A Trademark Graphic Encryption Algorithm Based on Discrete Chaotic System and Its Performance Analysis

Ji Xu[1], Bo Sun[2(✉)], Xujiong Ma[1], Peng Li[1], and Jun Mou[1]

[1] School of Food Science and Technology, Dalian Polytechnic University, Dalian 116034, China
[2] School of Management, Dalian Polytechnic University, Dalian 116034, China
sunbo_0709@126.com

Abstract. Based on chaos system and DNA encryption algorithm, a novel encryption scheme for enterprise trademark image has been proposed. Firstly, chaotic sequence generate by chaotic map is employed for disrupt the value of each pixel point in the encrypted trademark, In next stage, image matrix are encode into DNA sequence and through DNA calculation operation to diffusing the image matrix, Finally obtain cipher image. Experimental simulation results show that the algorithm can effectively encrypt the trademark image, and the correlation with the original image is very low, and it has a large key space can resist conventional attack and convenient for practical application. The trademark encryption algorithm based on chaotic system and DNA sequence operation proposed in this paper has a good application value in the protection of enterprise intellectual property rights.

Keywords: DNA sequence · 3D discrete chaotic model · Dynamic analysis · Image encryption algorithm

1 Introduction

With the rapid development of computer science and communication, data protection has become increasingly serious issue to internet industries. Because of the registered trademark include many sensitive information, they have special value to enterprise. As turn out, They may be more easily to be the target of attacker [1]. Based on traditional data encryption algorithms such as DES and AES can effectively protect sensitive data of enterprises from attacker [2, 3]. However, considering the characteristics of strong correlation between adjacent pixels and large amount of data in the image data of trademarks, and with the constant change of data attack mode, the technical details of the above algorithm can no longer competent the requirements of data encryption. As a result, design new encryption algorithm on the basis of high-randomness sequence with more better performance and randomness drawn more and more attention.

Chaotic maps have advantages are shown in complexity, good ergodicity in the phase space and sensitivity to initial parameters, which is suitable infiltrated into information security [4, 5]. Therefore, in accordance with chaotic maps, a variety of

J. Jin et al. (Eds.): GreeNets 2019, LNICST 282, pp. 204–217, 2019.
https://doi.org/10.1007/978-3-030-21730-3_22

image encryption algorithm has been widely used in image processing field [6–26, 30]. For instance, the encryption algorithm on based of HD discrete chaotic map [4, 17], it has good encryption features, including have larger information entropy space, good Pixels Change Rate (Number of Pixels Change Rate, NCPR) and the Unified Average Changing Intensity (UACI) reduce the correlation between the encrypted image and the plaintext image.

In this paper, a novel encryption algorithm based on HD discrete chaotic map and DNA encode operation of trademark image has proposed. The rest part of this paper structure as follow. In Sect. 2, dynamics analysis of the chaotic system is carried out, show the corresponding analysis results. In Sect. 3, the genetic coding law of DNA is briefly explained. In Sect. 4, describe the encryption algorithm and decryption algorithm workflow respectively, and shows the encryption and decryption image. In Sect. 5, according to the obtained images, the security performance of the algorithm has analyzed, and the results of relevant technical performance indexes are presented. In Sect. 6, obtain important conclusion.

2 Characteristic Analysis of 3D Discrete Chaotic System

2.1 Chaos Dynamics Analysis of 3D Discrete Chaos Model

As discussed in Sect. 1, In this research, a new 3D discrete chaotic map based on Sine and ICMIC map has accepted. The chaotic map is defined as Eq. (1).

$$\begin{cases} x_{i+1} = a\sin(bz_i)\sin(\frac{c}{x_i}) \\ y_{i+1} = a\sin(bx_{i+1})\sin(\frac{c}{y_i}) \\ z_{i+1} = a\sin(by_{i+1})\sin(\frac{c}{z_i}) \end{cases} \tag{1}$$

Set system parameters $a = 1$, $b = 2\pi$, $c = 11.5$, initial value $(x_0, y_0, z_0) = [0.3, 0.5, 0.6]$. At this point, the system phase diagram is shown in Fig. 1.

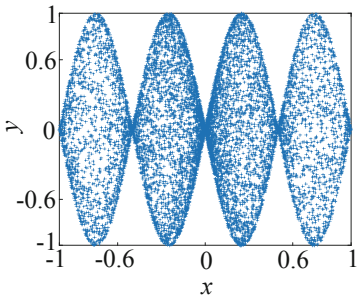


Fig. 1. Chaotic attractor phase diagram in the x-y plane

As show in Fig. 1, On the one view point, the attractor phase diagram occupies most of the region in the *x*-*y* plane, indicating that the system has a large key space., On another advantage point, The phase diagram is symmetric about the X-axis and Y-axis in the *x*-*y* plane. Because of the ergodicity of the chaotic system and sensitivity to initial conditions, the state of the system at the next moment is unpredictable. Therefore, it is more advantageous to use this system to generate pseudo-random sequences.

2.2 Influence of Parameters on System Performance

Keep the initial value of the system (x_0, y_0, z_0) = [0.3, 0.5, 0.6], change the parameters and use Lyapunov exponent spectrum and bifurcation diagram to evaluate system performance. The Fig. 2 shown the LEs and BDs of 3D-SIMM.

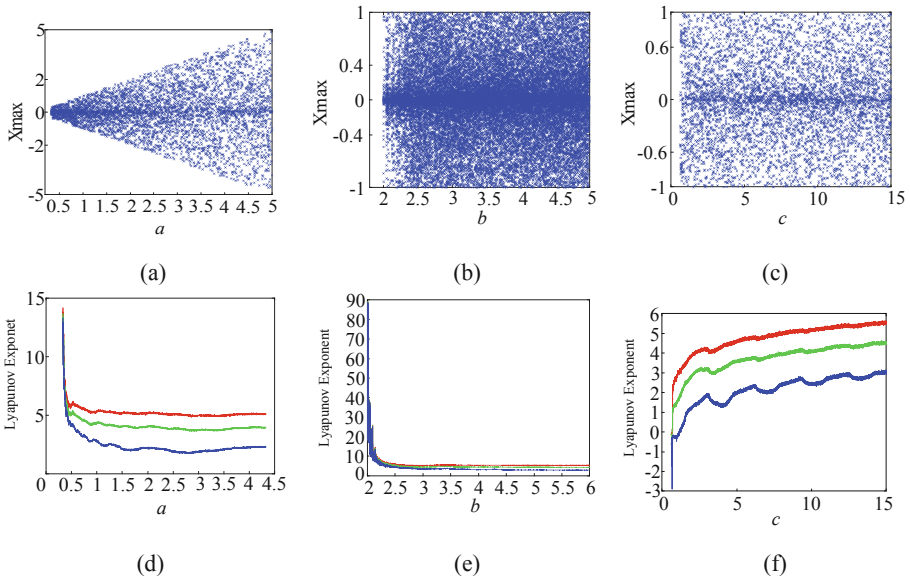


Fig. 2. Lyapunov exponent spectrum and bifurcation diagram

When parameters $a = 1$, $b = 2\pi$, $c = 11.5$, the Lyapunov exponent of the system are obtained as (λ_1, λ_2, λ_3) = (5.2325, 4.2972, 2.7538). on the basic of Lyapunov exponent, the system is hyper-chaotic.

When parameters had changed, As shown in Figs. 2(a) and (d), 3D-SIMM is hyper-chaotic when $a \in [0.33, 5]$, As shown in Figs. 2(b) and (c), When $b \in [2, 8]$, the system is hyper-chaotic. As shown in Figs. 2(c) and (f), When $c \in [0.62, 15]$, the system is hyper-chaotic.

2.3 Entropy Complexity of Permutation

The randomness of the system can be expressed by permutation entropy. The higher of permutation entropy number show good randomness of the system. Set $d = 5$ for the embedded dimension and time delay is 1. The entropy results of system arrangement are shown in Fig. 3.

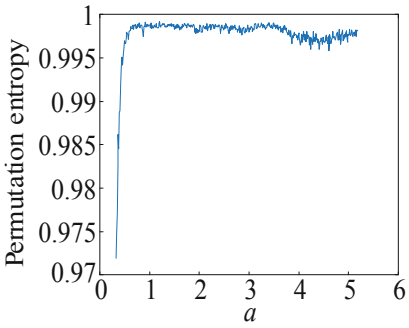


Fig. 3. Permutation entropy complexity

When the system parameter a $\in$ (0.33, 5), the entropy of system is 0.997, which is close to the theoretical value 1. It can proved the system has good randomness and generate more complex chaotic sequences.

3 DNA Coding Rules

The basic unit of deoxyribonucleic acid (DNA) is the deoxynucleotide. In the process of encryption, algorithm is subject to the principle of base complementary pairing. The specific content as follows: Adenine (A) is associated with Thymine (T). Cytosine (C) pairs with Guanine (G). According to the principle of base complementary pairing, the number of elements in DNA sequence follows the Eq. (2).

$$\begin{cases} x_i \neq L(x_i) \neq L(L(x_i)) \neq L(L(L(x_i))) \\ x_i = L(L(L(L(x_i)))) \end{cases} \tag{2}$$

The law of correspondence between DNA and binary number and the law of addition and subtraction of the four basic elements of DNA are shown in the following Tables 1 and 2.

Table 1. The law of encoding

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

Table 2. Addition and subtraction rules

+	A	C	G	T	–	A	C	G	T
A	A	C	G	T	A	A	T	G	C
C	C	G	T	A	C	C	A	T	G
G	G	T	A	C	G	G	C	A	T
T	T	A	C	G	T	T	G	C	A

4 Encryption Algorithm Design

4.1 Key Format

Set (a, b, c) are system parameters, (x_0, y_0, z_0) are initial values, m and n as the number of iterations required by the system to generate pseudo random sequences. On the other side, the initial deoxynucleotide code was c_0, the code of DNA coding and decoding rules was expressed as $\alpha(\alpha \in [1, 8])$ and $\beta(\beta \in [1, 6])$, respectively, and the code of base complementary pairing rules was $L_i(L \in [1, 6]$, i = 1, 2…, 8). The key format composition involved in the algorithm designed in this paper are shown in Table 3.

Table 3. Key format

a	b	c	x_0	y_0	z_0	m	n	c_0	α	β	L_i

4.2 Encryption Algorithm Flow

In this paper, The encryption algorithm designed includes image matrix scrambling and pixel number diffusion. In the scrambling part, at the begin, a pseudo-random sequence generated and transformed by 3D-SIMM, the image matrix of the encrypted object is scrambled by this sequence. In the pixel diffusion part, the scrambled image matrix and pseudo-random sequence are encoded into DNA sequence, and then the image pixel points are diffused. Finally, the algorithm will obtain the final pixel value matrix and output the encrypted image. The specific encryption process is shown in Fig. 4.

The detailed steps of the encryption algorithm are as follows:

Step 1: Input the image and convert it into the pixel value matrix. According to the Eqs. (3) and (4), use initial value and system parameters of the chaotic map to obtain the new system variable values of the chaotic map.

$$S = \frac{\sum_{i=1}^{H}\sum_{j=1}^{W} I(i,j)}{10^{10}} \tag{3}$$

$$\begin{cases} x_0^{'} = x_0 + S \\ y_0^{'} = y_0 + S \\ Z_0^{'} = Z_0 + S \end{cases} \tag{4}$$

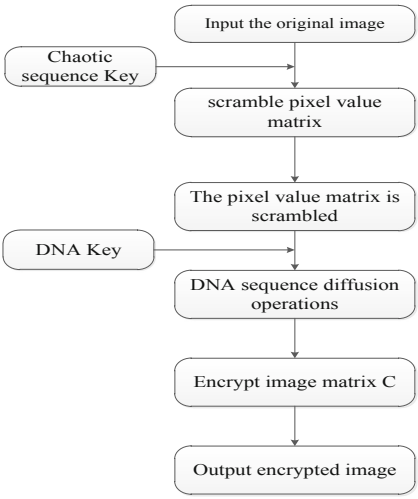


Fig. 4. The flow chart of algorithm

Step 2: Set $N = MAX(H, W)$, change the initial value of the chaotic system, and defer to Eq. (1), repeat iterative calculation $(m + N)$ times get the chaotic sequence. For good randomness of the chaotic sequence and the sensitivity of the initial value of the chaotic system, the data generated by the first m times of calculation is abandoned. Moreover, the times of row and column scrambling of image matrix in the scrambling part is determined by Eq. (5).

$$\begin{cases} Br = \mathrm{mod}((\lfloor |x_i| \rfloor) \times 10^{16}, \dfrac{W}{2}) \\ Bc = \mathrm{mod}((\lfloor |y_i| \rfloor) \times 10^{16}, \dfrac{H}{2}) \end{cases} \tag{5}$$

Step 3: The image matrix is introduced into the algorithm program, and the row and column of the matrix are scrambled respectively. First, the element of pixel matrix is shifted to the left, and the new row scrambling vector TK2 is obtained.

Step 4: Reconstruct the TK2 pixel value matrix with the size of $H \times M$ and start the column scrambling calculation. The detail as follow, the element of TK2 is move up, and get new column scrambling vector TK3. After reconstructing TK3, the scrambled image matrix TK is obtained.

Step 5: The scrambled image matrix is changed into binary numbers matrix, and the matrix size is $H \times 8 \times W$. On the ground of DNA coding rules, the numerical matrix is converted to form the DNA sequence matrix S1, which is $H \times 4 \times W$ in size.

Step 6: According to the initial value and system parameters of the chaotic system, a set of pseudo-random sequence numbers are generated after $(n + H \times W)$ calculation. The generation of the sequence follows the Eq. (6).

$$\begin{cases} k_1 = \mathrm{mod}((\lfloor |x_i| \rfloor) \times 10^{16}, 256) \\ k_2 = \mathrm{mod}((\lfloor |y_i| \rfloor) \times 10^{16}, 256) \\ k_3 = \mathrm{mod}((\lfloor |z_i| \rfloor) \times 10^{16}, 256) \end{cases} \tag{6}$$

Step 7: Use random number sequence matrix K1 to diffusion pixel value matrix S1. The specific process is basic on the principle of base complementary pairing, scrambling the original DNA combination of matrix S1, generate new DNA sequences. Then, according to the principle of DNA addition, combining the new DNA sequence and pseudo-random data matrix K1 and obtain the pixel value matrix C1 of the encrypted image.

Step 8: Recover matrix C1 and restore it to the pixel value matrix C represented by decimal number.

Step 9: Output the results. Therefore, the encrypted image is obtained. Complete the encryption process.

4.3 Decryption Algorithm Flow

In this paper, the decryption algorithm is the inverse process of the encryption algorithm. Firstly, in the decryption part, the receiver get the encrypted image, encodes the image matrix into DNA sequence, and use the 3D-SIMM discrete chaotic system to generate decode sequence. Use this sequence to reconstruct trademark image. In the process of scrambled restoration part, the undecrypted image matrix will be restored, and the original decrypted image matrix is restored to the decimal number pixel value matrix. The algorithm will obtain the final decrypted image. The specific decryption process is shown in Fig. 5.

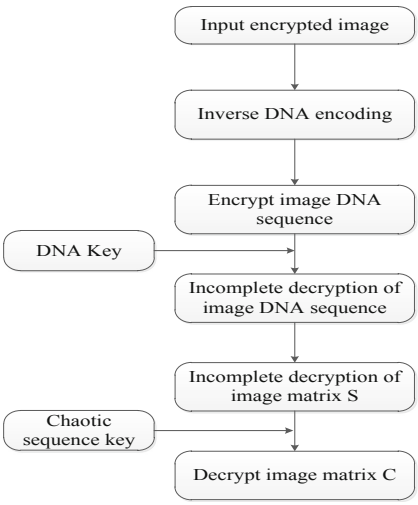


Fig. 5. The flow chart of algorithm

Step 1: Input the encrypted image, generate the image matrix of $H \times W$, and inversely encode the image matrix to generate the DNA sequence C1, the size of which is $H \times 4 \times W$.

Step 2: Generate pseudo random sequence as decryption key according to Eq. (1), and restore the DNA sequence of the encrypted image. In the process of reduction, get a new pixel diffusion sequence, and the new pixel diffusion sequence is combine with the decrypted pseudo random sequence according to the principle of base complementation and pairing. The incomplete DNA sequence S1 is obtained.

Step 3: Transform S1 into an $H \times M$ matrix and compile it into a binary image matrix TK. Then, the chaotic sequence generated by Eq. (1) can scramble TK.

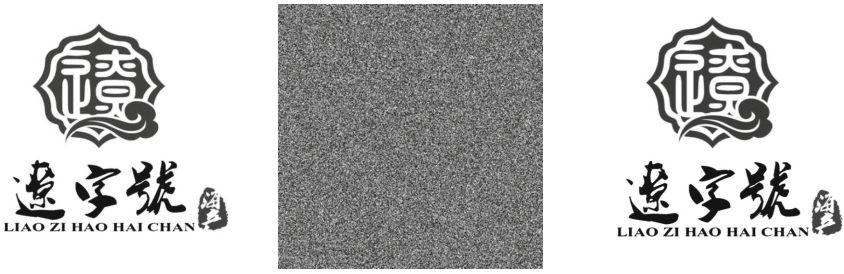
Step 4: Scramble the rows and columns of TK separately. The procedure is to move elements in TK down to generate the column scrambling vector TK3.

Step 5: Reconstruct TK3 into an $H \times M$ image matrix and start the row scrambling calculation. The process is to move a member of TK3 to the right and get a new row scrambling vector TK3. After reconstruction of TK3, the decrypted image matrix TK5 is obtained.

Step 6: Convert the decrypted image matrix to a decimal number image matrix and output the decrypted result. Complete the decryption process.

4.4 Simulation Results of the Algorithm

This paper takes the sea cucumber trademark of a certain brand in China as the encryption object, and the target image size is 512 × 512 pixels. in the key format, when $a = 1$, $b = 2\pi$, $c = 11.5$, $[x_0, y_0, z_0] = [0.3, 0.5, 0.6]$, $c_0 = \mathrm{C}$, $\alpha = 1$, $\beta = 3$. The encryption and decryption results are shown in Fig. 6.



(a)original image (b)Encryption image (c)Decryption image

Fig. 6. Simulation test results

5 Encryption Performance Analysis

5.1 Key Space Analysis

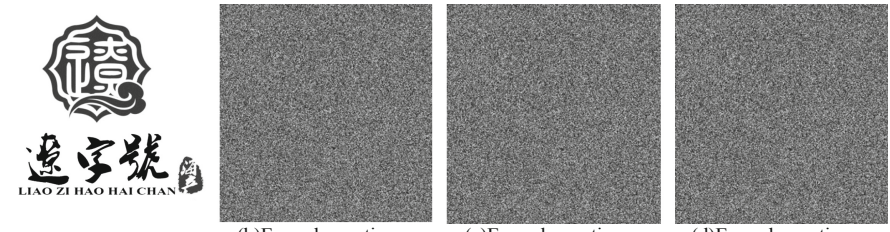
The key space involved in this algorithm should be large enough for resist brute force attack. When the computer computational accuracy is 10^{-15}, the key space size formed

by a, b, c and x_0, y_0, z_0 is 10^{90}, conversion to 2^{299}. Beside, c_0 represents four deoxynucleotides, α, β respectively represent six base pairs calculation rules, and L_i represents eight DNA coding rules used by the algorithm. The key space constituted by this part is $2^2 \times 2^6 \times 2^{20} = 2^{28}$. As a result, the key space of this algorithm can reach 2^{327}, with a large key space, as shown in Table 4, compared to other algorithm, the algorithm proposed in this study can effectively resist violence attack.

Scheme	Proposed	Ref. [21]	Ref. [19]	Ref. [20]
Key space	2^{327}	2^{319}	2^{90}	2^{78}

5.2 Key Sensitivity Analysis

In order to test the sensitivity of the algorithm to keys, the initial value will be change of 10^{-16}, and use new secret key to decrypted the encrypted image. The decryption results are shown in Fig. 7.



(a)Decryption image (b)Error decryption image ($x+10^{-16}$) (c)Error decryption image ($y+10^{-16}$) (d)Error decryption image ($z+10^{-16}$)

Fig. 7. Initial value sensitivity analysis

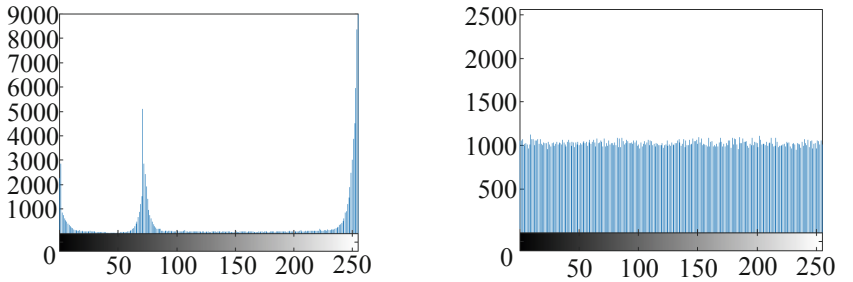
The results show that when the secret key is change, the algorithm cannot get the correct decrypted image. Hence, the algorithm has good sensitivity to initial value.

5.3 Statistical Performance Analysis

The statistical performance of the encrypted image is analyzed to measure the degree of confidentiality of the trademark image information of the algorithm designed in this paper.

5.3.1 Histogram Analysis

Histogram reflects the distribution of pixel values in the image, the abscissa reflects the gray value of the pixel, and the ordinate reflects the distribution of the pixel value in the image. According this, the histogram analysis results of pixel value distribution of trademark image and encrypted image are shown in Fig. 8.



(a) original picture histogram (b) encryption picture histogram

Fig. 8. Histogram analysis results

As shown in Fig. 8(b), the histogram of the encrypted image is a smooth histogram image, with pixel points distributed in different pixel value intervals, while as shown in Fig. 8(a), pixel values are relatively concentrated in different regions. Through comparison, it can be seen that the correlation between the encrypted image and the original image has been reduced, so that the encrypted image can effectively resist the histogram attack.

5.3.2 Image Correlation Coefficient Analysis

The image correlation coefficient is used to measure the correlation between adjacent pixels in different directions, and compare correlation coefficient between plaintext image and cipher image to prove algorithm has good security performance, The result obtained as following.

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(X)D(Y)}} \tag{7}$$

$$\mathrm{cov}(x, y) = E\{[x - E(x)][y - E(y)]\} \tag{8}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{9}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} [x_i - E(x)]^2 \tag{10}$$

Theoretically, due to the strong correlation between adjacent pixels, the cipher image correlation should be reduced than trademark picture and correlation coefficient of cipher image should close to 0. After simulation experiment, the correlation coefficient between the trademark image and the encrypted image are shown in Fig. 9.

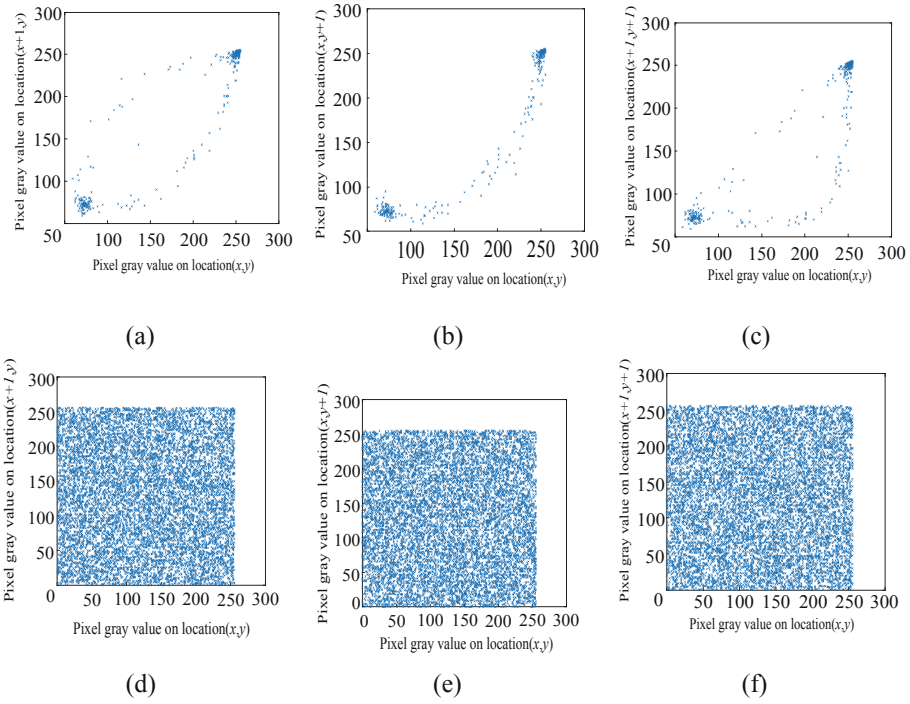


Fig. 9. The correlation coefficient analysis results

Table 5. Table of correlation coefficient

Direction	Original image	Encryption image
Horizontal	0.9653	−0.0051
Vertical	0.9602	−0.0030
Diagonal	0.9331	0.0004

As can be seen from Table 5, The correlation coefficient results show that in adjacent position, the original image has strong correlation and the distributed of pixel point is intensive, the encryption image has low correlation, almost close to 0 and the pixel point distribute all pixel area. As shown in Table 6, compared to other algorithm, the algorithm proposed in this research can effectively reduce the correlation with the original image. Therefore, the proposed scheme has good security performance.

Table 6. Table of correlation comparison

Scheme	Horizontal	Vertical	Diagonal
Proposed	−0.0051	−0.0030	0.0004
Ref. [22]	0.0036	0.0023	0.0039
Ref. [23]	−0.0048	−0.0112	−0.0045
Ref. [26]	−0.0066	−0.0089	0.0424

5.4 Information Entropy Analysis

Information entropy reflects the uncertainty of image information. Theoretically, the higher value of the entropy, the more uncertain the information and less visible the information. The calculation of information entropy is shown below.

For gray image L = 256, the theoretical value of information entropy is 8. Through calculation, the information entropy of the encrypted image is 7.9993, which is close to the theoretical value. As shown in Table 7 compared to other algorithm, the proposed algorithm can make the information in the encrypted image have great uncertainty.

Table 7. Table of information entropy

Scheme	Proposed	Ref. [7]	Ref. [22]	Ref. [23]
Entropy number	7.9993	7.9993	7.9980	7.9963

5.5 Differential Attack Analysis

NCPR and UACI were used to measure the performance of the algorithm to test the performance of the algorithm. The specific calculation method is shown as follows.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{L} \times 100\% \tag{11}$$

$$UACI = \frac{1}{L}\sum_{i,j} \frac{|C(i,j) - C_1(i,j)|}{256} \times 100\% \tag{12}$$

In this algorithm, the mean value of NCPR and UACI was calculated by repeated calculation for 10 times in the test of tolerance analysis performance. After calculation, the NCPR value was 99.63% and the UACI value was 33.41%. The technical index of this algorithm is close to the theoretical value. As shown in Table 8, between other algorithm, the proposed encryption can resist differential attack.

Table 8. Table of information entropy

Scheme	Proposed	Ref. [21]	Ref. [26]	Ref. [7]
NCPR	99.63%	99.62%	99.61%	99.60%
UACI	33.41%	33.06%	33.63%	33.47%

6 Conclusion

In this paper, an algorithm to encrypt the trademark image basic on 3D discrete chaotic map had designed. On the basic of 3D-SIMM map has good chaotic dynamic characteristics. Use this map to generate chaotic sequences have good randomness, and the encrypted image cannot be decrypted without a correct key. The performance analysis

shows that the encrypted image has a large entropy space and sensitivity to the initial value of the key. In conclude, this algorithm has good encryption characteristics, can effectively resist common attacks and protect the image information of trademarks, and is convenient for implementation and large-scale application. It provides effective guarantee for preventing trademark misappropriation and protecting the rights and interests of trademark owners.

References

1. Davison, M.: The legitimacy of plain packaging under international intellectual property law: why there is no right to use a trademark under either the paris convention or the trips agreement, pp. 81–108. Social Science Electronic Publishing (2012)
2. Biryukov, A., De Cannière, C.: Data Encryption Standard (DES). In: van Tilborg, H.C.A., Jajodia, S. (eds.) Encyclopedia of Cryptography and Security, vol. 28(2), pp. 295–301. Springer, Boston (2011). https://doi.org/10.1007/978-1-4419-5906-5
3. Singh, A., Marwaha, M., Singh, B., et al.: Comparative study of DES, 3DES, AES and RSA. Int. J. Comput. Technol. **9**(3), 97–102 (2013)
4. Ye, X.L., Mou, J., Luo, C.F., et al.: Dynamics analysis of Wien-bridge hyperchaotic memristive circuit system. Nonlinear Dyn. **92**(3), 923–933 (2018)
5. Ye, X.L., Wang, X.Y., Mou, J., et al.: Characteristic analysis of the fractional-order hyperchaotic memristive circuit based on the Wien bridge oscillator. Eur. Phys. J. Plus **133**(12), 516 (2018)
6. Liu, W., Sun, K., He, S.: SF-SIMM high-dimensional hyperchaotic map and its performance analysis. Nonlinear Dyn. **89**(4), 2521–2532 (2017)
7. Chai, X., Gan, Z., Lu, Y., et al.: A novel image encryption algorithm based on the chaotic system and DNA computing. Int. J. Mod. Phys. C **28**(05), 1 (2017)
8. Chen, J.X., Zhu, Z.L., Fu, C., et al.: A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism. Commun. Nonlinear Sci. Numer. Simul. **20**(3), 846–860 (2015)
9. Chai, X., Chen, Y., Broyde, L.: A novel chaos-based image encryption algorithm using DNA sequence operations. Opt. Lasers Eng. **88**(Complete), 197–213 (2017)
10. Norouzi, B., Seyedzadeh, S.M., Mirzakuchaki, S., et al.: A novel image encryption based on row-column, masking and main diffusion processes with hyper chaos. Multimed. Tools Appl. **74**(3), 781–811 (2015)
11. Luo, Y., Du, M., Liu, J.: A symmetrical image encryption scheme in wavelet and time domain. Commun. Nonlinear Sci. Numer. Simul. **20**(2), 447–460 (2015)
12. Aqeel-ur-Rehman, Liao, X., Hahsmi, M.A., et al.: An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using DNA and Chaos. Opt. Int. J. Light. Electron Opt. S0030402617311695 (2017)
13. Wei, X., Zhang, Q., Liu, L.: Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps. AEUE Int. J. Electron. Commun. **68**(3), 186–192 (2014)
14. Wang, X.Y., Gu, S.X., Zhang, Y.Q.: Novel image encryption algorithm based on cycle shift and chaotic system. Opt. Lasers Eng. **68**, 126–134 (2015)
15. Zhang, Y.: The image encryption algorithm based on chaos and DNA computing. Multimedia Tools Appl. **77**, 21589–21615 (2018)
16. Liu, W., Sun, K., He, Y., et al.: Color image encryption using three-dimensional sine ICMIC modulation map and DNA sequence operations. Int. J. Bifurc. Chaos **27**(11), 120511–121743 (2017)

17. Liu, W., Sun, K., Zhu, C.: A fast image encryption algorithm based on chaotic map. Opt. Lasers Eng. **84**, 26–36 (2016)
18. Huang, R., Rhee, K.H., Uchida, S.: A parallel image encryption method based on compressive sensing. Multimedia Tools Appl. **72**(1), 71–93 (2014)
19. George, S.N., Augustine, N., Pattathil, D.P.: Audio security through compressive sampling and cellular automata. Multimedia Tools Appl. **74**(23), 10393–10417 (2015)
20. George, S.N., Pattathil, D.P.: A secure LFSR based random measurement matrix for compressive sensing. Sens. Imaging **15**(1), 1–29 (2014)
21. Jain, A., Rajpal, N.: A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps. Multimedia Tools Appl. **75**(10), 5455–5472 (2016)
22. Zhang, Q., Guo, L., Wei, X.: Image encryption using DNA addition combining with chaotic maps. Math. Comput. Model. **52**(11–12), 2028–2035 (2010)
23. Belazi, A., El-Latif, A.A.A., Belghith, S.: A novel image encryption scheme based on substitution-permutation network and chaos. Signal Process. **128**, 155–170 (2016)
24. Wang, X., Wang, Q., Zhang, Y.: A fast image algorithm based on rows and columns switch. Nonlinear Dyn. **79**(2), 1141–1149 (2015)
25. Xingyuan, W.A.N.G., Teng, L.I.N., Qin, X.U.E.: A novel colour image encryption algorithm based on chaos. Signal Process. **92**(4), 1101–1108 (2012)
26. Zhongyun, H.U.A., et al.: 2D Sine Logistic modulation map for image encryption. Inf. Sci. **297**, 80–94 (2015)