A Novel Four-dimensional Hyperchaotic System and DNA Encoding Method for Image Encryption

Jianjun Zhu and Jian'E Zhao
(Corresponding author: Jian'E Zhao)

School of Electronics and Electrical Engineering, Zhengzhou University of Science and Technology
Zhengzhou 450000 China
Email: xdwangxd@163.com

(Received Sept. 21, 2023; Revised and Accepted Dec. 1, 2023; First Online Dec. 24, 2023)
The Special Issue on Data Fusion, Deep Learning and Optimization Algorithms for Data Privacy Protection
Special Editor: Prof. Shoulin Yin (Harbin Institute of Technology)

Abstract

Aiming at the problems of poor speed and insufficient security with traditional image encryption algorithms when encrypting robot images, an image encryption algorithm based on a four-dimensional Hyperchaotic system and deoxyribonucleic acid (DNA) encoding is proposed. The newly constructed four-dimensional hyperchaotic system scrambles the image after bit decomposition to generate the intermediate ciphertext image. The randomness of the key sequence is ensured by selecting multiple high-dimensional chaotic systems and modifying the initial value of chaotic systems. Finally, DNA encryption is performed on the image using the key sequence, and the final ciphertext image is obtained. During DNA encryption, a DNA-S cassette is generated to make nonlinear substitutions to the DNA code. Simulation results show that the encrypted robot image by the proposed algorithm has better distribution characteristics, which can resist statistical analysis and differential attacks, and has the advantages of ample critical space and good sensitivity to initial values.

Keywords: Four-dimensional Hyperchaotic System; Image Encryption; Key Sequence

1 Introduction

The problem of information security in modern society has attracted much attention from experts. Because digital image is vivid, intuitive, so it is widely used, the research of encryption algorithm for digital image has become one of the hot spots. The main technological evolution of image encryption can be summarized into five categories [1,3,7,14,15,21].

1) Matrix transformation. Changing the original pixel position to realize image encryption;
2) Based on the transformation domain. The time domain is transformed to the frequency domain, the frequency domain image is encrypted, and then the inverse transformation is converted to the time domain to form the ciphertext image;
3) Based on chaos theory. According to the sensitivity of the initial value of chaotic sequence, image encryption is realized;
4) Based on DNA coding. According to the principle of base complementary pairing, image information is combined with DNA sequence to generate the corresponding ciphertext information;
5) Based on neural networks. Using neural networks to scramble pixel positions or replace pixel value to realize image encryption.

In order to improve the anti-attack ability and reduce the computational complexity, the advantages and disadvantages of the above five methods are considered comprehensively. This paper presents a new image encryption algorithm based on four-dimensional hyperchaos. The essential reason for chaotic-based encryption is that chaotic sequences are sensitive to initial values, leading to pseudorandomness and ergodicity of phase trajectories [8,13,16].

Traditional chaotic image encryption algorithms are mostly based on low-dimensional chaotic systems [9,11, 22]. Because of the simple structure, small key space and low sequence complexity of the low-dimensional chaotic system, the encryption algorithm based on low-dimensional chaos has the advantages of fast running speed and high encryption efficiency, but the disadvantage is that the encryption security is not high.

Generally, compared with low-dimensional chaotic systems, hyperchaotic systems have more complex structure and higher sequence complexity. Therefore, the encryption algorithm based on hyperchaotic system has better encryption performance. For example, reference [27] proposed a hyperchaotic image encryption algorithm based on bit scrambling. Firstly, the chaotic sequence generated by Kent mapping was used to scramble the position of the plaintext pixel, and then the hyperchaotic sequence generated by Hyperhenon mapping was used to scramble the internal bit of each pixel, and finally the image pixel was diffused. Reference [18] proposed an image encryption algorithm based on bit-plane transformation. Firstly, the image was decomposed into 8 bit planes based on bits, and each bit plane was scrambled by a set of hyperchaotic sequences, and then merged into ciphertext images to realize image encryption. Comprehensive analysis of references [20, 24, 25] shows that they are all based on hyperchaotic systems and adopt bit-scrambling methods. However, the bit scrambling in reference [10] is limited to the pixel interior. The disadvantage is that bits cannot be exchanged between different pixels. In reference [23], bit scrambling is limited to the bit plane of each layer, and the disadvantage is that bits between different bit planes cannot be exchanged, which undoubtedly limits the degree of bit scrambling and further affects the effect of image encryption. Zhang *et al.* [29] proposed a parallel encryption algorithm based on a 5-dimensional hyperchaotic system, which divided image pixels into different levels and used parallel encryption between the same levels to improve the encryption speed. Cheng *et al.* [4] proposed a fast image encryption algorithm based on parallel system, which divides the image into blocks and computes in parallel to improve the encryption speed. The above algorithm improves the encryption efficiency to a certain extent. Because it is mainly based on central processing unit (CPU) parallelism [26], the number of parallelism is limited by the number of CPU threads, and parallelism is not considered in iterative chaotic sequences, the efficiency of robot image still cannot meet the requirements.

To further improve the efficiency and security of image encryption systems, some researchers combine chaotic-based schemes with deoxyribonucleic acid (DNA) rules. For example, Zhang *et al.* [28] used DNA coding and low-dimensional chaotic maps to design an image encryption system, but the randomness of the key stream was not high enough. To overcome this shortcoming, Cun *et al.* [6] proposed a color image encryption algorithm based on hyperchaotic systems and cellular automata. The algorithm utilized multiple high-dimensional chaotic systems to generate key streams and ensure the randomness of the key. Due to the limited DNA coding and operation rules, Wang *et al.* [17] proposed a secure Hash algorithm 256 based on chaos theory and Secure Hash algorithm 256, which used random number of DNA complementary rules of "XOR" operation to replace each pixel, it improved the security of the algorithm. However, the algorithm produced a large number of chaotic sequences and sorting operations, which could not meet the demand in efficiency.

In order to further improve the performance of image encryption, this paper extends the in-pixel bit scrambling and bit-plane bit scrambling to image bit global scrambling, and proposes a hyperchaotic image encryption algorithm based on bit-total scrambling. In this new algorithm, eight bit planes decomposed based on bit are spliced into a large bit plane from low to high level, and then the large bit plane is scrambled by hyperchaotic sequence to realize global scrambling of image bits. Finally, the image pixels are diffused forward and backward. Simulation results show that the new method not only has a large key space and is sensitive to the initial value, but also has a strong ability to resist external attacks and a good encryption effect.

The paper is organized as follows. In Section 2, the new four-dimensional hyperchaotic system is described in detail. Then, in Section 3 we present the DNA encoding, and in Section 4, Image encryption and decryption algorithm is shown. Experimental simulations and analysis are validated in Section 5. Finally, there is a conclusion in Section 6.

2 New Four-dimensional Hyperchaotic System

Cicek *et al.* [5] proposed a 3D continuous chaotic system, the equation was shown in Equation (1).

$$\left\{ \begin{array}{l} \dot{x} = -ax + yz \\ \dot{y} = -x + by \\ \dot{z} = cy^2 - dz \end{array} \right\} \tag{1}$$

When $a = 20$, $b = 10$, $c = 7$ and $d = 5$, the system is a three-dimensional chaotic system. In this paper, based on system (1), variable w is introduced into the second equation of the system. The y^2 in third equation is changed as xy. The variable y is added to the fourth equation to construct a new four-dimensional hyperchaotic system, whose equation is shown in Equation (2).

$$\left\{ \begin{array}{l} \dot{x} = -ax + yz \\ \dot{y} = -x + by + w \\ \dot{z} = c|xy| - dz \\ \dot{w} = -ey \end{array} \right\} \tag{2}$$

When $a = 18$, $b = 10$, $c = 9$, $d = 7$, $e = 2$, it uses the Jacobian method to calculate the Lyapunov exponent: $LE1 = 2.3998$, $LE2 = 0.1354$, $LE3 = -0237$, $LE4 = -17.5109$. Two Lyapunov exponents are greater than 0, and one Lyapunov exponent is approximately equal to 0. The sum of all Lyapunov exponents is less than 0, so the system can be judged as a four-dimensional hyperchaotic system.

Therefore, the chaotic attractors of the new four-dimensional hyperchaotic system obtained in x-y plane, y-z plane and z-w plane are shown in Figure 1.

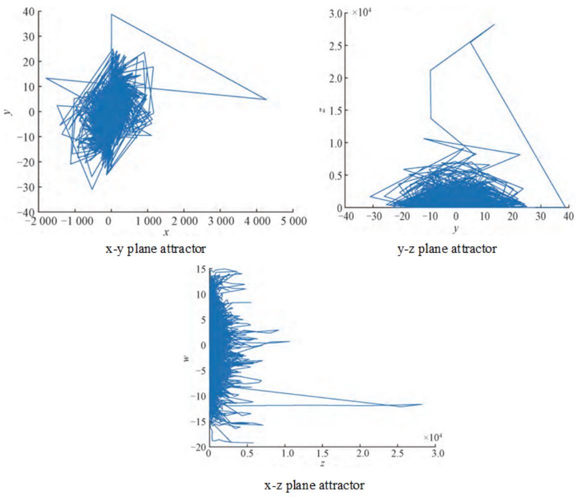


Figure 1: A new four-dimensional hyperchaotic attractor

3 DNA Encoding

3.1 DNA Complementarity Rule and Algebraic Operation

The DNA sequence contains four nucleic acid bases, namely, adenine (A), cymetidine (C), ornipurine (G), and thymetidine (T). Where A and T, C and G are complementary. In a binary system, 0 and 1 are complementary. Similarly, the binary numbers 00 and 11 are complementary, and 01 and 10 are also complementary. Using four bases A, C, G and T to represent the binary numbers 00, 01, 10 and 11, there are 24 DNA coding schemes. However, only eight numbers satisfy the base complementation pairing rule. The encoding rules are shown in Table 1.

Table 1: DNAS encoding rule

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

In this paper, DNA sequences are used to encrypt images. By using A, C, T and G to represent the binary values 00, 01, 10, and 11, each 8-bit pixel value of the image can be encoded as a DNA sequence with length 4. For example, the pixel value 155 can be encoded as "GCGT" by Rule 1. In order to facilitate the application of DNA computation in cryptography, some biological and algebraic operations are introduced to DNA sequences, such as addition (+), subtraction (-), XOR (exclusive OR) operation, etc.

3.2 DNA-S Box Replacement Procedure

In order to make up for the shortage of operation rules in DNA encryption, S-box in DES is used to encode and replace DNA encryption. In cryptography, S-box is the basic structure of symmetric key encryption algorithm to perform nonlinear replacement computation. The S-box in DES algorithm is a fixed S-box, which can map 6-bit input to 4-bit output. In this paper, DNA coding rule 1 is used to convert S-box into DNA-S box, as shown in Table 2. By analogy, eight fixed S-boxes in DES algorithm can be converted into corresponding DNA-S boxes by using eight DNA coding rules [2]. The resulting DNA-S cassette can replace three DNA codes with two DNA codes. The replacement steps are as follows:

1) Group the encoded DNA sequences, and each group consists of two DNA codes.

2) Two key sequences are calculated, and the first key sequence is used to fill each group of DNA sequences into three; The second key sequence is used to select DNA-S boxes for each group to be replaced.

3) Input each group of DNA sequences into the DNA-S box. The newly filled DNA codes are used to find the rows, and the remaining codes are found in the columns to obtain two new DNA codes and complete the replacement.

Table 2: DNA-S box

Rule	A	C	G	T
AA	TG	AA	CA	TT
AC	CA	TT	AC	TA
AG	TC	CT	TG	GA
AT	AC	CA	GA	AG
CA	AG	TG	TC	CA
CC	TT	AG	CG	GC
CG	GT	TC	AG	AC
CT	GA	AC	GT	CT
GA	AT	GG	TT	CC
GC	GG	CG	TA	GT

4 Image Encryption and Decryption Algorithm

The steps of the image encryption algorithm are as follows.

1) Set the size of the plaintext gray image as $M \times N$.

2) The plaintext image is decomposed into 8 bit planes according to bits, which are $a_1, \cdots, a_8$ respectively from low to high. The 8 bit planes are concatenated

into a large bit plane a in the order as shown in Figure 2. The large bit plane a is with 8M length and N width.

3) Set the equation coefficients of the new four-dimensional hyperchaotic system as a_0, b_0, c_0, d_0 and e_0. The initial values of the state variable is x_0, y_0, z_0, and w_0. The sequences generated by 1000 iterations of the hyperchaotic system are discarded, and then generations $(8M + N)$ are selected to generate 5 hyperchaotic sequences. It selects the hyperchaotic sequence $X = x_i$ whose length is truncated as $8M(i = 1, 2, \cdots, 8M)$ and hyperchaotic sequence with length truncated as $Y = y_i$.

4) The elements in sequence X are sorted in ascending order, and a position index sequence $Q = q_i$ is generated for storing the positions (subscripts) of elements in the ascending sequence in the original sequence X, as shown in figure 3. The complexity of four-dimensional hyperchaotic sequence is high, and the length of the selected sequence is relatively small, which ensures that the same sequence value will not appear in a sequence.

   Similarly, it performs the same operation on the sequence Y to obtain the second position index sequence $P = p_i$.

5) The position index sequence Q and P are jointly used to scramble the large bit plane, that is, the elements with coordinate (i, j) in the large bit plane are placed on the position with coordinate (q_i, p_j). At this point, it completes the scrambling of image bits.

6) The scrambled large bit plane is divided into 8 bit planes according to the order of the bit planes in step (2), and then the 8 bit planes are merged in bit order to transform into the intermediate ciphertext image. Then the intermediate ciphertext image is diffused. The diffusion operation is divided into two steps: forward diffusion and backward diffusion.

7) Forward diffusion of image pixels. The intermediate ciphertext image matrix is concatenated into a sequence $G = g_i, i = 1, 2, \cdots, M \times N$ according to rows. Let the image pixel sequence after forward diffusion be $H = h_i, i = 1, 2, \cdots, M \times N$. The forward diffusion operation is carried out according to Equations (2) and (3). The value of M_0 is an integer between 0 and 255.

$$h_1 = mod(g_1 + M_0 256). \tag{3}$$

$$h_i = mod(g_i + h_{i-1} 256), i \geq 2. \tag{4}$$

8) Backward diffusion of image pixels. Let the pixel sequence after back diffusion be $F = f_i, i = 1, 2, \cdots, M \times N$. According to Equations (4) and (5), back diffusion is performed. The value of M_0 is an integer between 0 and 255.

9) Transform the pixel sequence F after diffusion into a row of length M into a $M \times N$ image matrix, which is the ciphertext image. At this point, the image encryption is complete.

5 Experimental Simulation and Analysis

The simulation experiment software is MATLAB 2017a, the processor is Intel cool capacity i5-8250U, and the memory is 8GB. The selected image is Lena grayscale image with the size of 256×256. Setting the encryption algorithm key as $a_0 = 18$, $b_0 = 10$, $c_0 = 9$, $d_0 = 7$ and $e_0 = 2$, $x_0 = y_0 = z_0 = w_0 = 0.1$, $M_0 = M_1 = 35$. Experiment simulation results are shown in figure 4.

As can be seen from Figure 4, the plaintext image is encrypted by the proposed algorithm, and a completely different image is obtained. In order to evaluate the performance of the proposed encryption algorithm, this paper will analyze the encryption effect and security of the algorithm from the aspects of gray histogram, key space, key sensitivity, information entropy, correlation and differential attack.

5.1 Gray Histogram Analysis

Ciphertext images can effectively resist statistical analysis attacks only when they can hide their statistical features. Figure 5 shows the gray histogram of the original image and the encrypted image. The distribution characteristics of the two gray histogram are as follows: the gray histogram of plaintext image is very uneven, while the gray histogram of ciphertext image is relatively uniform. It shows that the algorithm can well conceal the statistical characteristics of plaintext images.

5.2 Key Space Analysis

An algorithm with good encryption performance must have a large enough key space to effectively resist the external exhaustive attack. The key of the algorithm in this paper can be divided into two parts: The first part is five equation coefficients and four initial values of state variables of the four-dimensional hyperchaotic system; In the second part, two parameter values are introduced from the outside when image pixels are diffused in the forward and reverse direction. Therefore, the key has 11 parameter values. Assuming that the computer processes data with a precision of 10^{15}, the key space size is $10^{(11 \times 15)} = 10^{165}$. To resist exhaustive attacks, the key space must be greater than 2^{100}. Since 10^{165} is much larger than 2^{100}, the proposed algorithm is sufficient to resist external exhaustive attacks.

a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8

Figure 2: Bit plane splicing sequence diagram

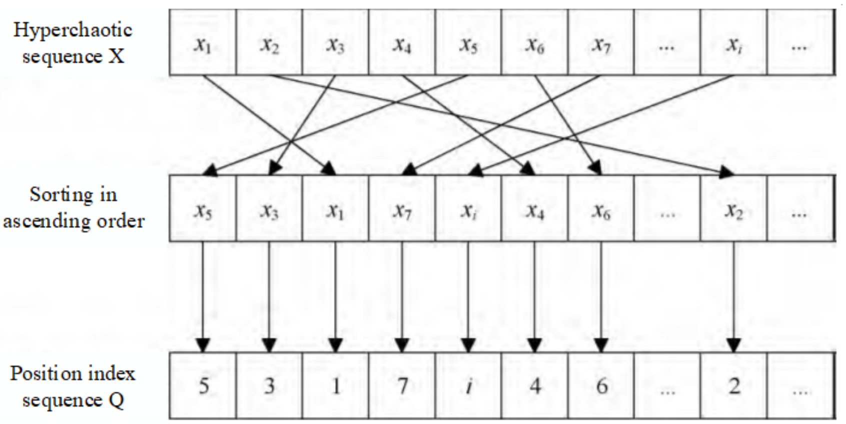
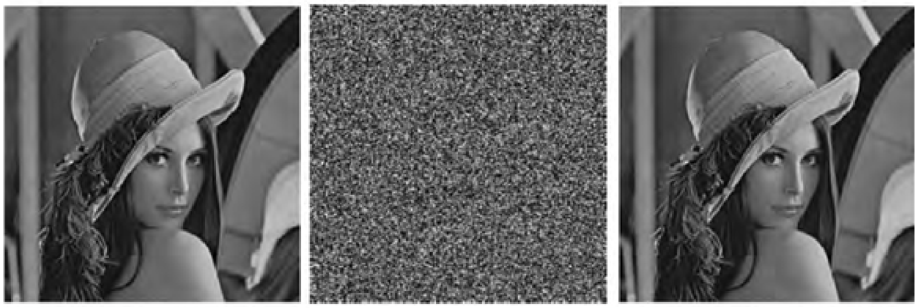
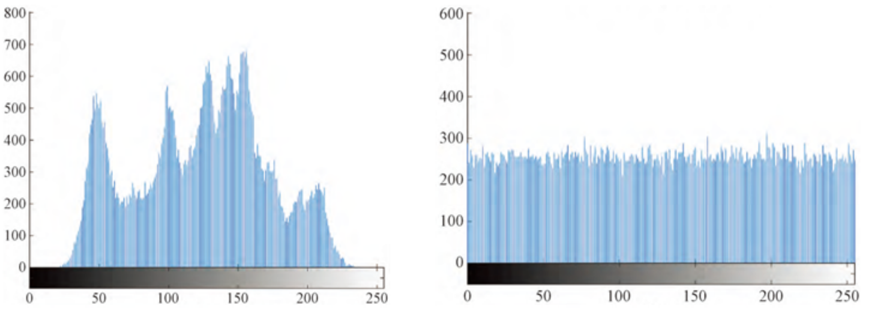

Hyperchaotic sequence X
x_1 x_2 x_3 x_4 x_5 x_6 x_7 ... x_i ...
Sorting in ascending order
x_5 x_3 x_1 x_7 x_i x_4 x_6 ... x_2 ...
Position index sequence Q
5 3 1 7 i 4 6 ... 2 ...

Figure 3: Generation position index sequence



(a) plaintext image (b) ciphertext image (c) Decrypted image

Figure 4: Experimental simulation result



(a) Histogram of plaintext image (b) Histogram of ciphertext image

Figure 5: Histogram analysis

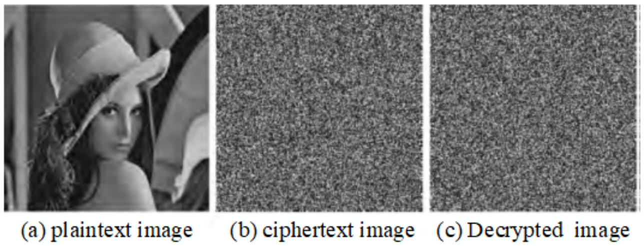

(a) plaintext image (b) ciphertext image (c) Decrypted image

Figure 6: Key sensitivity test

5.3 Key Sensitivity Analysis

A good encryption algorithm must be highly sensitive to small changes in the key. In order to test the sensitivity of the proposed algorithm to the key, in the decryption process, the parameter value x_0 in the key is changed from 0.1 to $0.1 + 10^{-16}$, and other parameter values of the key remain unchanged.

The decrypted image by using the wrong key is shown in Figure 6(c), which is completely different from the original figure in Figure 6(a), indicating that the decryption is failed. It can be seen that the plaintext image cannot be successfully recovered even if the key changes only extremely slightly, which proves that the sensitivity of the algorithm to the key is very high.

5.4 Information Entropy Analysis

Information entropy reflects the chaotic state of pixels in an image and is often used to analyze the effect of image encryption. For an image with a gray level of 256, the image information entropy is equal to 8 in the ideal case. Therefore, the closer the information entropy of ciphertext image is to 8, the better the image encryption effect is. The information entropy of ciphertext image encrypted by the proposed algorithm is 7.9972, which is very close to the ideal value, indicating that the algorithm has a strong ability to resist entropy attack.

5.5 Correlation Analysis

An attacker can attack an image by analyzing the correlation between adjacent pixels. Therefore, a good encryption algorithm should be able to reduce or even eliminate the correlation between adjacent pixels. The correlation between adjacent pixels is defined as follows:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{E(x)}\sqrt{D(x)}}. \quad (5)$$

Where,

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)).$$

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

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2.$$

To evaluate the ability of the proposed algorithm to reduce the correlation between adjacent pixels of an image, correlation coefficients were calculated in the horizontal, vertical and diagonal directions of Lena plaintext and ciphertext images. Meanwhile, the proposed algorithm is compared with the competitive algorithm, and the results are shown in Table 3.

The smaller correlation coefficient denotes the lower correlation. Therefore, this new algorithm can effectively reduce the correlation between adjacent pixels and enhance the ability of ciphertext image to resist statistical attacks.

5.6 Differential Attack Analysis

By making small changes to the plaintext, the attacker can analyze the difference between the ciphertext before and after the plaintext changes, and then obtain useful information. Algorithms with good encryption performance should be highly sensitive to plaintext changes. Even a very small change in the plaintext will make a huge change in the encrypted ciphertext. To evaluate the anti-differential attack capability of the proposed algorithm, NPCR (pixel change rate) and UACI (average change intensity) are used in this paper, which are defined as follows:

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

$$UACI = \frac{\sum_{i=1}^{P}\sum_{j=1}^{Q} |S(i,j) - S'(i,j)|/255}{M \times N} \times 100\%.$$

Where $D(i,j) = 0, S(i,j) = S'(i,j)$, $D(i,j) = 1, S(i,j) \neq S'(i,j)$; M and N are the length and width of the image respectively. S and S' are ciphertexts of two images. Where S is the ciphertext of the plaintext image. S' is the ciphertext obtained by encrypting the pixel value of a pixel point in the plaintext image after slightly changing it.

Ideally, the NPCR and UACI values of 8-bit gray image are 99.6094% and 33.4635%, respectively. In the simulation experiment, the Lena image is first encrypted to obtain the first ciphertext image, and then a random pixel point is selected from the original Lena image (ensure that the pixel value of the point is less than 255) to increase the pixel value of the point by 1, and then the Lena image after slight change is encrypted to obtain the second ciphertext image. The corresponding NPCR and UACI are calculated from the two ciphertext images. In order to avoid the contingency of the simulation experiment, five pixels in different positions are selected for the experiment, and the results are shown in Table 4. The two indexes performance of the competitive algorithms is also given, as shown in Table 5. According to Tables 4 and 5,

Table 3: Typical states of SEIR model

Method	Horizontal correlation	Vertical correlation	Diagonal correlation
Original image	0.8569	0.8665	0.8387
Proposed	0.0101	-0.0046	0.0008
Wang *et al.* [19]	-0.0352	0.0202	0.0375
Man *et al.* [12]	-0.0148	0.0037	0.0332

Table 4: NPCR and UACI values by changing the value of a pixel with proposed method

Index	(15,15)	(35,50)	(75,60)	(145,155)	(235,200)
NPCR	99.6077	99.6043	99.5347	99.5805	99.6095
UACI	33.5179	33.4272	33.4569	33.4819	33.4465

NPCR and UACI calculated by the proposed algorithm are very close to the ideal values. Therefore, the proposed algorithm has strong ability to resist differential attack.

Table 5: Other methods for NPCR and UACI

Method	NPCR	UACI
Wang *et al.* [19]	9.1553×10^5	6.2231×10^6
Man *et al.* [12]	0.3493	0.1173

6 Conclusions

In order to improve the secrecy performance of robot image, a hyperchaotic image encryption algorithm based on bit total scrambling and DNA is proposed in this paper. The innovative points of the algorithm are as follows: 1) the new four-dimensional hyperchaotic system adopted by the algorithm has the advantages of simple structure, fast calculation speed, large Lyapunov index and complex chaotic sequence, which is more conducive to image encryption; 2) The algorithm splashes 8 bit-planes of the image into a large bit-plane, and uses the hyperchaotic sequence to scramble the large bit-plane, realizing the global scrambling of image bits and enhancing the effect of bit-scrambling. Simulation results show that the new method not only has large key space, but also can effectively resist statistical analysis and differential attacks, and has better encryption effect and higher security. Considering that nowadays the minimum addressing unit of computer is generally byte, that is, 8bit, the algorithm based on bit scrambling proposed in this paper may produce a large number of repeated computations in the process of implementation, which will affect the computational efficiency. In the future, we will consider to improve the computational efficiency of the algorithm from the hardware aspect.

References

[1] I. Ahmed, M. Kashmoola, "CCF based system framework in federated learning against data poisoning attacks," *Journal of Applied Science and Engineering*, vol. 26, no. 7, pp. 973-981, 2022.

[2] X. Chai, X. Fu, Z. Gan, Y. Yu, Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Processing*, vol. 155, pp. 44-62, 2019.

[3] C. C. Chang, K. F. Hwang, M. S. Hwang, "Robust authentication scheme for protecting copyrights of images and graphics", *IEE Proceedings-Vision, Image and Signal Processing*, vol. 149, no. 1, pp. 43-50, 2002.

[4] G. Cheng, C. Wang, H. Chen, "A novel color image encryption algorithm based on hyperchaotic system and permutation-diffusion architecture," *International Journal of Bifurcation and Chaos*, vol. 29, no. 9, 2019.

[5] S. Cicek, A. Ferikoglu, I. Pehlivan, "A new 3D chaotic system: dynamical analysis, electronic circuit design, active control synchronization and chaotic masking communication application," *Optik*, vol. 127, no. 8, pp. 4024-4030, 2016.

[6] Q. Cun, X. Tong, Z. Wang, M. Zhang, "Selective image encryption method based on dynamic DNA coding and new chaotic map," *Optik*, vol. 243, 2021.

[7] K. Dong, R. Ali, P. Dominic, S. Ali, "The effect of organizational information security climate on information security policy compliance: The mediating effect of social bonding towards healthcare nurses," *Sustainability*, vol. 13, no. 5, pp. 2800, 2021.

[8] K. Fares, A. Khaldi, K. Redouane, E. Salah, "DCT & DWT based watermarking scheme for medical information security," *Biomedical Signal Processing and Control*, vol. 66, 2021.

[9] S. Han, E. Chang, T. Dillon, M. S. Hwang, C. C. Lee, "Identifying attributes and insecurity of a public-channel key exchange protocol using chaos synchro-

nization", *Chaos Solitons & Fractals*, vol. 40, no. 5, pp. 2569-2575, 2009.

[10] M. Kaur, D. Singh, "Multiobjective evolutionary optimization techniques based hyperchaotic map and their applications in image encryption," *Multidimensional Systems and Signal Processing*, vol. 32, no. 1, pp. 281-301, 2021.

[11] Z. Liu, D. Jiang, C. Zhang, H. Zhao, Q. Zhao, B. Zhang, "A novel fireworks algorithm for the protein-ligand docking on the autodock," *Mobile Networks and Applications*, vol. 26, pp. 657-668, 2021.

[12] Z. Man, J. Li, X. Di, Y. Sheng, Z. Liu, "Double image encryption algorithm based on neural network and chaos," *Chaos, Solitons & Fractals*, vol. 152, 2021.

[13] M. Mirtsch, K. Blind, C. Koch, G. Dudek, "Information security management in ICT and non-ICT sector companies: A preventive innovation perspective," *Computers & Security*, vol. 109, 2021.

[14] R. Reshmi, "Information security breaches due to ransomware attacks-a systematic literature review," *International Journal of Information Management Data Insights*, vol. 1, no. 2, pp. 100013, 2021.

[15] Z. Shaikh, A. Khan, L. Teng, A. Wagan, A. Laghari, "BIoMT modular infrastructure: The recent challenges, issues, and limitations in blockchain hyperledger-enabled e-healthcare application," *Wireless Communications and Mobile Computing*, vol. 2022, 2022.

[16] Q. Shi, S. Yin, K. Wang, L. Teng and H. Li, "Multichannel convolutional neural network-based fuzzy active contour model for medical image segmentation," *Evolving Systems*, vol. 13, no. 4, pp. 535-549, 2022.

[17] S. Wang, Q. Peng, B. Du, "Chaotic color image encryption based on 4D chaotic maps and DNA sequence," *Optics & Laser Technology*, vol. 148, 2022.

[18] T. Wang, M. Wang, "Hyperchaotic image encryption algorithm based on bit-level permutation and DNA encoding," *Optics & Laser Technology*, vol. 132, 2020.

[19] X. Wang, Y. Su, "Image encryption based on compressed sensing and DNA encoding," *Signal Processing: Image Communication*, vol. 95, 2021.

[20] X. Wang, S. Yin, M. Shafiq, A. Laghari, S. Karim, O. Cheikhrouhou, W. Alhakami, H. Hamam, "A new V-Net convolutional neural network based on four-dimensional hyperchaotic system for medical image encryption," *Security and Communication Networks*, vol. 2022, 2022.

[21] W. Wei, J. Tang, "Cooperative output regulation by Q-learning for discrete multi-agent systems in finite-time," *Journal of Applied Science and Engineering*, vol. 26, no. 6, pp. 853-864, 2022.

[22] Y. Xian, X. Wang, "Fractal sorting matrix and its application on chaotic image encryption," *Information Sciences*, vol. 547, pp. 1154-1169, 2021.

[23] C. Xu, J. Sun, C. Wang, "An image encryption algorithm based on random walk and hyperchaotic systems," *International Journal of Bifurcation and Chaos*, vol. 30, no. 4, 2020.

[24] Q. Xu, K. Sun, C. Cao, C. Zhu, "A fast image encryption algorithm based on compressive sensing and hyperchaotic map," *Optics and Lasers in Engineering*, vol. 121, pp. 203-214, 2019.

[25] F. Yang, J. Mou, J. Liu, C. Ma, H. Yan, "Characteristic analysis of the fractional-order hyperchaotic complex system and its image encryption application," *Signal processing*, vol. 169, 2020.

[26] S. Yin, H. Li, "GSAPSO-MQC:medical image encryption based on genetic simulated annealing particle swarm optimization and modified quantum chaos system," *Evolutionary Intelligence*, vol. 14, pp. 1817-1829, 2021.

[27] J. Zeng, C. Wang, "A novel hyperchaotic image encryption system based on particle swarm optimization algorithm and cellular automata," *Security and Communication Networks*, vol. 2021, 2021.

[28] J. Zhang, D. Huo, "Image encryption algorithm based on quantum chaotic map and DNA coding," *Multimedia Tools and Applications*, vol. 78, no. 11, pp. 15605-15621, 2019.

[29] Y. Zhang, L. Zhang, Z. Zhong, L. Yu, M. Shan, "Hyperchaotic image encryption using phase-truncated fractional Fourier transform and DNA-level operation," *Optics and Lasers in Engineering*, vol. 143, 2021.

Biography

Jianjun Zhu biography. Jianjun Zhu is with School of Electronics and Electrical Engineering, Zhengzhou University of Science and Technology. His interests are deep learning, AI, image processing.

Jian'E Zhao biography. Jian'E Zhao is with School of Electronics and Electrical Engineering, Zhengzhou University of Science and Technology. His interests are deep learning, AI, image processing.