Journal of Network Intelligence
Taiwan Ubiquitous Information
 ISSN 2414-8105 (Online)
Volume **5**, Number **1**, March **2020**

Research on Image Encryption Based on Hyperchaotic System

Xin Huang

Department of Electrical Engineering
Heilongjiang University
No.74 Xufu Road, Harbin, Heilongjiang, China
hx_enjoying@163.com

Matin Pirouz Nia

Computer Science Department
California State Univerity
2576 E. San Ramon,Fresno, CA 93740
mpirouz@csufresno.edu

Qun Ding*

Department of Electrical Engineering
Heilongjiang University
No.74 Xufu Road, Harbin, Heilongjiang, China
*Corresponding author: qunding@aliyun.com

Received Nov. 2018, Revised Oct. 2019

Abstract. *With the development of science and technology, the application of images is becoming more and more extensive, and the security issues they bring are also increasing. It is a difficult task for people to protect the security of image information. Based on the study of chaotic systems and various image encryption algorithms, this paper proposes a plaintext-associated image encryption algorithm based on the hyperchaotic Lorenz system. Since the initial value of the four-dimensional chaotic system is used as the key, the algorithm has a large enough key space to resist exhaustive attacks. In many classic cryptosystems, the key is the sole basis for generating encrypted images, that is, the generation of ciphertext images is controlled only by the keys and has nothing to do with the plaintext. Such image cryptosystems cannot effectively resist chosen plaintext attack or known plaintext attack. Therefore, this paper proposes a plaintext-related image encryption algorithm based on the hyperchaotic Lorenz system with positive significance. After the relevant test results show that the encryption algorithm has a faster encryption / decryption speed, high security and good encryption effect, can protect the image information security, and prevent information leakage.*
Keywords: Images, Hyperchaotic Lorenz system, Key, Plaintext-Related

1. **Introduction.** Since the intuitiveness of images is widely used, it also brings hidden dangers of information security leakage, which not only involves personal privacy issues, but also has a negative impact on society. Therefore, the proposed image encryption technology has positive significance [1–6]. In 1989, R. Matthews based on Logistic mapping research proposed a generalized Logistic map, and used this map to generate a large number of pseudo-random numbers for data encryption [7]. Since chaotic systems have the characteristics of dependence, ergodicity and randomness which are extremely sensitive to initial conditions and control parameters, more and more chaotic-based image encryption

algorithms are proposed. Image encryption schemes are based on chaotic systems [8, 9], DNA encoding [10–20], compressed sensing [21], grayscale encoding [22], and bit-level permutation [23–25] . An image encryption algorithm based on seven-dimensional (7D) hyperchaotic system and simultaneous row-column exchange is proposed [1]. The parameters and initial values of the 7D hyperchaotic system are generated by SHA-512 hash function. A two-dimensional encryption operation image encryption scheme based on chaos and plaintext is proposed [2]. The block parity performed in the first round of encryption is used to associate the plaintext information with the key, thereby enabling the encryption scheme to defend against plaintext attacks. Repetitive coding is employed in the second round of encryption to protect plaintext related parameters from noise and data loss attacks. A block scrambling-based encryption scheme is proposed, which uses JPEG compression to enhance the security of the encryption-compression (EtC) system [3]. A new logic tent mapping algorithm is proposed, which introduces a parameter related to the SHA-3 hash value of the plaintext image as the key parameter [4]. The algorithm can resist the choice of plaintext attack. A combined chaotic system is defined by Logistic system, Sine system and Tent system, and a color image encryption algorithm based on chaotic system is proposed [26]. A two-dimensional (2D) logic-sinusoidal coupling mapping (LSCM) is proposed [27]. Based on the proposed 2D-LSCM, a 2D-LSCM based image encryption algorithm (LSCM-IEA) is proposed. The permutation algorithm of the algorithm replaces the image pixels with different rows and columns. The diffusion algorithm spreads a small amount of the original image to the entire encryption result. In the work of [28], based on the analysis of the security of pure CTM scheme, combined with the rectangular transformation and CTM principle, a new image encryption algorithm is proposed. The sensitivity of the key is further improved by generating a key stream associated with the key and the normal image. A method for constructing a simple and effective chaotic system using the difference between two identical one-dimensional chaotic map output sequences is introduced [29]. In the work of [30], an image encryption scheme based on memory hyperchaotic system, cellular automata (CA) and DNA sequence operation is proposed, which consists of a diffusion process. This paper proposes an image encryption algorithm based on plaintext correlation based on hyperchaotic system. First, the image scrambling algorithm is studied and a plaintext correlation scrambling algorithm is proposed. The algorithm is used twice with the addition modulus diffusion algorithm to make the plaintext information be completely hidden. After the image information is diffused, scrambled and then diffused, an encrypted image with good encryption effect is finally obtained.

2. **Chaotic sequence generator.**

2.1. **Hyperchaotic Lorenz system.**

Adding a nonlinear controller to the three-dimensional Lorenz chaotic system, which extends the three-dimensional Lorenz system to four dimensions. The system equation is:

$$\begin{cases} \dot{x} = a(y - x) + \omega \\ \dot{y} = cx - zx - y \\ \dot{z} = xy - bz \\ \dot{\omega} = -yz + r\omega \end{cases} \tag{1}$$

where a, b, c, r are the real parameters restricted in a certain variable region, x, y, z, ω are the variables of the equation. When $a = 10$, $b = 28$, $c = 8/3$, $-1.52 \leq r \leq -0.006$, equation (1) is in a hyperchaotic state. Without loss of generality, when the initial value

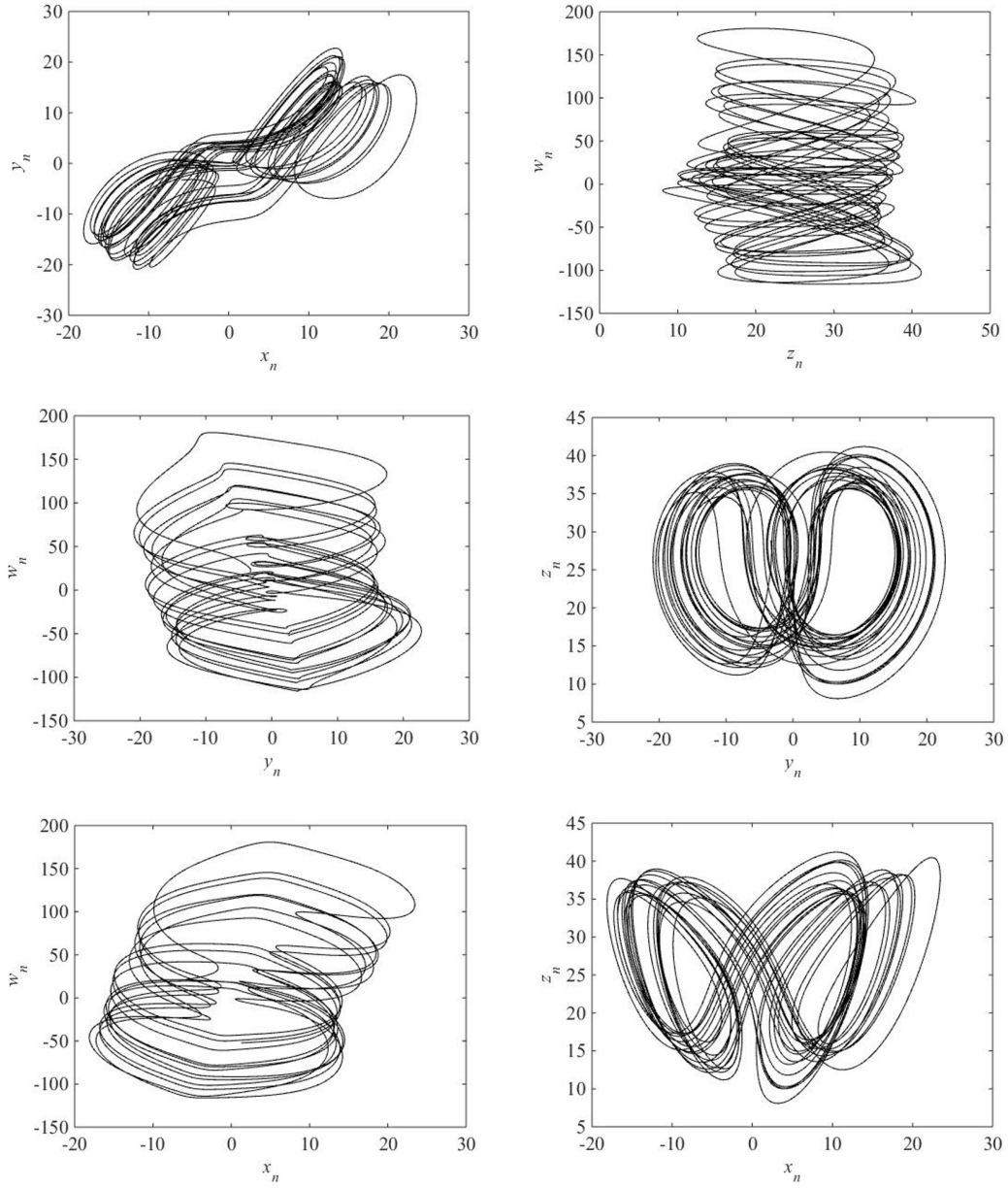


FIGURE 1. Attractor phase diagram of hyper chaotic system

is set as (1.1, 2.2, 3.3, 4.4), the phase diagram of equation (1) is shown in figure 1 when the system parameter $r = -1$.

Under this parameter, the four Lyapunov exponent of the system are: 0.343111, 0.163088, 0.002345, and -15.187859, two of them are greater than 0, in that the system is also called a hyperchaotic system. As shown as figure 2.

2.2. **Generation of random matrices.** The state value of the chaotic system is a floating point type, which is not directly used in a digital image encryption system. If the gray level is R, the chaotic state value needs to be converted into an integer type of $0 \sim R - 1$. In this essay, Lorenz system of hyperchaotic system is used as a sequence generator to generate four random matrices of the same size as plaintext. Let P be the plaintext image that represents the input, and the size is $M \times N$, When $L = \max(M, N)$. Put x_0, y_0, z_0, w_0 to the equation (1), the iteration step length is 0.0001. Four vectors

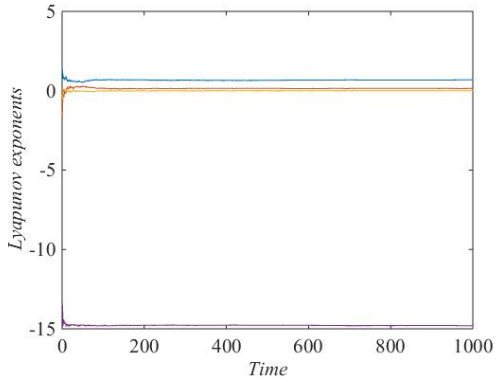


FIGURE 2. Lyapunov exponent of the hyperchaotic Lorenz system

$\{x_0, y_0, z_0, w_0\}$ of length $M \times N$ are obtained without the transition state, four matrices of size $M \times N$ are generated by using these four vectors K_1, K_2, K_3 and K_4 , so that:

$$K_1(i,j) = \text{floor}\left(\left(x_{(i-1)\times N+j} + y_{(i-1)\times N+j} + r1 + 100 \bmod 1\right) \times 10^{13}\right) \bmod R \quad (2)$$

$$K_2(i,j) = \text{floor}\left(\left(y_{(i-1)\times N+j} + z_{(i-1)\times N+j} + r2 + 100 \bmod 1\right) \times 10^{13}\right) \bmod R \quad (3)$$

$$K_3(i,j) = \text{floor}\left(\left(z_{(i-1)\times N+j} + \omega_{(i-1)\times N+j} + r3 + 100 \bmod 1\right) \times 10^{13}\right) \bmod L \quad (4)$$

$$K_3(i,j) = \text{floor}\left(\left(\omega_{(i-1)\times N+j} + x_{(i-1)\times N+j} + r4 + 100 \bmod 1\right) \times 10^{13}\right) \bmod L \quad (5)$$

The calculated matrix K_1 is used for forward diffusion, K_1 is used for reverse diffusion, K_3 and K_4 are used for scrambling modules. The initial values r_1, r_2, r_3, r_4 of the chaotic system are 8-bit random integers with a value range of $[0, 255]$.

3. Plaintext-related image scrambling and diffusion algorithm.

3.1. Plaintext-related image scrambling.

The image is determined by the size of the pixel and the position of the pixel. Scrambling is the change of the pixel order of the original image. For example, the positions of two pixels P_A, P_B in the image are $(x, y)$and (δ, ξ), and the two pixel positions are exchanged, that is, the position of P_A is (δ, ξ), P_B is (x, y) are changed. The position of the pixels can be changed to achieve the effect of encryption, and δ and ξ are the changes according to certain rules, as follows:

$$\delta = \left(\sum_{j=1}^{M} P(x,j) - P(x,y)) + K_3(x,y) + 1\right) \bmod M \quad (6)$$

$$\xi = \left(\sum_{i=1}^{N} P(i,y) - P(x,y)) + K_4(x,y) + 1\right) \bmod N \quad (7)$$

where $i = 1, 2, \cdots, M$ $j = 1, 2, \cdots, N$. With the above operation to enhance the association plain text

3.2. Diffusion algorithm.

The diffusion algorithm is to hide the pixel information of the plain text image in as many ciphertext pixels as possible without changing the pixel position of the original image. Commonly used diffusion algorithms include XOR operation, GF domain addition operation, GF domain multiplication operation and modulus operation. Based on the exclusive OR operation, the diffusion algorithm of the addition mode operation is a commonly used algorithm in image encryption. The latter runs much faster in Matlab than the former, which is due to the weak bit manipulation capabilities

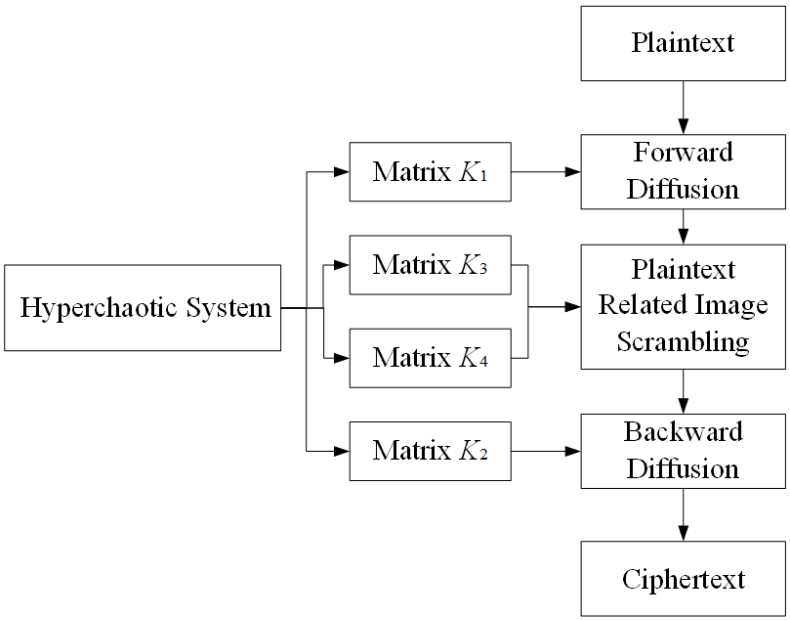


FIGURE 3. Encryption algorithm structure diagram

of Matlab software. $P(i)$ and $C(i)$ can be used to represent the original image and the encrypted image. The pixel $K(i)$ and is a cipher pixel. The formula is:

$$C\left(i\right)=\left(P\left(i\right)+K\left(i\right)\right) \bmod 256 \tag{8}$$

In order to diffuse the information of any pixel in the plaintext into the entire image of the ciphertext, this method needs to be cycled twice.

4. Design and results of image encryption.

4.1. Design of image encryption.

The plaintext image scrambling algorithm is mainly composed of a plaintext independent forward module, a plaintext independent backward module, a plaintext related scrambling module, and a chaotic sequence generation module. Its structure is shown in Figure 3.Specific steps are as follows:

Step1: Let P be the plaintext image that represents the input, and the size is $M \times N$, When $L=\max(M,N)$.

Step2: The key is represented by k , $k=\{x_0,y_0,z_0,w_0,r_1,r_2,r_3,r_4\}$, here x_0,y_0,z_0,w_0 are the initial values and r_1,r_2,r_3,r_4 of the chaotic system are 8-bit random integers whose value interval is $[0,255]$ .Generates four matrices according to the formula 2,3,4,5.

Step3:The matrices P, K_1, K_2 are transformed from two dimensions to a one-dimensional matrix of length $M \times N$, which are represented by O, E_1 and E_2respectively.

Step4:The first round of diffusion replaces the encryption formula respectively by

$$C_{(0)}=\left(O_{(0)}+E_{1(0)}+r_1+r_2\right) \bmod 256 \tag{9}$$

$$C_{(l)}=\left(O_{(l)}+E_{1(l)}+C_{(l-1)}\right) \bmod 256 \tag{10}$$

Where r_1 and r_2 are the constant parameters referenced for encryption, they are also keys, $l=1,2,\cdots,L-1$

Step5:Let pixel $C_{(l)}$ and $C_{(m+n)}$ switch their positions, here are the computational formulas about m and n ,$l=0,2,\cdots,L-1$.

$$\delta=\left(\sum_{j=1}^{M}K_3(x,j)-K_3(x,y))+C_l+1\right) \bmod M \tag{11}$$

$$\xi = \left(\sum_{i=1}^{N} K_4(i,y) - K_4(x,y)) + C_l + 1 \right) \bmod N \tag{12}$$

Finally, we get the scrambling matrix D from matrix C.

Step6:The second round of diffusion instead of the adjoint formula is respectively derived from

$$F_{(L)} = \left(E_{2(L)} + D_{(L)} + r_3 + r_4 \right) \bmod 256 \tag{13}$$

$$F_{(l)} = \left(E_{2(l)} + D_{(l)} + F_{(l+1)} \right) \bmod 256 \tag{14}$$

It means, here r_3 and r_4 are the constant parameters referenced for encryption, they are also keys. The matrix F is the ciphertext image after the calculations above. The decryption process is the inverse process mentioned above. From the above formula, it can be seen that the relationship between ciphertext and ciphertext and key is not a simple linear operation but includes nonlinear module extraction.Therefore, the algorithm can resist the selective plaintext attack.

4.2. **The results of image encryption.** According to the improved encryption algorithm in the previous section, choose three gray scale Lena, Pepper, Baboon whose size are 512×512 to do encrypting processing, encryption after decryption results with the same method, results of encryption and decryption is shown in Figure 4:

According to the encryption results, it can be seen that the encrypted image is no longer recognizable to the original image, and the decrypted restored image is exactly the same as the plaintext image.

5. Security analyses and experimental results.

5.1. **Encryption and decryption time.** Without losing generality, the key is taken as $k = 0.7512, 0.4567, 0.7878, 0.9872, 782, 89, 26$.

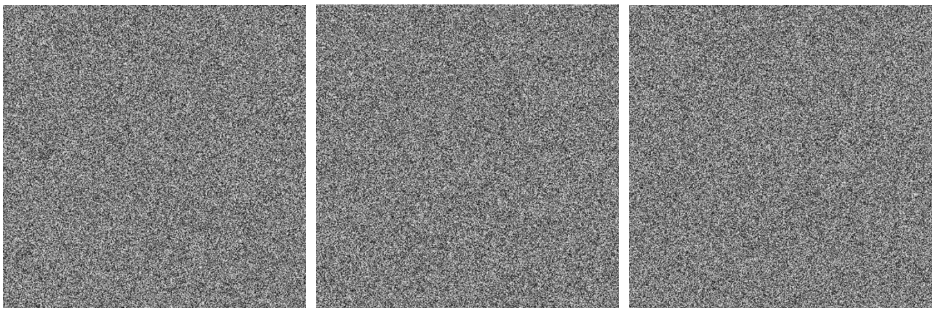
Table 1. The encryption and decryption time

Encryption time	Decryption time
1.5665	1.6156

5.2. **Key space.** The key space is the set of all legitimate keys. For the digital image encryption system proposed in this paper, the key is the initial value of the hyperchaotic Lorenz system and eight-bit random numbers, which are included as follows:$K = \{x_0, y_0, z_0, w_0, r_1, r_2, r_3, r_4\}$, among these numbers, $x_0 \in (-40, 40)$, $y_0 \in (-40, 40)$, $z_0 \in (1, 81)$, $\omega_0 \in (-250, 250)$, and the pace of x_0 , y_0 and z_0 is 10^{-13} ,the pace of ω_0 is 10^{-12},and r_1, r_2, r_3, r_4 are 4 eight-bit random integers, the value interval of which is $[0, 255]$,and the compensation is 1, so the key space size is 1.0995×10^{69} , and the key entropy is about 229b.

5.3. **Statistical characteristics of ciphertext.** This paper will be used to encrypt plaintext images into noisy pattern ciphertext images based on hyperchaotic Lorenz system . Also there is a figure which comparing the histogram and correlation characteristics between plaintext and its corresponding ciphertext image. As shown in Figure 5. Without losing the generality, the key is taken as k=$\{0.7512, 0.4567, 0.7878, 0.9872, 782, 89, 26\}$. As shown in Figure 5, the image of the ciphertext has a flat histogram while the histogram of the plaintext is up and down. We often use χ^2 Statistics (unilateral test hypothesis) to measure the difference in quantity. The commonly used level of significance is 0.05, and

(a) Lena original data (b) Pepper original data (c) Baboon original data



(d) Lena ciphertext (e) Pepper ciphertext (f) Baboon ciphertext

(g) Decrypted the Lena image (h) Decrypted the Pepper image (i) Decrypted the baboon image

FIGURE 4. Plaintext association algorithm encryption and decryption results

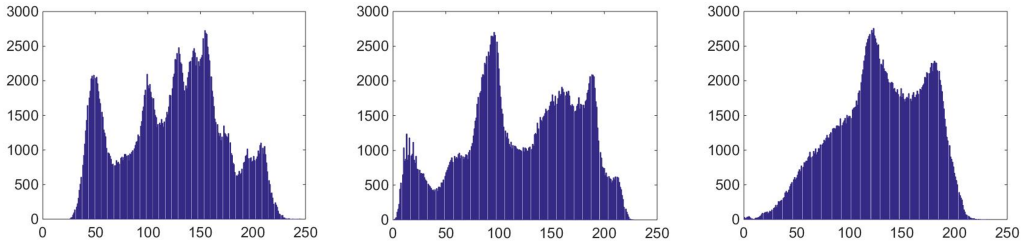
TABLE 2. χ^2test results

image	Lena	Pepper	Baboon
Plaintext	1.5806×10^5	1.2014×10^5	1.8739×10^5
Ciphertext	248.1719	258.4961	255.7285

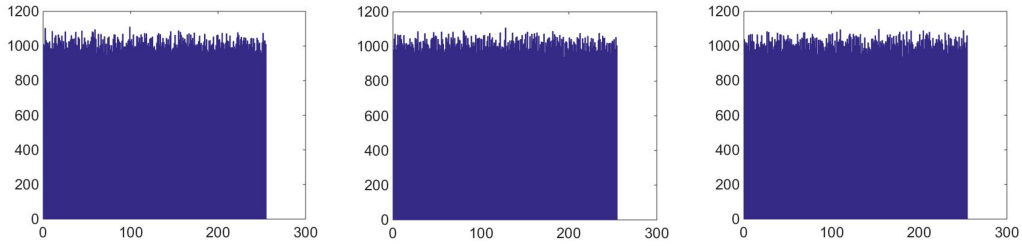
the χ^2 test is performed on the histogram of the image shown in Figure 5, and the χ^2 test results are shown in the Table 2 .

It is known from Table 2 that the calculated values of the χ^2 statistics of plaintext images are obviously greater than $\chi^2_{0.01}(255)$, while the calculated value of the ciphertext's χ^2 statistics is less than $\chi^2_{0.01}(255)$, and the 3 ciphertext can be considered to be approximately uniform.

In addition to image histogram, we need to compare the correlation properties between plaintext and ciphertext images. Generally, the plaintext image has strong correlation between adjacent pixels in horizontal, vertical, positive diagonal direction and Anti angular



(a) Lena plaintext histogram (b) Pepper plaintext histogram (c) Baboon plaintext histogram



(d) Lena ciphertext histogram (e) Pepper ciphertext histogram (f) Baboon ciphertext histogram

FIGURE 5. Histogram of images

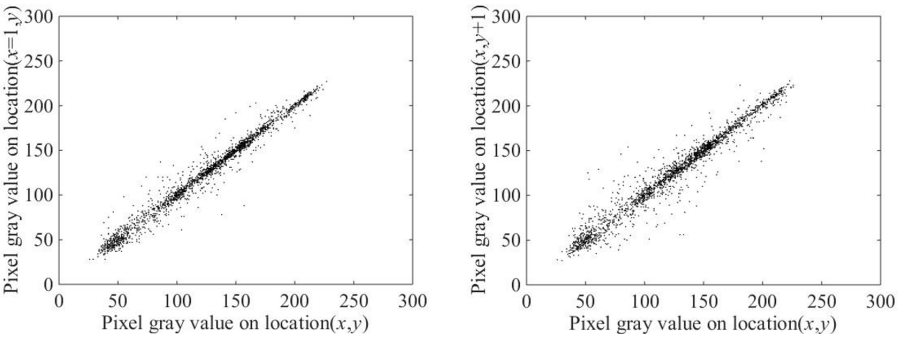
direction, and there should be no correlation between the adjacent pixels in the ciphertext image. Table 3 is the statistical result of correlation coefficient between plaintext and ciphertext.

TABLE 3. Correlation coefficient of plaintext and ciphertext

Image		**Horizontal**	**Vertical**	**Diagonal**
Lena	Plaintext	0.984930	0.971415	0.9590889
	ciphertext	-0.004204	0.0038422	-0.010919
Pepper	Plaintext	0.978633	0.9803303	0.966881
	ciphertext	-0.002301	0.017459	-0.002470
Baboon	Plaintext	0.768000	0.863453	0.722173
	ciphertext	-0.003464	0.014699	0.008106

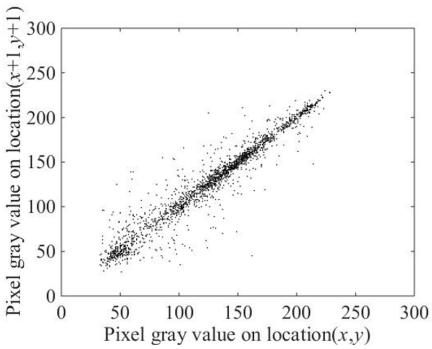
From table 3, we can see that the correlation between adjacent pixels in the plaintext image is very large, and the correlation of adjacent points in the ciphertext image is close to 0, which is almost irrelevant. Figure 6 shows the correlation between plaintext and ciphertext of Lena image in all directions.

5.3.1. *Sensitivities of plaintext.* Plaintext sensitivity analysis means that the encryption system uses the same key to encrypt two original images with little difference. If the two ciphertext images obtained are very different, the plaintext sensitivity of the encryption system is very strong. If the calculation result is very close to the theoretical value, the plaintext sensitivity is very strong. The ciphertext sensitivity analysis is similar to the plaintext sensitivity analysis. The ciphertext image is decrypted after minor changes, and the difference between the decrypted image and the original image is compared. If the differences are very different, it indicates that the encryption system has strong ciphertext sensitivity. Both are verified by calculating the values of NPCR, UACI, and BACI. Suppose that the pixels of the two original images at (i, j) are different,

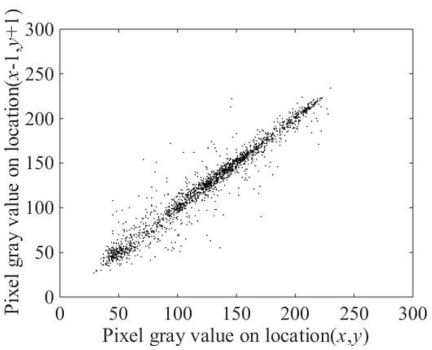


(a) Horizontal direction

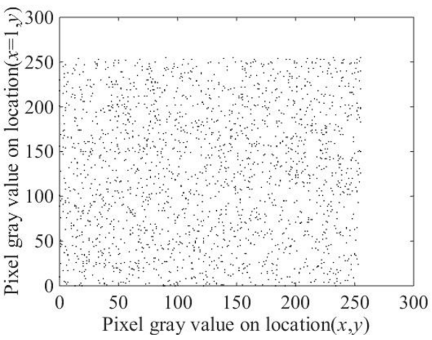
(b) Vertical direction



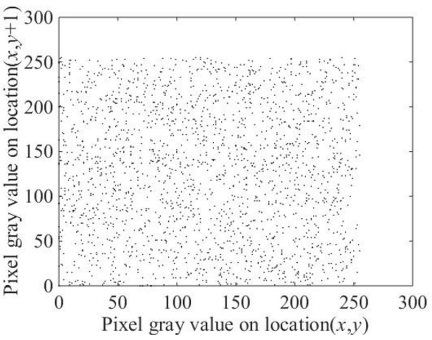
(c) Positive diagonal direction



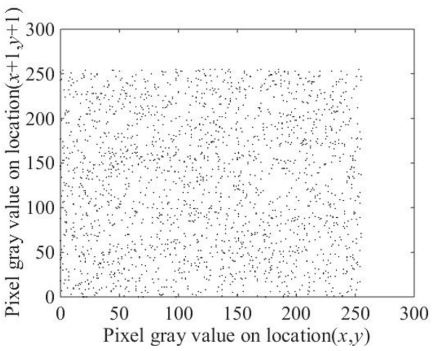
(d) Anti angular direction



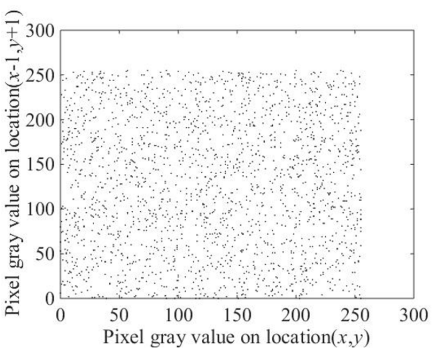
(e) Horizontal direction



(f) Vertical direction



(g) Positive diagonal direction



(h) Anti angular direction

FIGURE 6. The correlation between plaintext and ciphertext of Lena image in all directions.

respectively$P_1(i,j)$and$P_2(i,j)$, then the calculation formulas of NPCR, UACI, and BACI

are:

$$NPCR = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|Sign\left(P_1\left(i,j\right)+P_2\left(i,j\right)\right)\right| \times 100\% \tag{15}$$

$$Sign\left(x\right) = \begin{cases} 1, x > 0 \\ 0, x = 0 \\ -1, x < 0 \end{cases} \tag{16}$$

$$UACI = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{\left|P_1\left(i,j\right)-P_2\left(i,j\right)\right|}{255} \times 100\% \tag{17}$$

$$BACI = \frac{1}{\left(M-1\right)\left(N-1\right)}\sum_{i=1}^{(M-1)(N-1)}\frac{m_i}{255} \times 100\% \tag{18}$$

The average values of NPCR, UACI and BACI obtained through 50 repeated experiments are shown in Table 4 and Table 5.

Table 4. Plaintext sensitivity

	Lena	**Pepper**	**Baboon**	**Theoretical value**
NPCR	99.6104	99.6099	99.6100	99.6094
UACI	33.4587	33.4653	33.4642	33.4635
BACI	26.7255	26.7258	26.7874	26.7712

Table 5. Plaintext sensitivity

	Lena	**Theoretical value**	**Pepper**	**Theoretical value**	**Baboon**	**Theoretical value**
NPCR	99.6121	99.6094	99.6123	99.6094	99.6099	99.6094
UACI	28.6429	28.6239	29.6286	29.6233	27.8174	27.8478
BACI	21.3233	21.3217	22.1791	22.1894	20.6252	20.6312

5.4. **Information entropy.** Information entropy reflects the uncertainty of image information. Generally speaking, the greater the entropy, the greater the uncertainty (the greater the amount of information), the less visible information. The formula of the information entropy is shown in formula (19):

$$H = -\sum_{i=0}^{L} p(i)\log_2 p(i) \tag{19}$$

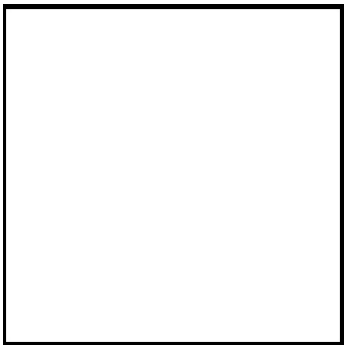
Here L is the gray level of the image, $p(i)$ indicates the probability of the gray value i .

For gray random images of $L = 256$, the theoretical value of information entropy H is 8.The information entropy of plaintext images Lena, Pepper and Baboon and their corresponding ciphertext images is listed in Table 6.

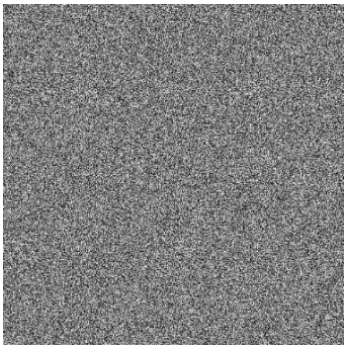
TABLE 6. Information entropy

Image	Lena	Pepper	Baboon
Plaintext	7.445 513	7.593 374	7.358 538
Ciphertext	7.999 303	7.999 335	7.999 328

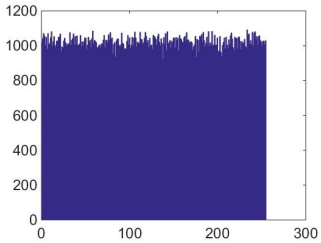
5.5. **Known plaintext attack and chosen plaintext attack.** A good encryption system can effectively resist known plaintext attacks. As shown in Figure 6, the attacker selects two images of all white and all black, which are 512×512, to encrypt, and the encrypted image is confused, and the histogram is balanced. It can be seen from the Table 7 that the information entropy of the ciphertext image obtained after encryption is close to 8, so it can be inferred that the system can resist the known plaintext attack and the chosen-plaintext attack.



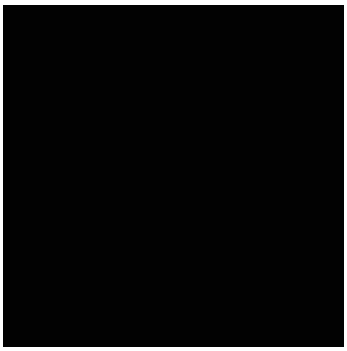
(a) An all-white image



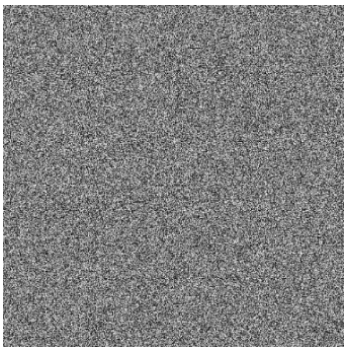
(b) The ciphertext obtained by encrypting the all-white image



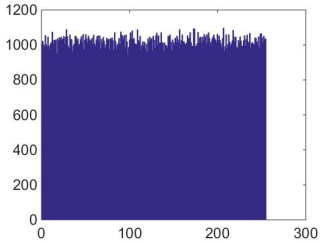
(c) The statistical histogram of the ciphertext image



(d) An all-black image



(e) The ciphertext obtained by encrypting the all-black image



(f) The ciphertext obtained by encrypting the all-black image

FIGURE 7. Known plaintext attack and chosen plaintext attack

TABLE 7. Known plaintext attack and chosen plaintext attack

Image	Entropies	Horizontal	Vertical	Diagonal
All white	0	NaN	NaN	NaN
Cipher of all white	7.999332	0.017797	0.003019	0.050719
All black	0	NaN	NaN	NaN
Cipher of all black	7.999419	-0.023741	-0.020398	0.010108

5.6. **Compare with other systems.** The size is 256 × 256 Lena encryption and other system performance were compared as shown in the Table 8, the correlation between the ciphertext between, this systems is relatively good, relatively close to 0, in the comparison of information entropy in the ciphertext, and this algorithm is more close to 8. By comparing the values of NPCR and UACI, the algorithm has high sensitivity to plaintext and can also resist known plaintext attacks and chosen plaintext attacks. Therefore, the performance of our scheme has better image than the other scheme of encryption scheme.

TABLE 8. Compare with other systems

Image	Horizontal	Vertical	Diagonal	Entropies	NPCR	UACI
Ours	0.00673	-0.0037	0.0060	99.6077	33.4465	7.9975
Ref.[11]	-0.0015	-0.0032	0.0008	99.61	33.46	7.9972
Ref.[23]	0.0068	-0.0054	0.0010	99.61	33.46	7.9967
Ref.[33]	-0.0029	-0.0017	-0.0191	99.5986	33.4561	7.9971

6. **Conclusion.** An effective image encryption algorithm is proposed, which is based on the plain-text correlation encryption algorithm of hyperchaotic system functions. In order to resist the known plaintext attack and the chosen plaintext attack, the plaintext-related image scrambling is carried out. Finally, the final encryption effect is achieved through the use of matrix generated by chaotic sequence. This paper also analyzes the effect of encryption, it can be found that the algorithm can well resist the brute force attack, and chosen plaintext attack which verifies the security and effectiveness of the algorithm..

REFERENCES

[1] S. L. Sun, Y. N. Guo, R. K. Wu, A Novel Image Encryption Scheme Based on 7D Hyperchaotic System and Row-column Simultaneous Swapping, *IEEE Access*, vol. 7, pp. 28539-28547, 2019.

[2] S. Ma, Y. Zhang, Z. G. Yang, et al, A New Plaintext Related Image Encryption Scheme Based on Chaotic Sequence,*IEEE Access*, vol. 7, pp. 30344-30360, 2019.

[3] T. Chuman, W. Sirichotedumrong, H. Kiya, Encryption Then Compression Systems Using Grayscale Based Image Encryption for JPEG Images,*IEEE Transactions on Information Forensics and Security*, vol. 14, no. 6, pp. 1515-1525, 2019.

[4] C. X. Zhu, K. H. Sun,Cryptanalyzing and Improving a Novel Color Image Encryption Algorithm Using RTEnhanced Chaotic Tent Maps,*IEEE Access*, vol. 6, pp. 18759-18770, 2018.

[5] W. P.Wang, X.Wang, X.Luo, et al,Finite-Time Projective Synchronization of Memristor-Based BAM Neural Networks and Applications in Image Encryption,*IEEE Access*, vol. 6, pp. 56457-56476, 2018.

[6] N. A.Loan,N. N.Hurrah, S. A.Parah,et al, Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption, *IEEE Access* ,vol. 6, pp. 19876-19897, 2018.

[7] X. Q. Fu, B. C. Liu, Y. Y. Xie,et al, Image EncryptionThenTransmission Using DNA Encryption Algorithm and The Double Chaos, *IEEE Photonics Journal*, vol. 10, no. 3, pp. 1-15, 2018.

[8] R. S. Lan, J. W. He, S. H. Wang, et al, Integrated chaotic systems for image encryption, *Signal Processing*, vol. 147, pp. 133-145, 2018.

[9] Y. Q. Zhang, X. Y. Wang, A symmetric image encryption algorithm based on mixed linear-nonlinear coupled map lattice, *Information Sciences*, vol. 273, pp. 329-351, 2014.

[10] X. L. Chai, X. L. Fu, Z. H. Gan, et al, A color image cryptosystem based on dynamic DNA encryption and chaos, *Signal Processing*, vol. 155, pp. 44-62, 2019.

[11] S. L. Sun, A Novel Hyperchaotic Image Encryption Scheme Based on DNA Encoding, Pixel-Level Scrambling and Bit-Level Scrambling, *IEEE Photonics Journal*, vol. 10, no.2, pp. 1-14, 2018.

[12] S. L. Sun, Chaotic image encryption scheme using two-by-two deoxyribonucleic acid complementary rules, *Optical Engineering*, vol. 56, no.11, 2017.

[13] T. Hu, Y. Liu, L. H. Gong, et al, Chaotic image cryptosystem using DNA deletion and DNA insertion, *Signal Processing*, vol. 134, pp. 234-243, 2017.

[14] X. L. Chai, Y. R. Chen, L. Broyde, A novel chaos-based image encryption algorithm using DNA sequence operations, *Optics and Lasers in Engineering*, vol. 88, pp. 197-213, 2017.
[15] X. Y. Wang, H. L. Zhang, X. M. Bao, Color image encryption scheme using CML and DNA sequence operations, *Biosystems*, vol. 144, pp. 18-26, 2016.
[16] X. Y. Wang, Y. Q. Zhang, X. M. Bao, A novel chaotic image encryption scheme using DNA sequence operations, *Optics and Lasers in Engineering*, vol. 73, pp. 53-61, 2015.
[17] Kalpana, J.,Murali, P., An improved color image encryption based on multiple DNA sequence operations with DNA synthetic image and chaos, *Optik*, vol. 126, no.24, pp. 5703-5709, 2015.
[18] Y. S. Zhang, W. Y. Wen, M. T. Su, et al, Cryptanalyzing a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system, *Optik*, vol. 125, no.4, pp. 1562-1564, 2014.
[19] Q. Zhang, X. P. Wei, A novel couple images encryption algorithm based on DNA subsequence operation and chaotic system, *Optik*, vol. 124, no.23, pp. 6276-6281, 2013.
[20] X. P. Wei, L. Guo, Q. Zhang, et al, A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system, *Journal of Systems and Software*, vol. 85, no.2, pp. 290-299, 2012.
[21] H. Huang, X. He, Y. Xiang, et al, A compression-diffusion-permutation strategy for securing image, *Signal Processing*, vol. 150, pp. 183-190, 2018.
[22] P. Ping, J. Y. Fan, Y. C. Mao, et al, A Chaos Based Image Encryption Scheme Using Digit-Level Permutation and Block Diffusion, *IEEE Access*, vol. 6, pp. 67581-67593, 2018.
[23] Y. P. Li, C. H. Wang, H. Chen, A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation, *Optics and Lasers in Engineering*, vol. 90, pp. 238-246, 2017.
[24] W. Zhang, H. Yu, Y. L. Zhao, et al, Image encryption based on three-dimensional bit matrix permutation, *Signal Processing*, vol. 118, pp. 36-50, 2016.
[25] Y. Q. Zhang, X. Y. Wang, A new image encryption algorithm based on non-adjacent coupled map lattices, *Applied Soft Computing*, vol. 26, pp. 10-20, 2015.
[26] Parvaz, R., Zarebnia, M., A combination chaotic system and application in color image encryption, *Optics & Laser Technology*, vol. 101, pp. 30-41, 2018.
[27] Z. Y. Hua, F. Jin, B. X. Xu, et al, 2D Logistic-Sine-coupling map for image encryption, *Signal Processing*, vol. 149, pp. 148-161, 2018.
[28] X. L. Wu, B. Zhu, Y. T. Hu, et al, A novel colour image encryption scheme using rectangular transform-enhanced chaotic tent maps, *IEEE Access*, pp. 1-1, 2017.
[29] Pak, C., L. L. Huang, A new color image encryption using combination of the 1D chaotic map, *Signal Processing*, vol. 138, pp. 129-137, 2017.
[30] X. L. Chai, Z. H. Gan, K. Yang, et al, An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations, *Signal Processing: Image Communication*, vol. 52, pp. 6-19, 2017.
[31] C. Y. Song, Y. L. Qiao, A Novel Image Encryption Algorithm Based on DNA Encoding and Spatiotemporal Chaos, *Entropy*, vol. 17, no.12, pp. 6954-6968, 2015.
[32] G.H. Xu, Shekofteh, Y., Akgul, A., C. B. Li, Panahi, S., A New Chaotic System with a Self-Excited Attractor:Entropy Measurement, Signal Encryption, and Parameter Estimation, *Entropy*, vol. 20, pp. 86, 2018.
[33] X. Y. Wang, X. Q. Zhu, Y. Q. Zhang, An Image Encryption Algorithm Based on Josephus Traversing and Mixed Chaotic Map, *IEEE Access*, vol. 6, pp. 23733-23746, 2018.