Image Encryption Based on Hyperchaotic Systems And DNA Encoding

Lei Wang
(Corresponding author: Lei Wang)

Basic Department, Zhengzhou University of Science and Technology
Email: chenwwencww@163.com

(Received Dec. 25, 2022; Revised and Accepted Apr. 16, 2023; First Online Apr. 30, 2023)
The Special Issue on Computational Intelligence Networks for Privacy and Security in Evolving Internet of Multimedia Things
Special Editor: Prof. Shoulin Yin (Harbin Institute of Technology)

Abstract

To effectively improve the quality of image encryption and the security of data transmission, this paper proposes a new image encryption theme based on Hyperchaotic systems and DNA encoding. First, L plaintext images are operated by a double-layer cross-coupled piece-wise linear chaotic map (PWLCM). And the noise-like images are obtained by XOR merging. Then, based on the chaotic sequence, the image plaintext is encoded by DNA, and the image scrambling and diffusion are realized by DNA operation, so the image encryption is completed. Finally, Simulation results show that this new encryption algorithm's number of Pixels Change Rate (NPCR) and Unified Average Change Intensity (UACI) is close to or higher than the theoretically calculated values. Furthermore, the Peak Signal Noise Ratio (PSNR) is less than 10, indicating that the proposed algorithm is susceptible to plaintext and key and can effectively resist differential attacks.

Keywords: DNA Encoding; Hyperchaotic Systems; Image Encryption; Scrambling and Diffusion

1 Introduction

With the development of network, there are many information carriers. Digital image has become the most extensive communication medium in network communication because of its high fidelity and vivid image. But in the actual network life and real life, there are a lot of images are used fraudulantly, copyright infringed [5, 15, 16]. For example, some people will use other people's photos to carry out illegal activities, violating others' privacy. No one wants their privacy violated. Therefore, the security of image information becomes the focus of people's attention, and some image encryption technology is urgently needed to protect the image information.

Image information redundancy is large. Generally for text encryption practical encryption algorithms such as DES [21], 3DES [2] and so on, it cannot achieve good results on the image, therefore, chaotic encryption is arised. Since many earlier chaotic systems are easy to be attacked and cracked, resulting in information exposure. So high-dimensional chaotic systems, hyperchaotic systems, deep learning, wavelet transform combined with chaotic system image encryption operations have been emerged.

Chaos is widely used in the field of image encryption because of its randomness, high sensitivity to initial value and replicability [20]. There are two kinds of image encryption methods. One is to improve the original chaotic mapping to increase its complexity and security. The second is to improve the encryption algorithm. Reference [17] expanded the scope of the mapping by improving the Logistic mapping. Reference [6] increased the complexity of sequences and enhanced the scrambling diffusion effect by improving Henon mapping. Reference [18] improved Lorenz equation to make its chaotic behavior more complicated. Reference [24] combined Sine mapping and Logistic mapping to form a chaotic system with higher complexity.

Traditional encryption algorithms, such as Arnold scrambling transform [8] and Hilbert scrambling transform [14], have some defects and low security. Therefore, reference [12] proposed an encryption algorithm that scrambled filling curves and adjacent pixel bits. Reference [23] proposed a hybrid Encryption algorithm based on the advantages of Data Encryption Standard (DES) algorithm, such as high efficiency, strong security and good performance, combined with Logistic mapping. Reference [4] proposed the calculation of Deoxyribo Nucleic Acid (DNA), which provided a new direction for image encryption algorithm technology. In reference [10], two-dimensional Logistic mapping was used to generate chaotic sequences, and DNA coding algorithm was combined to encrypt images. In reference [19], Lorenz and Rossler double chaotic system was used by combining with DNA coding to increase the complexity of computation and difficulty of cracking. In this paper, an improved Hyperchaotic chaotic map with better chaos is designed.

An image encryption algorithm based on Hyperchaotic systems and DNA encoding is proposed by combining with the DNA sequences with high parallelism and abundant storage space.

2 Related Works

2.1 Piece-wise Linear Chaotic Map (PWLCM)

When selecting any chaotic mapping in image encryption, two important characteristics of chaotic mapping, namely ”simplicity” and ”ergodicity”, must be considered. Compared with other one-dimensional chaotic systems, PWLCM is relatively uniform in phase distribution and has simple equations, satisfying the above two features [3]. Therefore, the PWLCM system will be used in this paper to generate random sequences, its dynamic equation is defined as follows:

$$x_{i+1} = F_p(x_i) \quad = \quad \left\{ \begin{array}{l} x_i/p \text{ if } 0 \leq x_i < p \\ x_i - p/0.5 - p \text{ if } p \leq x_i < 0.5 \\ F_p(1 - x_i) \; 0.5 \leq \mathrm{x_i} < 1 \end{array} \right\}$$

Where, p is the control parameter, whose value range is $(0, 0.5)$. $x_i \in [0, 1)$ is the state variable. In the encryption algorithm in this paper, in order to obtain a more unpredictable chaotic sequence, PWLCM mapping is used to carry out double-layer cross-coupling operation, and the behavior trajectory generated is more complex and not easy to predict, which can achieve a better image scrambling effect.

2.2 2D-CTMM Chaotic System

Low-dimensional chaotic system runs fast, but it has some problems, such as small key space, easy to predict behavior trajectory and low security performance. However, the behavior trajectory of high-dimensional chaotic system is difficult to predict and the structure is complex, which leads to the decrease of encryption rate. After weighing encryption rate and encryption security, this paper combines one-dimensional tent chaotic mapping [9] and one-dimensional cubic chaotic mapping to propose two-dimensional cubic tent chaotic mapping (2D-CTMM). This is a new chaotic system, which combines two one-dimensional chaotic systems. Compared with other high-dimensional chaotic systems, 2D-CTMM has a simple structure. Compared with low-dimensional chaotic system, its behavior trajectory is not easy to predict. On the premise that encryption security is satisfied, 2D-CTMM has a relatively high running rate, and its system equation is shown in Equations (1) and (2):

$$x_{i+1} \quad = \quad \left\{ \begin{array}{l} 4ax_i + 4by_i/0.5mod1 \text{ if } y_i < 0.5 \\ 4ax_i + 4b(1 - y_i)/0.5mod1 \text{ if } y_i \geq 0.5 \end{array} \right. \quad (1)$$

$$y_{i+1} \quad = \quad \left\{ \begin{array}{l} 4ay_i + 4bx_i/0.5mod1 \text{ if } x_i < 0.5 \\ 4ay_i + 4b(1 - x_i)/0.5mod1 \text{ if } x_i \geq 0.5 \end{array} \right. \quad (2)$$

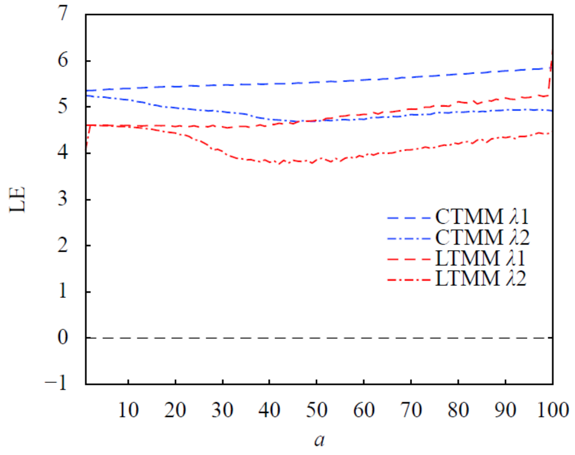

Figure 1: Comparison of LE curve between CTMM and LTMM

Where, a and b are control parameters of the 2D-CTMM system. mod is complementary function. Since the modular operation of a 2D-CTMM chaotic system is whole-office bounded, it can always fold the value into a fixed range, so the value of the control parameter can be set to any large value. In this article, the parameter range is set to $a, b \in [1, 100]$.

2.3 Performance Analysis of 2D-CTMM Chaotic System

Lyapunov exponent (LE) is a key quantitative index to measure the dynamic characteristics of the system, which describes the convergence rate or divergence rate of the system trajectory. When there are multiple Lyapunov exponentials greater than zero in a chaotic system, it indicates that the chaotic system has hyperchaotic behavior.

Compared with other two-dimensional chaotic maps, Two-dimensional logistic tent modular map (2D-LTMM) shows better chaotic characteristics, so in this paper, the Lyapunov exponential curve of 2D-CTMM and 2D-LTMM is compared, as shown in Figure 1. The initial value is set as $x0 = 0.528$, $y0 = 0.135$, control parameter $b = 50$, $a \in [1, 100]$. As can be seen from Figure 1, 2D-CTMM is in hyperchaotic behavior in the whole interval range, and compared with 2D-LTMM, 2D-CTMM has a larger LE value, indicating that it has more complex chaotic characteristics.

2.4 DNA Encoding Rule and Operation

According to the base-complementary pairing rules in biology, adenine (A) complements thymine (T) and cytosine (C) complements guanine (G). This is similar to the complementarity of 0 and 1 in binary, with the binary number being 00, 01, 10 and 11. There are 24 encoding rules according to permutation and combination, but only 8 encoding rules in Table 1 are left according to DNA encoding rule [22]. The operations of DNA sequence mainly include addition, subtraction and XOR operations. Eight kinds of rules correspond to eight kinds of DNA arithmetic rules.

Table 1: DNA encoding rule

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

3 Proposed Image Encryption Algorithm

Known plaintext matrix P and the chaotic sequence generated by the key set $A = A_1, A_2, \cdots, A_I | I \in C^*$, $B = B_1, B_2, \cdots, B_I | I \in C^*$. Where A_I and B_I represent the $I - th$ chaotic sequence. C^* represents the set of positive integers. In this paper, the encryption process of the image encryption algorithm based on Hyperchaotic systems and DNA encoding is shown in Figure 2. First, it takes each element in sets A and B to 8 decimal places, and maps the element in set A to [1, 8] through certain operations to obtain $Q = Q_1, Q_2, \cdots, Q_I | I \in C^*$. Similarly, it maps the elements of set B to [1,8] and [1,3] respectively, and gets $W = W_1, W_2, \cdots, W_I | I \in C^*$ and $E = E_1, E_2, \cdots, E_I | I \in C^*$. Q and W correspond to 8 encoding rules, and E corresponds to 3 operation rules. Secondly, the elements in set A are converted into a ciphertext matrix of the same size $(M \times N)$ as the plaintext matrix P. Each element in the plain-text and ciphertext matrices is converted to an 8-bit binary number. According to the DNA encoding rules in Table 1, DNA encoding is performed for every 2 bits of binary number. If the plaintext encoding rule is determined by Q and the ciphertext encoding rule is determined by W, each element can be converted into four DNA encodes. In order to ensure that the matrix size remains $M \times N$ after DNA encoding, the plaintext and ciphertext are partitioned according to every 4 DNA codes to generate a new plaintext matrix P' and a new ciphertext matrix A' with size $M \times N$ and composed of DNA codes. Then, DNA operation is carried out on DNA code blocks at corresponding positions in the new plaintext matrix and the new ciphertext matrix. The operation rules are determined by E, and the scrambling matrix R is obtained. Next, starting with the last element, each element in the scrambled matrix R is DNA computed with the previous element to obtain the diffusion matrix R'. Finally, the diffusion matrix is decoded for DNA and restored to binary sequence, and the final encrypted image matrix R'' is obtained by reconstructing the matrix.

3.1 Key Generation

In the process of generating the system key, this paper uses two improved mappings. The first mapping produces the initial values x_0, y_0 and parameters a, b of the chaotic sequence. The second mapping produces the initial values x'_0, y'_0 and parameters a', b' of the chaotic sequence. The generating process of initial values x_0, x'_0, y_0, y'_0 is connected with the original image information to form a dynamic key and achieve an one-password encryption effect. Parameters a, a', b, b' are used as fixed keys.

Firstly, XOR operation is performed by pixel and an 8-bit binary number, then all pixel values are added to generate a new value, and then divided by the size of the plaintext image. Finally, the decimal part is taken as the key. The calculation formula is as follows:

$$K_i = mod(sum(P \oplus N_i)/(M \times N), 1).$$

Where, K is the generated key and P is the plaintext information. N_i is any number in the range of 0 to 255. mod indicates mod operation. $M \times N$ is the size of the plaintext image.

3.2 Generation of Decision Parameters

The image encryption algorithm based on hyperchaotic sequence and DNA encoding in this paper has three decision parameters, Q, W and E. Q is used to determine the DNA encoding mode of the plaintext and the final decoding mode, which is generated by the first chaotic sequence. W is used to determine the DNA encoding mode of the ciphertext. E is used to determine the algorithm and is generated by the second chaotic sequence.

Firstly, it takes the decimal part of the sequence, and then converts the sequence value to 0-255. The calculation formula is as follows:

$$\begin{aligned} A'(i) &= A(i) - floor(A(i)). \\ A''(i) &= mod(floor(A'(i) \times 10^8), 256). \end{aligned}$$

Then the parameters Q, W and E are generated. The size of Q and W ranges from 1 to 8, corresponding to 8 encoding rules. The range of E is 1-3 corresponding to 3 operation modes, and the values of $Q(i)$, $W(i)$ and $E(i)$ are converted into:

$$\begin{aligned} Q(i) &= \mathrm{mod}(A''(i), 8) + 1. \\ W(i) &= \mathrm{mod}(B''(i), 8) + 1. \\ E(i) &= \mathrm{mod}(B''(i), 3) + 1. \end{aligned}$$

3.3 Scrambling and Diffusion Operations

First, the elements in the plaintext and ciphertext matrices are converted to binary numbers. According to the

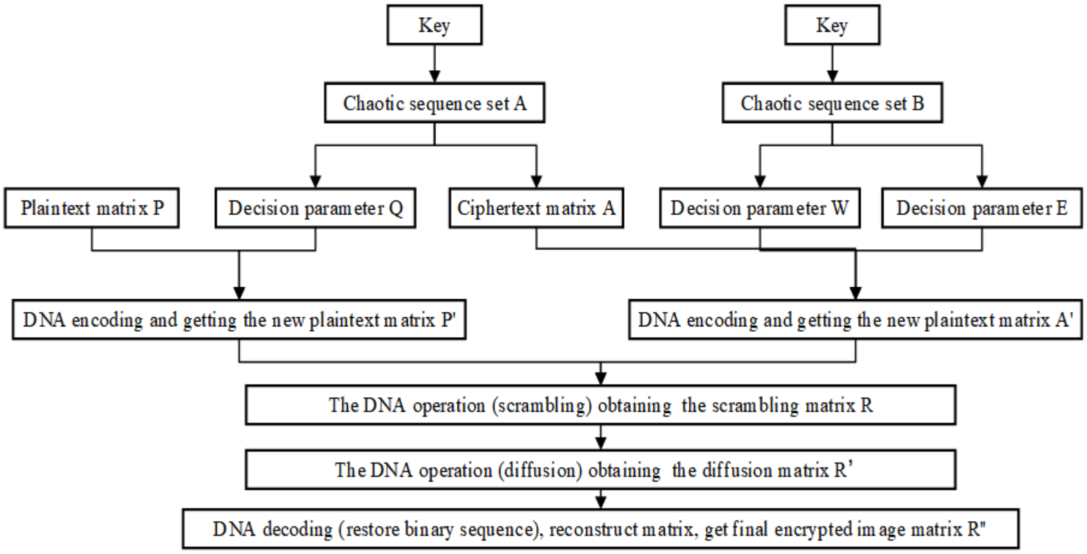
Key
Chaotic sequence set A
Key
Chaotic sequence set B
Plaintext matrix P
Decision parameter Q
Ciphertext matrix A
Decision parameter W
Decision parameter E
DNA encoding and getting the new plaintext matrix P'
DNA encoding and getting the new plaintext matrix A'
The DNA operation (scrambling) obtaining the scrambling matrix R
The DNA operation (diffusion) obtaining the diffusion matrix R'
DNA decoding (restore binary sequence), reconstruct matrix, get final encrypted image matrix R"

Figure 2: Image encryption process

encoding rules in Table 1, every 2 bits are used for DNA encoding, and every 4 DNA codes form an encoding block. The plaintext selects the encoding rule according to the Q value, and the ciphertext selects the encoding rule according to the W value, and each element corresponds to different Q and W, realizing dynamic encoding. Then the scrambling operation is performed. According to the corresponding E value, DNA operation is performed on the plaintext block and ciphertext block. The calculation formula is as follows:

$$R(i) = f(A(i), P(i), E(i)).$$

Where, $R(i)$ is the block of the $i-th$ block after scrambling. f is DNA operation. $A(i)$ is the $i-th$ ciphertext block after DNA encoding. $P(i)$ is the $i-th$ plaintext block after DNA encoding. $E(i)$ is the operation mode selected by block i.

Then there is the diffusion operation. DNA operation is performed again on $R(i)$ and the previous scrambled block $R(i-1)$. The calculation method is also determined by the value of E. The calculation formula is as follows:

$$R'(i) = f(R(i), R(i-1), E(i)).$$

4 Image Encryption Performance Analysis

4.1 Encryption Effect and Histogram Analysis

The dynamic key $x_0 = 0.8945$, $y_0 = 0.3694$, $x_0' = 0.9978$, $y_0' = 0.3642$ is generated by the improved hyperchaotic mapping. Fixed key $a = 12.0011$, $b = 40.0012$, $a' = 16.3779$, $b' = 42.8676$. A 256-level gray image of 512×512 is selected and MATLAB2020b platform is adopted for simulation experiment. The image encryption effect and histogram are shown in Figures 3 and 4.

Image decryption is the reverse process of encryption. First, two chaotic sequences are generated using the eight keys used in encryption, and the decision parameters, DNA decoding, and inversion rules are generated from them. That is, DNA addition is decrypted by subtraction, and subtraction is decrypted by addition. Then, according to DNA inversion rules and decision parameters, the diffusion and scrambling operations are carried out successively. Finally, DNA decoding is used to restore the binary sequence to get the decrypted image. The image decryption effect and histogram are shown in Figures 3 & 4. As can be seen from figure 3, the decrypted image is completely consistent with the original image and its histogram after decryption using the proposed algorithm, indicating that the proposed algorithm has a good decryption effect. As can be seen from Figure 4, the encrypted image can no longer distinguish the original image information visually and is close to the noisy image. The gray value distribution of encrypted images is more uniform, which means that the images are more difficult to identify, provide less effective information, and have higher security.

4.2 Information Entropy Analysis

Information entropy [11] is one of the indicators to measure the effect of image encryption. The maximum entropy of a grayscale image is 8. Ifthe encryption effect is better, the information entropy is closer to 8. The calculation formula is as follows:

$$H(x) = -\sum_{i=1}^{2N-1} P_i log_2 P_i.$$

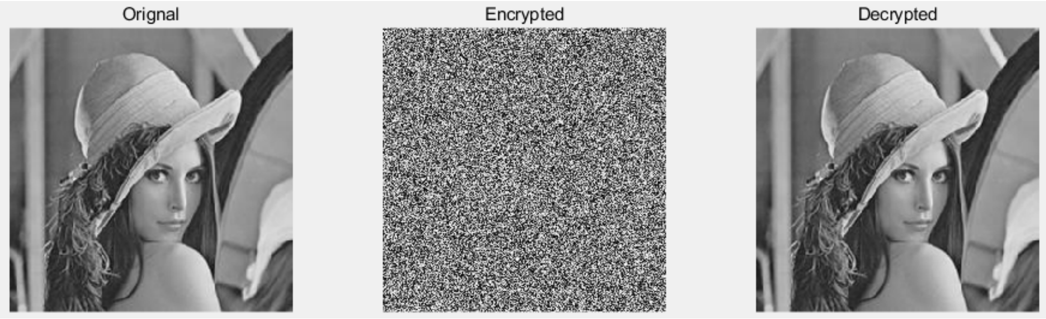

Figure 3: Encryption and decryption effect

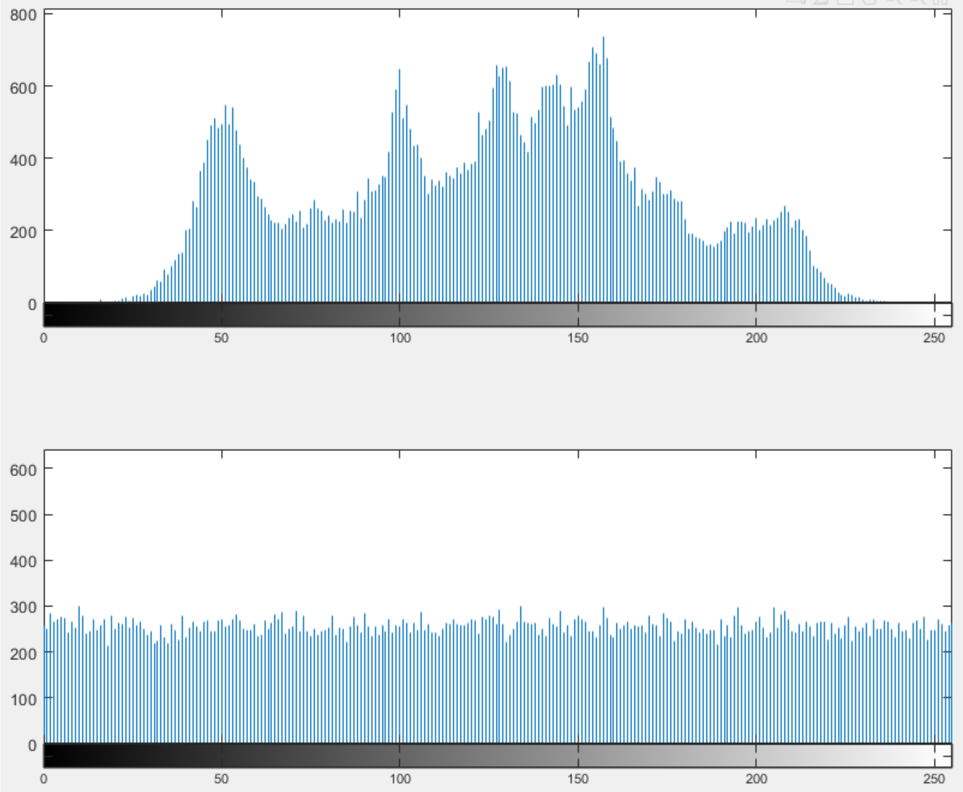

Figure 4: Encryption and decryption image gray histogram

Where, $H(x)$ is information entropy. P_i is the probability of gray value i.

The plaintext image in figure 3 is selected and the ciphertext image is encrypted by the algorithm in this paper. The entropy of plaintext and ciphertext information is calculated and compared with the entropy values obtained in reference [7] and reference [13]. The results are shown in Table 2.

Table 2: Plaintext and ciphertext entropy of different algorithms

Method	Plaintext entropy	Ciphertext entropy
Proposed	7.3733	7.9995
reference [7]	7.4543	7.9974
reference [13]	7.3451	7.9896

As can be seen from Table 2, in the three algorithms, the image information entropy after encryption with the proposed algorithm is closer to 8, indicating that the proposed algorithm has better encryption effect.

4.3 Differential Attack Resistance and Sensitivity Analysis

Differential attack is mainly through changing the original image information, and then encrypting with the same key by comparing the difference before and after the image encryption to find the difference between the plaintext and the key, so as to decipher the encrypted image. Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are used to evaluate the differential attack resistance capability. NPCR reflects the ratio of different gray values of different images at the same position. UACI reflects the average density of change between different images. The larger NPCR and UACI denote the better differential attack resistance, the stronger sensitivity, and the better encryption effect. NPCR and UACI are calculated as follows:

$$NPCR = \frac{\sum_{i,j} G(i,j)}{M \times N} \times 100/\%.$$

$$UACI = \frac{1}{M \times N} \sum_{i,j} \frac{R_1(i,j) - R_2(i,j)}{255} \times 100/\%.$$

In the formula, $R_1(i,j)$ and $R_2(i,j)$ are the pixel values of pixel points in $i-th$ row and $j-th$ column of the original encrypted image and the changed encrypted image respectively. When $R_1(i,j) = R_2(i,j)$, $G(i,j) = 0$, otherwise $G(i,j) = 1$.

In reference [1], the 256-grade gray image was theoretically calculated according to Equations (**??**) and (**??**), and the theoretical calculated values of NPCR and UACI were 99.6094% and 33.465%, respectively.

In the experiment of plaintext sensitivity analysis, firstly, the new algorithm in this paper is used to encrypt the original plaintext image to form the original encrypted image. Then, the pixel value of a certain point in the original plaintext image is changed, and the new algorithm is used for encryption to form a new encrypted image. The original encrypted image is compared with the new encrypted image to obtain NPCR and UACI. In the experiment, $P(i,j)$ represents the pixel value of coordinate point (i,j). The pixel value of the coordinate (20,30) is changed from 12 to 13, the pixel value of the coordinate (155,100) is changed from 14 to 15, the pixel value of the coordinate (200,300) is changed from 169 to 170, and the pixel value of the coordinate (512,512) is changed from 65 to 66. The test results are shown in Table 3.

Table 3: Plaintext sensitivity of the proposed algorithm

Index	NPCR	UACI
P(20,30)	99.6151	33.4862
P(155,100)	99.6372	33.4015
P(200,300)	99.6179	33.4062
P(512,512)	99.6234	33.4323

As can be seen from Table 3, the calculated NPCR and UACI values are close to or higher than the theoretical calculated values in reference [1] when the pixel value of a coordinate point of the plaintext image is slightly changed and encrypted by the new algorithm in this paper. It shows that the proposed algorithm can effectively resist differential attacks and has high plaintext sensitivity.

5 Conclusion

This paper proposes an image encryption algorithm based on hyperchaotic mapping and DNA coding, which enhances the security of images, expands the key space, and improves the ability to resist differential attacks. However, the new algorithm in this paper only applies to 256-level gray image encryption. The subsequent plan is to carry out research on color image encryption, extract RGB channels of color images, and carry out chaotic encryption for each channel and between channels, so as to further improve the application of the algorithm in the field of image encryption.

Acknowledgments

This study was supported by the Key Project of Science and Technology Department of Henan Province, Project No. 172102210113. The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] H. N. Abdullah, H. A. Abdullah, "Image encryption using hybrid chaotic map," *2017 International*

Conference on Current Research in Computer Science and Information Technology (ICCIT). IEEE, pp. 121-125, 2017.

[2] R. P. Adhie, Y. Hutama, A. S. Ahmar, *et al.*, "Implementation cryptography data encryption standard (DES) and triple data encryption standard (3DES) method in communication system based near field communication (NFC)," *Journal of Physics: Conference Series. IOP Publishing*, vol. 954, no. 1, pp. 012009, 2018.

[3] A. Ali, M. A. Khan, R. K. Ayyasamy, *et al.*, "A novel systematic byte substitution method to design strong bijective substitution box (S-box) using piece-wise-linear chaotic map," *PeerJ Computer Science*, vol. 8, pp. e940, 2022.

[4] H. R. Amani, M. Yaghoobi, "A new approach in adaptive encryption algorithm for color images based on DNA sequence operation and hyper-chaotic system," *Multimedia Tools and Applications*, vol. 78, pp. 21537-21556, 2019.

[5] 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.

[6] Y. Chen, S. Xie, J. Zhang, "A hybrid domain image encryption algorithm based on improved henon map," *Entropy*, vol. 24, no. 2, pp. 287, 2022.

[7] M. Gupta, V. P. Singh, K. K. Gupta, *et al.*, "An efficient image encryption technique based on two-level security for internet of things," *Multimedia Tools and Applications*, vol. 82, no. 4, pp. 5091-5111, 2023.

[8] H. Huang, Z. Cai, "Duple color image encryption system based on 3D non-equilateral arnold transform for IIoT," *IEEE Transactions on Industrial Informatics*, 2022.

[9] S. Kanwal, S. Inam, M. T. B. Othman, *et al.*, "An effective color image encryption based on henon map, tent chaotic map, and orthogonal matrices," *Sensors*, vol. 22, no. 12, pp. 4359, 2022.

[10] H. Liu, B. Zhao, L. Huang, "A remote-sensing image encryption scheme using DNA bases probability and two-dimensional logistic map," *IEEE Access*, vol. 7, pp. 65450-65459, 2019.

[11] Y. Liu, T. Zhi, M. Shen, *et al.*, "Software-defined DDoS detection with information entropy analysis and optimized deep learning," *Future Generation Computer Systems*, vol. 99-114, no. 129, 2022.

[12] P. Praveenkumar, R. Amirtharajan, K. Thenmozhi, *et al.*, "Fusion of confusion and diffusion: A novel image encryption approach," *Telecommunication Systems*, vol. 65, no. 65-78, 2017.

[13] Y. Sang, J. Sang, M. S. Alam, "Image encryption based on logistic chaotic systems and deep autoencoder," *Pattern Recognition Letters*, vol. 153, pp. 59-66, 2022.

[14] V. K. Sharma, P. C. Sharma, H. Goud, *et al.*, "Hilbert quantum image scrambling and graph signal processing-based image steganography," *Multimedia Tools and Applications*, vol. 81, no. 13, pp. 17817-17830, 2022.

[15] A. Shobanadevi, G. Maragathm, S. M. P. Gangadharan, *et al.*, "Internet of Things-based data hiding scheme for wireless communication," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1-8, 2022.

[16] W. Wan, J. Wang, Y. Zhang, *et al.*, "A comprehensive survey on robust image watermarking," *Neurocomputing*, Vol. 488,?pp. 226-247, 2022.

[17] H. Xiang, L. Liu, "An improved digital logistic map and its application in image encryption," *Multimedia Tools and Applications*, vol. 79, pp. 30329-30355, 2020.

[18] L. Wang, H. Song, P. Liu, "A novel hybrid color image encryption algorithm using two complex chaotic systems," *Optics and Lasers in Engineering*, vol. 77, pp. 118-125, 2016.

[19] S. Wang, L. Hong, J. Jiang, "An image encryption scheme using a chaotic neural network and a network with multistable hyperchaos," *Optik*, vol. 268, pp. 169758, 2022.

[20] X. Wang, S. Yin, M. Shafiq, A. 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, pp. 1-14, 2022.

[21] W. Yihan, L. Yongzhen, "Improved design of DES algorithm based on symmetric encryption algorithm," *2021 IEEE International Conference on Power Electronics, Computer Applications (ICPECA). IEEE*, pp. 220-223, 2021.

[22] 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.

[23] Q. Zhang, "An overview and analysis of hybrid encryption: The combination of symmetric encryption and asymmetric encryption," in *2nd international conference on computing and data science (CDS)*, IEEE, pp. 616-622, 2021.

[24] J. Zheng, L. F. Liu, "Novel image encryption by combining dynamic DNA sequence encryption and the improved 2D logistic sine map," *IET image processing*, vol. 14, no. 11, pp. 2310-2320, 2020.

Biography

Lei Wang biography. Wang Lei (1980-), Associate professor, Zhengzhou University of Science and Technology, born in Nanyang, Henan Province, 450064, China. He is mainly engaged in differential equation theory and algorithm research.