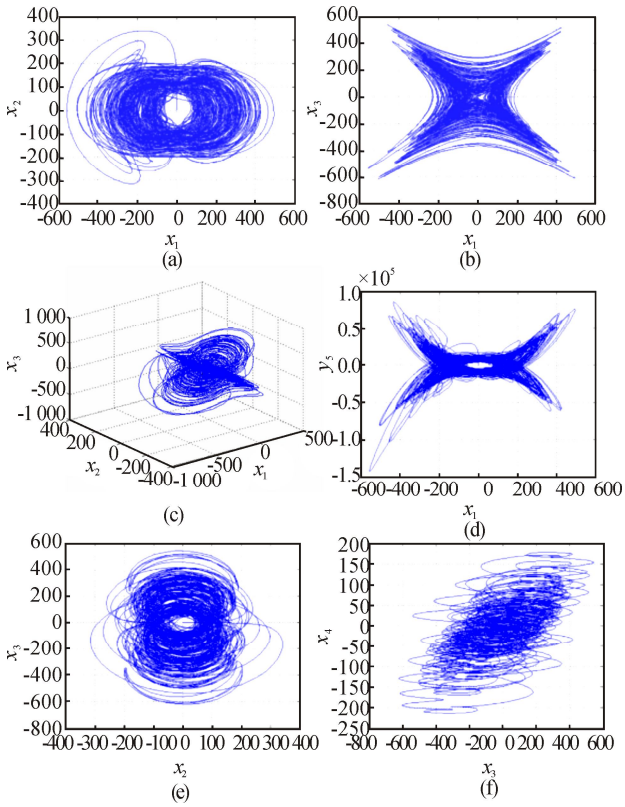


Fig.1 Attractor graphs of chaotic system: (a) x_1-x_2 projection on the plane; (b) x_1-x_3 projection on the plane; (c) x_1-x_2-x_3 projection in three-dimensional space; (d) x_1-x_5 projection on the plane; (e) x_2-x_3 projection on the plane; (f) x_3-x_4 projection on the plane

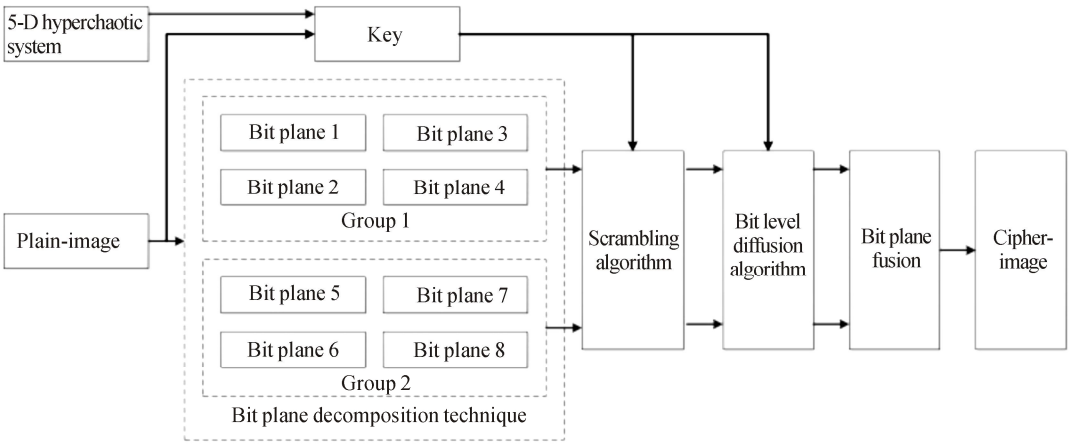


Fig.2 Flow chart of encryption algorithm

These two sub blocks have the same size $M'\times N'$, where $M'=4\times M$, $N'=4\times N$.

Step 2: Taking $\boldsymbol{key}_1=(x_1, x_2, x_3, x_4, x_5)$ as the initial values of the 5-dimensional hyperchaotic system, iterate the chaotic system N_0+L' times (the number of iterations is controlled by the plain-image itself to effectively resist the selected plaintext attacks shown as Eq.(3)), obtain a chaotic sequence $\{c_1, c_2, c_3,... c_{N_0+L'}\}$ with length m, discard the first N_0 times to eliminate the impact of avalanche effect, where L' is the size of $\boldsymbol{img}1$ and $\boldsymbol{img}2$, i.e., $L'=M'\times N'$, and then obtain the remodeling matrix through Eq.(4).

$$N_0 = M' + N' + \mathrm{mod}(\frac{\mathrm{sum}(\boldsymbol{img}1)}{M' + N'}, M + N), \tag{3}$$

$$\begin{cases} a = \mathrm{mod}(\mathrm{floor}(c_i \times 10^{14}), M') + 1 \\ \boldsymbol{A}_1 = \mathrm{reshape}(a, M', N') \end{cases}. \tag{4}$$

Step 3: Similarly, use the method in Step 2 to obtain the chaotic matrix $\boldsymbol{A}_2$.

$$N_0 = M' + N' + \mathrm{mod}(\frac{\mathrm{sum}(\boldsymbol{img}2)}{M' + N'}, M + N), \tag{5}$$

$$\begin{cases} b = \mathrm{mod}(\mathrm{floor}(c_i \times 10^{14}), M') + 1 \\ \boldsymbol{A}_2 = \mathrm{reshape}(b, M', N') \end{cases}. \tag{6}$$

Step 4: Using chaotic matrices $\boldsymbol{A}_1$ and $\boldsymbol{A}_2$, construct matrix control table $\boldsymbol{C}$ and chaotic coordinate pairs $\boldsymbol{XT}$ and $\boldsymbol{YT}$ according to

$$\boldsymbol{C}(i,j) = \begin{cases} 1 & (\mathrm{abs}(\boldsymbol{A}_1(i,j) - i) < M'/4) \\ 0 & \text{others} \end{cases}, \tag{7}$$

$$\begin{cases} \boldsymbol{X} = \mathrm{unique}(\boldsymbol{C}(1:\frac{M\times N}{2})) \\ \boldsymbol{XT} = (\mathrm{find}(\boldsymbol{X} = 0)) = [] \end{cases}, \tag{8}$$

$$\begin{cases} \boldsymbol{Y} = \mathrm{unique}(\boldsymbol{C}(\frac{M\times N}{2} : M\times N)) \\ \boldsymbol{YT} = (\mathrm{find}(\boldsymbol{Y} = 0)) = [] \end{cases}. \tag{9}$$

According to the control matrix $\boldsymbol{C}$ generated above, the chaotic coordinate pairs $\boldsymbol{XT}$, $\boldsymbol{YT}$, the two groups of images start from the first element of their own, from left to right, and from top to bottom, exchange the elements of the two subgraphs. The exchange rules are as follows.

Step 1: Exchange elements in $\boldsymbol{img}1$.

If $\boldsymbol{C}(i, j)=0$, exchange $\boldsymbol{img}1(i, j)$ and $\boldsymbol{img}1(\boldsymbol{XT}(i, j), \boldsymbol{YT}(i, j))$. If $\boldsymbol{C}(i, j)=1$, exchange $\boldsymbol{img}1(i, j)$ and $\boldsymbol{img}2(\boldsymbol{XT}(i, j), \boldsymbol{YT}(i, j))$.

Step 2: Exchange elements in $\boldsymbol{img}2$.

If $\boldsymbol{C}(i, j)=0$, exchange $\boldsymbol{img}2(i, j)$ and $\boldsymbol{img}2(\boldsymbol{XT}(i, j), \boldsymbol{YT}(i, j))$. If $\boldsymbol{C}(i, j)=1$, exchange $\boldsymbol{img}2(i, j)$ and $\boldsymbol{img}1(\boldsymbol{XT}(i, j), \boldsymbol{YT}(i, j))$.

Step 3: The scrambled image $\boldsymbol{T}$ is obtained by fusing the high-order image $\boldsymbol{img}1$ and the low-order image $\boldsymbol{img}2$.

According to the nature of diffusion, an excellent algorithm should make the ciphertext very sensitive to the transformation of the plaintext. For bit level diffusion, this means that the change of one bit in the plaintext can change the probability of 50% of each bit in the ciphertext. In this paper, the previous bit and an element of the chaotic matrix $\boldsymbol{C}$ are used to change the bit value of the current position. The size of the chaotic matrix $\boldsymbol{P}$ and the intermediate ciphertext result $\boldsymbol{T}$ is $M'\times N'$, and the bit diffusion is as follows

$$\boldsymbol{O}(i,j)\begin{cases} \boldsymbol{T}(i,j)\oplus\boldsymbol{T}(M',N')\oplus\boldsymbol{P}(i,j), & i=1, j=1 \\ \boldsymbol{T}(i,j)\oplus\boldsymbol{O}(i-1,N')\oplus\boldsymbol{P}(i,j), & i\neq 1, j=1. \\ \boldsymbol{T}(i,j)\oplus\boldsymbol{O}(i,j-1)\oplus\boldsymbol{P}(i,j), & j\neq 1 \end{cases} \tag{10}$$

This paper will discuss the experimental results of the algorithm and analyze its encryption performance. Python 3.7.4 is used to verify the proposed algorithm. The experimental environment for this experiment is Intel (R) core (TM) i7-7700hq CPU @ 2.80 GHz CPU and personal computer with 16 GB memory. The operating system is Microsoft Windows 10.

Random numbers plays a vital role in the field of image security. SP800-22 is a software package released by the National Institute of Standards and Technology (NIST) for random testing of data streams, including 16 random tests. These tests often use probability statistics to check whether the data stream meets the characteristics of randomness, such as periodicity, correlation and

distribution.

This paper tests the randomness of the pseudo-random sequence $\boldsymbol{C}_i$ generated by the 5-dimensional hyperchaotic system. The experimental results are shown in Tab.1. As seen from the table, the key tested in this paper has successfully passed all randomization tests. Therefore, we believe that the key generated by the chaotic system has very good randomness.

Tab.1 Randomness test results of key

	Test name	Result
1	Frequency test	Pass
2	Frequency test within a block	Pass
3	Runs test	Pass
4	Test for the longest run of ones in a block	Pass
5	Binary matrix rank test	Pass
6	Discrete Fourier transform (spectral) test	Pass
7	Non-overlapping template matching test	Pass
8	Overlapping template matching test	Pass
9	Maurer's "Universal Statistical" test	Pass
10	Lempel-Ziv compression test	Pass
11	Linear complexity test	Pass
12	Serial test	Pass
13	Approximate entropy test	Pass
14	Cumulative sums (Cusum) test	Pass
15	Random excursions test	Pass
16	Random excursions variant test	Pass

The key space is the total numbers of different key combinations that can be used in the encryption (decryption) algorithm. The larger the key space of the algorithm, the stronger the ability to resist brute force cracking. The key in this paper is mainly the initial value of chaotic system. Theoretically, the key space can be infinite, but it is limited by the floating-point numbers stored by the computer. According to IEEE 754 floating-point storage standard, the storage space of a single precision floating-point number is 32 bits, so the key space of the algorithm is $2^{32\times5}$. For a cryptosystem, if the size of the key space is greater than 2^{100}, brute force attacks may not be feasible[24]. Obviously, this encryption has enough key space to resist all types of violent attacks.

The image histogram represents the distribution value of the pixel intensity within the image. To make statistical attacks more difficult. Fig.3 shows the histogram of Lena image, corresponding encrypted image and decrypted image. In Fig.3, we can see that the gray values in Fig.3(b) are evenly distributed, which is significantly different from the gray value distribution in Fig.3(a) of the plain text image. Moreover, we can also find that the image and gray distribution of the plaintext image Fig.3(a) and the decrypted image Fig.3(c) are almost the same. In addition, we encrypted more images through the algorithm. The plaintext image, the ciphertext image and their corresponding gray histogram are shown in Fig.4. In Fig.4(d), we can see that the gray value of the ciphertext image is evenly distributed, which further proves the ability of the algorithm to resist statistical attacks.

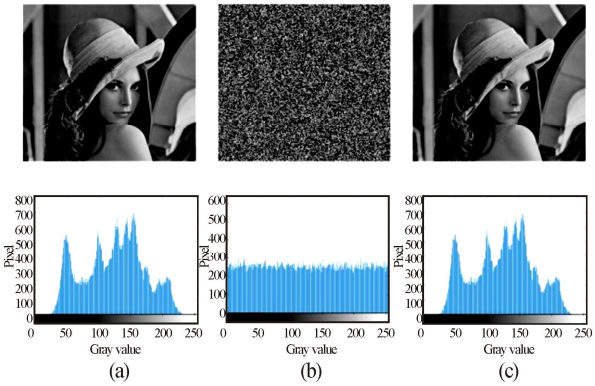


Fig.3 Histogram analysis：(a) The Lena image and its histogram; (b) Encrypted image and its histogram; (c) Decryted image and its histogram

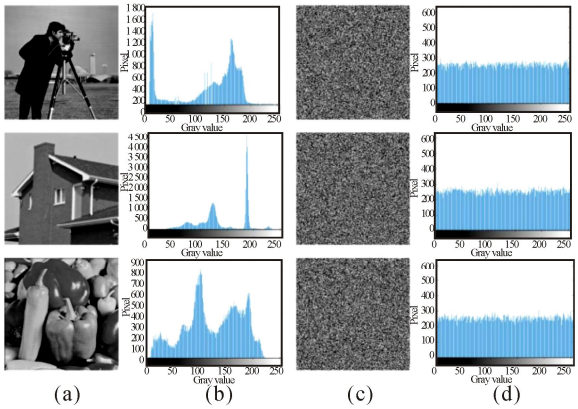


Fig.4 Histogram analysis：(a) Plaintext images; (b) Gray histograms of the plaintext images; (c) Ciphertext images; (d) Histograms of the ciphertext images

Information entropy is the index and method Shannon borrowed from thermodynamics to measure randomness. The mathematical expression of information entropy is as follows

$$H(m)=\sum_{i=0}^{2^L-1}p(m_i)\log_2\frac{1}{p(m_i)}, \tag{11}$$

where $p(m_i)$ is the probability of m_i. If the randomness of a group of data is higher, the information entropy will be larger. On the contrary, if the information has certain statistical laws, the entropy of the information will be smaller. In the process of image encryption, entropy analysis can be performed on the encrypted image to measure the reliability of an encryption algorithm. For a random system in each state, the information entropy value in the ideal state is 8 bits. When the information entropy of a ciphertext image is closer to 8 bits, it indicates that the randomness of the ciphertext image is stronger, which can explain the superiority of the algorithm. The information entropy of the ciphertext image is 7.997 4, which is very close to 8. This shows that the encryption process of this scheme can realize the random distribution of pixels in the encrypted image and has high security. Tab.2 shows the comparison algorithm, which shows that the scheme has certain advantages.

Tab.2 Information entropy

	Lena	Ref.[25]	Ref.[26]	Ref.[27]
Cipher-image	7.997 9	7.997 5	7.997 4	7.997 3

The correlation of adjacent pixels in horizontal, vertical and diagonal directions reflects the correlation degree of adjacent pixels in the image. An ideal encryption algorithm should be able to effectively reduce the correlation between adjacent pixels or even achieve zero correlation as far as possible to resist statistical attacks. To analyze and compare the correlation between the adjacent pixels of the plaintext image and the encrypted image, we randomly select 20 000 adjacent pixel values from each position of the plaintext image and the encrypted image. As shown in Fig.5, the correlation of adjacent pixels in three directions is shown. The distribution of adjacent pixels in the plaintext image is highly concentrated, which means that the plaintext image has a strong correlation, while the distribution of the ciphertext image is relatively uniform, proving the effectiveness of this scheme.

To further calculate the correlation coefficient of each pair of pixels, we use the following equation

$$\begin{cases} r_{xy} = \operatorname{cov}(x,y)/\sqrt{D(x)D(y)} \\ E(x) = \dfrac{1}{S}\sum_{i=1}^{S} x_i \\ D(x) = \dfrac{1}{S}\sum_{i=1}^{S}(x_i - E(x))^2 \\ \operatorname{cov}(x,y) = \dfrac{1}{S}\sum_{i=1}^{S}(x_i - E(x))(y_i - E(y)) \end{cases}, \tag{12}$$

where x and y are the gray values of two adjacent pixels in the image, and N is the total number of pixel values selected from the image, where N=20 000. We selected 5 images including Lena and cameraman and their ciphertext images for correlation analysis. The calculation results are shown in Tab.3. From the table, we can see that the correlation coefficients of the plaintext image in the horizontal, vertical and diagonal directions are all close to 1, while the correlation coefficients of the encrypted ciphertext image in the three positions are all close to 0, which proves that the ciphertext image has extremely low correlation between adjacent pixels in the horizontal, vertical and diagonal directions.

To further demonstrate the superior performance of the proposed encryption algorithm in correlation, we have conducted some comparative experiments. We compared the proposed algorithm with Refs.[25]—[27]. The comparison results are shown in Tab.3. Our algorithm has excellent performance in horizontal, vertical and diagonal directions. The above series of reliable experimental results mean that the algorithm has good performance against statistical attacks.

As we all know, there are four common attacks, namely, selected plaintext attacks, known plaintext attacks, selected ciphertext attack and known ciphertext attack. The plaintext attacks are the most powerful of the four common attacks. If the proposed encryption algorithm can resist this attack, it can resist the other three types of attacks[28]. In the key generation phase, where N is related to plaintext, different plaintext images will produce different N_0 values, so the proposed scheme can effectively resist the selected plaintext attacks.

A good encryption algorithm should be able to resist noise attacks. As shown in Fig.6, 0.01, 0.05 and 0.1 Gaussian noises are used to attack. Even if 0.1 Gaussian noise is added, the decrypted image is still recognizable. Therefore, our algorithm has good robustness and can effectively resist noise attacks.

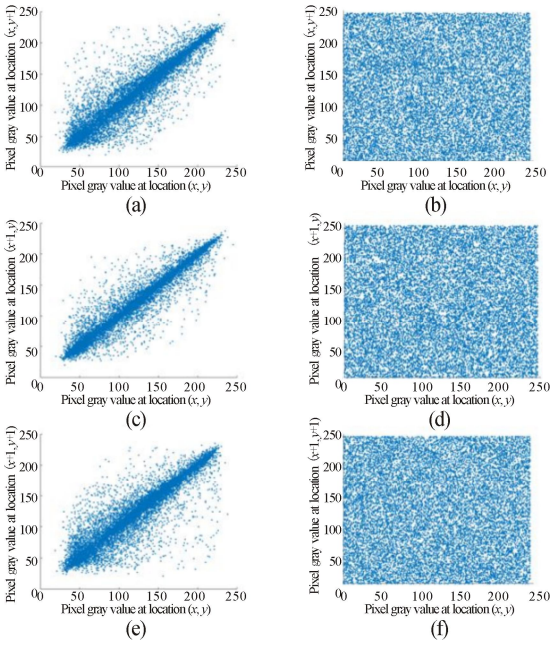


Fig.5 Pixel correlation coefficient analysis: (a) Horizontal adjacent pixel correlation of the plain image; (b) Horizontal adjacent pixel correlation of cipher image; (c) Vertical adjacent pixel correlation of the plain image; (d) Vertical adjacent pixel correlation of the green component of the cipher image; (e) Diagonal adjacent pixel correlation of the blue component of the plain image; (f) Diagonal adjacent pixel correlation of the cipher image

Tab.3 Correlation coefficients of the cipher images

Direction	Horizontal	Vertical	Diagonal
Lena	0.003 4	−0.003 2	0.001 1
Cameraman	0.018 0	−0.006 6	0.003 6
House	0.006 0	0.001 2	0.000 2
Peppers	0.000 8	0.003 1	−0.002 7
Montage	0.020 8	−0.002 6	−0.000 1
Ref.[25]	−0.014 8	0.010 6	−0.013 4
Ref.[26]	0.003 0	0.002 4	−0.005 5
Ref.[27]	0.004 4	0.003 3	0.070 1

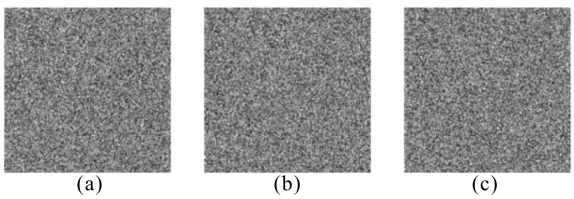


Fig.6 Noise attack analysis: (a) Adding 0.01 Gaussian noises; (b) Adding 0.05 Gaussian noises; (c) Adding 0.1 Gaussian noises; (d) Decrypted image of (a); (e) Decrypted image of (b); (f) Decrypted image of (c)

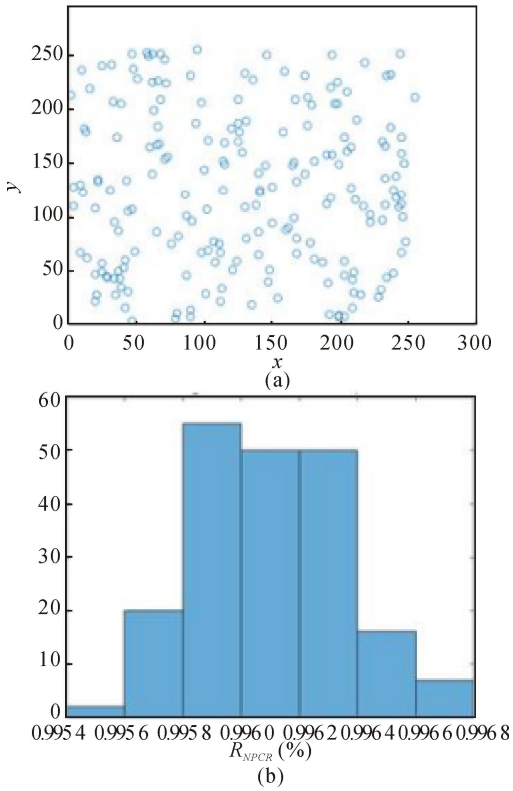
The ability to resist differential attacks means that an ideal cryptosystem should ensure that any small change in the plaintext image can lead to great changes in the ciphertext image. Pixel change rate (*NPCR*) and average change intensity (*UACI*) are two important indicators to measure the resistance of an image encryption algorithm to differential attacks. *NPCR* is defined as follows

$$R_{NPCR}=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}D(i,j)\times 100\%. \tag{13}$$

$\boldsymbol{C}_1$ and $\boldsymbol{C}_2$ represent two ciphertext images after changing a pixel value in the same plaintext image. *UACI* is defined as follows

$$I_{UACI}=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{\left|\boldsymbol{C}_1(i,j)-\boldsymbol{C}_2(i,j)\right|}{255}\times 100\%. \tag{14}$$

To ensure the randomness of the experiment, 200 points are randomly selected to test the sensitivity of the ciphertext of the algorithm. The distribution of points is shown in Fig.7(a). The experimental results are shown in Fig.7(b) and (c) below. From the experimental results, we can see that the minimum value of R_{NPCR} is 99.54%,



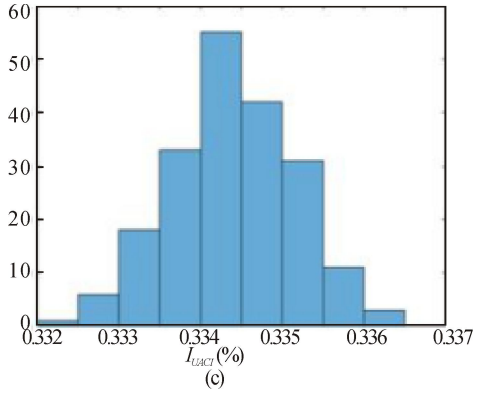


Fig.7 Correlation analysis of differential attacks: (a) Distribution of points; (b) R_{NPCR} (%); (c) I_{UACI} (%)

the maximum value is 99.68%, the minimum value of I_{UACI} is 33.32%, and the maximum value is 33.37%. Therefore, we can also see that the algorithm is excellent in the transformation of the numbers and intensity of pixels, and the dense image is relatively sensitive to the plaintext image, which also proves that the algorithm has certain advantages in resisting differential attacks.

In this paper, a bit level image encryption scheme based on hyperchaotic is proposed. Before scrambling, the plaintext image is first decomposed into high-level group and low-level group, and the chaos control matrix is used to determine the internal or inter group scrambling. Finally, the security of the ciphertext image is improved through bit level diffusion. The advantage of this scheme is that bit level intra group and inter group scrambling can effectively destroy the statistical information of pixels. Combined with the diffusion algorithm, dual encryption ensures the security of the algorithm. Experimental simulation and performance analysis prove the feasibility and effectiveness of this scheme. In the next step, this work will be used as the research basis to deeply study the application of bit level encryption algorithm in Gaussian gated images.

Statements and Declarations

The authors declare that there are no conflicts of interest related to this article.

References

[1] WANG J, LI J, DI X, et al. Image encryption algorithm based on bit-level permutation and dynamic overlap diffusion[J]. IEEE access, 2020, 8：160004-160024.

[2] LI S, CHEN G, CHEUNG A, et al. On the design of perceptual MPEG-video encryption algorithms[J]. IEEE transactions on circuits and systems for video technology, 2007, 17(2)：214-223.

[3] WANG X Y, YANG L, LIU R, et al. A chaotic image encryption algorithm based on perceptron model[J]. Nonlinear dynamics, 2010, 62(3)：615-621.

[4] MATTHEWS R. On the derivation of a “chaotic” encryption algorithm[J]. Cryptologia, 1989, 13(1)：29-42.

[5] ZHU Z, ZHANG W, WONG K, et al. A chaos-based symmetric image encryption scheme using a bit-level

permutation[J]. Information sciences, 2011, 181(6): 1171-1186.
[6] ZHANG L, WANG Y, ZHANG D. Research on multiple-image encryption mechanism based on Radon transform and ghost imaging[J]. Optics communications, 2022, 504: 127494.
[7] YU X, CHEN H, XIAO J, et al. Incoherent optical image encryption based on coded aperture correlation holography[J]. Optics communications, 2022, 510: 127889.
[8] PARAMESHACHARI B D, PANDURANGA H T. Medical image encryption using SCAN technique and chaotic tent map system[M]//Recent advances in artificial intelligence and data engineering. Singapore: Springer, 2022: 181-193.
[9] MANCY L, VIGILA S M C. Protection of encrypted medical image using consent based access control[J]. International journal of medical engineering and informatics, 2022, 14(1): 43-51.
[10] TU S, UR REHMAN S, WAQAS M, et al. Optimisation-based training of evolutionary convolution neural network for visual classification applications[J]. IET computer vision, 2020, 14(5): 259-267.
[11] CHEN T H, LI K C. Multi-image encryption by circular random grids[J]. Information sciences, 2012, 189: 255-265.
[12] RAVICHANDRAN D, BANU S A, MURTHY B K, et al. An efficient medical image encryption using hybrid DNA computing and chaos in transform domain[J]. Medical & biological engineering & computing, 2021, 59(3): 589-605.
[13] ZHANG J, HUANG Z, LI X, et al. Quantum image encryption based on quantum image decomposition[J]. International journal of theoretical physics, 2021, 60(8): 2930-2942.
[14] LORENZ E N. Deterministic nonperiodic flow[J]. Journal of atmospheric sciences, 1963, 20(2): 130-141.
[15] FRIDRICH J. Symmetric ciphers based on two-dimensional chaotic maps[J]. International journal of bifurcation and chaos, 1998, 8(06): 1259-1284.
[16] HUA Z, ZHOU Y, PUN C M, et al. 2D sine logistic modulation map for image encryption[J]. Information sciences, 2015, 297: 80-94.
[17] ZHANG X, WANG L, CUI G, et al. Entropy-based block scrambling image encryption using DES structure and chaotic systems[J]. International journal of optics, 2019.
[18] LIN J, ZHAO K, CAI X, et al. An image encryption method based on logistic chaotic mapping and DNA coding[C]//MIPPR 2019: Remote Sensing Image Processing, Geographic Information Systems, and Other Applications, 2019, Wuhan, China. Washington: SPIE, 2020, 11432: 363-369.
[19] HUA Z, ZHOU Y. Image encryption using 2D logistic-adjusted-sine map[J]. Information sciences, 2016, 339: 237-253.
[20] CHEN S, LÜ J. Parameters identification and synchronization of chaotic systems based upon adaptive control[J]. Physics letters A, 2002, 299(4): 353-358.
[21] from the symbolic sequences generated by chaos system[J]. Chaos, solitons & fractals, 2004, 22(2): 359-366.
[22] HUA Z, ZHOU Y, CHEN C L P. A new series-wound framework for generating 1D chaotic maps[C]//2013 IEEE Digital Signal Processing and Signal Processing Education Meeting (DSP/SPE), August 11-14, 2013, USA. New York: IEEE, 2013: 118-123.
[23] ZAREI A. Complex dynamics in a 5-D hyper-chaotic attractor with four-wing, one equilibrium and multiple chaotic attractors[J]. Nonlinear dynamics, 2015, 81(1): 585-605.
[24] MAN Z, LI J, DI X, et al. Double image encryption algorithm based on neural network and chaos[J]. Chaos, solitons & fractals, 2021, 152: 111318.
[25] ZHANG Y. A new unified image encryption algorithm based on a lifting transformation and chaos[J]. Information sciences, 2021, 547: 307-327.
[26] GAO X, MOU J, XIONG L, et al. A fast and efficient multiple images encryption based on single-channel encryption and chaotic system[J]. Nonlinear dynamics, 2022, 108(1): 613-636.
[27] GUPTA M, SINGH V P, GUPTA K K, et al. An efficient image encryption technique based on two-level security for internet of things[J]. Multimedia tools and applications, 2022: 1-21.
[28] WANG X, TENG L, QIN X. A novel color image encryption algorithm based on chaos[J]. Signal processing, 2012, 92(4): 1101-1108.