PROCEEDINGS OF SCIENCE

A Novel Hyper Chaos-based Image Encryption Algorithm Using Dynamic DNA Coding and SHA-256

Shuqin Zhu[1]
School of Computer Science; Liaocheng University
Liaocheng, 252000, China
E-mail: shuqinzhu2008@163.com

Wenhong Wang
School of Computer Science; Liaocheng University
Liaocheng, 252000, China
E-mail: wangwenhong@lcu-cs.com

Chaolei Ban
School of materials science and engineering; Liaocheng University
Liaocheng, 252000, China
E-mail: banchaolei@163.com

This paper presents a new hyper chaos-based image encryption algorithm which makes use of dynamic DNA coding and SHA-256. Different DNA encoding rules are adopted for different pixels, according to a random matrix generated by a five-dimension hyper-chaotic system with the initial value related to the SHA-256 hash value of the plaintext image. Since the initial values of the five-dimension hyper-chaos system are related to the hash value of the explicit image, the five-dimension hyper-chaos system generates distinct key streams per plaintext image, even for the same initial conditions of the chaos system. Therefore, the new encryption algorithm can withstand the chosen-plaintext attacks. Moreover, the dynamic encoding technology enhances the security of the ciphertext image. The result of this experiment and relevant safety analysis show that the algorithm has a large space and good statistical characteristics of cipher image. In addition, the ciphertext is very impressible to the plaintext and the secret key, can bear chosen-plaintext attacks. As a result, this new algorithm has good application prospects in image secure communication and storage applications.

ISCC2017
16-17 December 2017
Guangzhou, China

[1]The work is financially supported by Shandong Province Nature Science Foundation (Grant.ZR2017MEM019).

PoS(ISCC 2017)006

1. Introduction

Chaotic system is a very interesting physical phenomena generated from a nonlinear system, characterized by its unpredictability with completely dependence on initial conditions. In fact, hyper-chaos characterized with more than one positive Lyapunov exponent and more complicated dynamics behaviors has wider application prospects. It is very essential to generate hyper-chaos with more complex dynamical behavior [1-6]. Li et al designed a hyper-chaos by adding a state-feedback controller to the first control input to drive a unified chaotic system to generate hyper-chaos [1]. Murali et al proposed the methodology of generating simple hyper-chaos circuits with a stable oscillator and an unstable one [2]. Sprott et al investigated a special and novel chaotic system with only one stable equilibrium point [3] , while Qiang Lai et al proposed a new three-dimension autonomous chaotic system with coexisting attractors[4]. Chen E. and Min Lequan constructed a kind of 4D discrete hyper-chaotic system with one-line equilibria[5] · Moreover, Shouquan Pang and Yongjian Liu presented a new 4D hyper-chaotic system, which is derived from a linear controller to a three-dimension Lü system [6]. This paper demonstrates a five-dimension hyper-chaotic system based on the 4D hyperchaotic system described in [6], which displays more complicated dynamics behavior.

With the fast development of network technology, a growing number of digital images need to be stored and transmitted. Due to the openness and sharing of the network, the security problem of digital images has become more serious. Image encryption is one of the most effective measures to protect images. However, digital image is characterized by the large amount and high redundancy, so the traditional encryption scheme is not suitable for image encryption. Because the chaotic system has the characteristics of sensitivity to initial conditions and system parameters, pseudo randomness, uncertainty and ergodicity, it is consistent with the two basic principles of cryptography: diffusion and confusion. Digital image encryption based on chaos has been a hotspot; also, many image encryption algorithms based on chaos have been proposed [7-11]. However, these algorithms are all traditional ones based on diffusion-scrambling structure. Because DNA computing has the advantages of high information density, parallelism and ultra-low energy consumption, it has penetrated into the field of cryptography. In recent years, many cryptographic systems based on DNA have been proposed, and DNA is used as an information carrier, which conveys information in the form of DNA sequences. Some image encryption methods based on DNA coding and chaos have been proposed [12-17]. Gehani et al introduced the one-time pad image encryption with DNA, which is effective, but contains complex biological operations [12]. An image encryption method is proposed in [13]. In each encryption process, the initial conditions of chaos can be automatically adapted, and the image pixels are encoded by DNA. At the same time, each nucleotide in the DNA encoded image is randomly transformed into base pairs by following the DNA complementary rule. Q Zhang et al presented an image encryption algorithm using DNA encoding and two chaotic maps [14]. However, this technique has severe drawbacks as analyzed by H. Hermia et al [15] - they found that the encryption scheme could not be decrypted or resist chosen plaintext attacks. Anchal Jain and According to the image encryption technique using DNA operations and chaotic maps [16] as proposed by Navin Rajpal, the input image is encoded with DNA first, then the image is added to the mask generated by chaotic system. An intermediate result is the complemented DNA based on a complement matrix produced by two chaotic maps. Finally, the resultant matrix is permuted, followed by DNA decoding to get the cipher image. Xiaoling Huang and Guodong Ye suggested a novel image encryption algorithm utilizing hyper-chaos and DNA sequence [17]. Firstly, a pseudo-random sequence generated by a four-dimension hyper-chaos system is transformed in a biologic DNA sequence to diffuse the image blocks.

Afterwards, a circular permutation is performed on the plain-image when it is in DNA status.

The core of these encryption algorithms is DNA encoding and DNA computing, which include complementary rules of base, DNA addition, DNA subtraction and DNA XOR operation. However, some encryption methods are vulnerable in several aspects. Firstly, keys can be obtained through a pair of plaintext images and corresponding ciphertext images; secondly, the encryption process is insensitive to the changes of the plain image or of the secret key. In addition, the encoding/decoding rules of the plain image and the key matrix are fixed. Therefore, remedial methods and high security image encryption schemes should be developed for security enhancement.

Based on the above analyses, a chaos- based image encryption algorithm using dynamic DNA coding and SHA-256 is introduced in this paper. The algorithm has three advantages. First, pixels in different positions use different DNA encoding or decoding rules according to the random matrix generated by a five-dimension hyper-chaotic system. Secondly, the initial values of the chaotic system are calculated by using the SHA 256 hash of the plain image and the given values. There are different initial values and system parameters for different plain images. Thus, the mentioned algorithm can effectively resist the chosen-plaintext and known-plaintext attacks.

By a glance at this paper, Section 2 introduces the hyper-chaotic system and Section 3 Sections describes the dynamic DNA coding technology. The proposed image encryption process and simulation results are explained in details in Section 4. Security analysis is conducted in the Section 5, and finally the conclusion is given.

2. The New Hyperchaotic System and Its Dynamics Analysis

2.1 The Generation of Hyper-chaos Via A Linear Controller

Consider the chaotic system found by Shouquan Pang and Yongjian Liu [6]:

$$\begin{cases} \dfrac{\partial x}{\partial t} = a(y-x) \\ \dfrac{\partial y}{\partial t} = cy - xz + u \\ \dfrac{\partial z}{\partial t} = xy - bz \\ \dfrac{\partial u}{\partial t} = -k_1 x - k_2 y \end{cases} \tag{2.1}$$

Given that (a, b, c, k_1, k_2) = (36, 3, 20, 2, 2), the corresponding chaotic orbits are described in Fig 1(*a*)–(*f*), which has four Lyapunov exponents: λ_{LE1}= 1.4106, λ_{LE2}= 0.1232, λ_{LE3}= 0.0000, λ_{LE4}= −20.5339, and the Lyapunov dimension is D_L=3.0747.

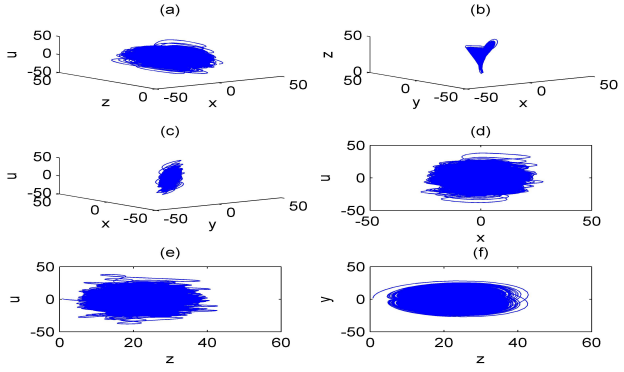

Figure 1 : The orbits of hyperchaotic Lü system (1) (a) x-z-u; (b) x-y-z; (c) y-x-u; (d) x–u; (e) u-z; (f) z-y

A linear feedback controller is added to the second equation of the system (2.1) to obtain the following hyper-chaotic system (2.2)

$$\begin{cases} \dfrac{\partial x}{\partial t} = -a(y-x) \\ \dfrac{\partial y}{\partial t} = -c(x+y) - xz - pu \\ \dfrac{\partial z}{\partial t} = -xy - bz \\ \dfrac{\partial u}{\partial t} = -my + fw \\ \dfrac{\partial w}{\partial t} = -eyz \end{cases} \tag{2.2}$$

When (a, b, c, p, m, e, f) = (25, 2, 10, 1, 16, 2, 1), the corresponding chaotic attractor is depicted in Fig. 2(a)–(f), which has five Lyapunov exponents: λ_{LE1}=1.599, λ_{LE2}=0.982, λ_{LE3}=−0.039, λ_{LE4}=−0.09, λ_{LE5}= −13.5.

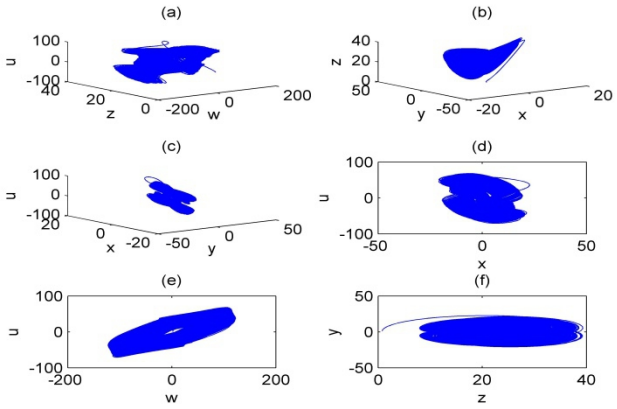

Figure 2 : The orbits of new hyper-chaotic system (2) (a) *w-z-u*; (b) *x-y-z*; (c) *y-x-u*;(d) *x–u*; (e) *u-w*; (f) *z-y*

2.2 Dynamic behaviors of the new hyperchaotic system

This section is mainly about the study onthe dynamical behavior of hyperchaotic system (2.2), including dissipation, equilibrium and stability.

(1) Dissipativity

For system (2.2), a conclusion can be made as follows:

$$\Delta V = \frac{\partial \dot{x}}{\partial x} + \frac{\partial \dot{y}}{\partial y} + \frac{\partial \dot{z}}{\partial z} + \frac{\partial \dot{u}}{\partial u} + \frac{\partial \dot{w}}{\partial w} = -a - b + c = -17 < 0$$

For a = 25, b = 2, c = 10 and any values p, m, e, f. In that case, the system is dissipative with an exponential contraction rate $V0e^{-(a+b-c)t}$, which has nothing to do with P, m, e, f . This indicates that each volume containing the system orbit shrinks to zero as $t \to \infty$ at an exponential rate − (a+b−c). Therefore, all system orbits are eventually limited to a subset of zero volumes.

(2) Equilibria and stability

Obviously, the origin O (0, 0, 0, 0, 0) is a unique equilibrium. Linearizing system (2.2) at O (0, 0, 0, 0, 0) now yields the Jacobian matrix

$$J=\begin{bmatrix} -a & a & 0 & 0 & 0 \\ c & c & 0 & -p & 0 \\ 0 & 0 & -b & 0 & 0 \\ 0 & m & 0 & 0 & f \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

By solving the equation (2.3)

$$|\lambda I - J| = o \tag{2.3}$$

the five eigenvalues of the matrix are obtained, which are x_1=-31.0190, x_2=15.1689, x_3=0.8501, x_4=-2, x_5=0. The five characteristic roots are real roots, but are not all negative. According to Routh-Hurwitz theorem, the equilibrium point is unstable, and the possibility of the existence of chaos in the system is proved theoretically.

3. DNA Coding and DNA Operation

A DNA sequence contains four nucleic acid bases A (adenine), C (cytosine), G (guanine), and T (thymine), where A and T are in a pair while C and G are in another pair for the complementary property. In order to comply with the complement rule [14], there are eight kinds of coding schemes as listed in Table 1. A grayscale value can be expressed as a DNA sequence. For example, the pixel value 102 has a binary representation 01100110, and then the DNA sequence can be interpreted as TATA by encoding rule 6 in Table 1. Inversely, any DNA sequence with length 4 corresponds to an 8-bit gray value. For instance, GCCT is considered as 01101000 by rule 8, and its decimal value is 104.

Pairs	1	2	3	4	5	6	7	8
A	0	0	0	0	1	1	1	1
	0	0	1	1	0	0	1	1
C	0	1	0	1	0	1	0	1
	1	0	0	1	0	1	1	0
G	1	0	1	0	1	0	1	0
	0	1	1	0	1	0	0	1
T	1	1	1	1	0	0	0	0
	1	1	0	0	1	1	0	0

Table 1: Eight DNA Encoding Rule

X	Complement (X)
A	T
T	A
C	G
G	C

Table 2: The DNA Complement

4. The Proposed Image Encryption Algorithm

4.1 Dynamic Encoding of the Plaintext Image in DNA Sequence

The application of DNA coding rules is determined among some image encryption algorithms based on chaos and DNA coding. Since there are only 8 DNA encoding rules, it will lead to the low competency for anti-brute force attack, which will further cause safety issues.

Concerning that, this paper proposes a dynamic DNA coding method, namely, selecting different DNA encoding rule among the 8 DNA encoding rules listed in Table 1, according to the random matrix generated by chaotic system . Pixels in different positions are coded with different DNA coding rules. For example, B_1 is plain text image matrix, C is the random matrix whose elements represent encoding rules, and the first element of the matrix B_1 is encoded with the first rule in Table 1, according to the matrix C. Namely, the pixel value 12 has a binary representation as 00001100, then the DNA sequence can be read as AATA by encoding rule 1 in Table 1. Therefore, the encoded matrix B_2 is formed directly according to B1and C.

$$B_1=\begin{bmatrix} 12 & 201 & 122 \\ 122 & 133 & 098 \end{bmatrix} \quad C=\begin{bmatrix} 1 & 4 & 7 \\ 2 & 3 & 5 \end{bmatrix}$$

$$B_2=\begin{bmatrix} A & A & T & A & C & G & T & A & C & A & G & G \\ G & T & C & C & T & C & A & A & T & A & C & A \end{bmatrix}$$

4.2 Generation of the Initial Conditions of the New Hyperchaotic System by SHA-256 hash

Iterating the hyper-chaotic system (2.3) from the initial conditions x_0, y_0, z_0, u_0, w_0, and chaotic sequences will be obtained. However, in order to enhance the security of the proposed algorithm and the relationship between key and plaintext image, a new method is designed in this study to renovate the initial conditions. The image hash function is usually for the generation of fixed length output as a shortened digest of raw data. Here SHA-256 is used to generate the 256-bit hash value, which can be divided into 32 blocks K with the same size of 8-bit, the i^{th} block $k_i \in [0, 255]$, $i = 1, 2, \ldots, 32$. Then K can be expressed as $K = k_1, k_2, \ldots, k_{32}$. The new initial conditions x_0, y_0, z_0, u_0, w_0 can be renewed by the following:

$$\begin{cases} x_0 = x_0' + \dfrac{(k_1 \oplus k_2 \oplus k_3 \oplus k_4 \oplus k_5 \oplus k_6 \oplus k_7 \oplus k_8)}{256} \\ y_0 = y_0' + \dfrac{(k_9 \oplus k_{10} \oplus k_{11} \oplus k_{12} \oplus k_{13} \oplus k_{14} \oplus k_{15} \oplus k_{16})}{256} \\ z_0 = z_0' + \dfrac{(k_{17} \oplus k_{18} \oplus k_{17} \oplus k_{20} \oplus k_{21} \oplus k_{22} \oplus k_{23} \oplus k_{24})}{256} \\ u_0 = u_0' + \dfrac{(k_{25} \oplus k_{26} \oplus k_{27} \oplus k_{28} \oplus k_{29} \oplus k_{30} \oplus k_{31} \oplus k_{32})}{256} \\ w_0 = w_0' + \dfrac{(k_4 \oplus k_8 \oplus k_{12} \oplus k_{16} \oplus k_{20} \oplus k_{24} \oplus k_{28} \oplus k_{32})}{256} \end{cases} \quad (4.1)$$

4.3 Generation of Random Sequence based on Chaotic System

It is assumed that plain-image P has a size of $m \times n$. For the updated initial condition (x_0, y_0, z_0, u_0, w_0), one can obtain five hyper-chaotic sequences X, Y, Z, U, W. $X=\{x_1, x_2, x_3, \ldots, x_{mn}\}$, $Y=\{y_1, y_2, y_3, \ldots, y_{mn}\}$, $Z=\{z_1, z_2, z_3, \ldots, z_{mn}\}$, $U=\{u_1, u_2, u_3, \ldots, u_{mn}\}$, $W=\{w_1, w_2, w_3, \ldots, w_{mn}\}$.

1) Preprocessing hyper-chaotic sequences X and Y by Eq. (4.2), and getting two random sequences $S=\{s_1, s_2, \ldots, s_{mn}\}$ and $T=\{t_1, t_2, t_3, \ldots, t_{mn}\}$. S, $T \in [1, 2, 3, 4, 5, 6, 7, 8]$. Then, transform the two random sequences S and T to two matrixs S and T of size $m \times n$ by *Eq.*(4.3).

$$\begin{cases} s_i = mod\left(floor\left(x_i \times 10^{14} \right), 8 \right) + 1 \\ t_i = mod\left(floor\left(y_i \times 10^{14} \right), 8 \right) + 1 \end{cases} \tag{4.2}$$

$$\begin{cases} S = reshape\left(S, m, n \right) \\ T = reshape\left(T, m, n \right) \end{cases} \tag{4.3}$$

2) Transforming hyper-chaotic sequences U and Z to random matrix K according *Eq.*(4.4)

$$\begin{cases} D = \cos^2\left(\left(U + Z \right)/2 \right) \\ K = mod\left(round\left(10^{15} D \right), 256 \right) = \left(k_{1,} k_{2,} .., k_{mn} \right) \\ K = reshape\left(K, m, n \right) \end{cases} \tag{4.4}$$

3) Preprocessing hyper-chaotic sequences W by *Eq.*(4.5), and getting four random sequences $RR=\{rr_1, rr_2, \ldots, rr_{mn}\}$, $TT=\{tt_1, tt_2, \ldots, tt_{mn}\}$, $TG=\{tg_1, tg_2, \ldots, tg_{mn}\}$, $ZZ=\{zz_1, zz_2, \ldots, zz_{mn}\}$. The four random vectors are combined into a random sequence CC of length $4mn$, shown by (4.6), then by the Eq. (4.7) and preprocessing sequence CC. Sequence $R=\{r_1, r_2, \ldots, r_{4mn}\}$ can be obtained, and the random sequence R can be transformed to a random matrix of size $m \times 4n$.

$$\begin{cases} rr_i = mod\left(fix\left(\left| w_i \right| \times 10^7 \right), 10 \right) \\ tt_i = mod\left(fix\left(\left| w_i \right| \times 10^8 \right), 10 \right) \\ tg_i = mod\left(fix\left(\left| w_i \right| \times 10^9 \right), 10 \right) \\ zz_i = mod\left(fix\left(\left| w_i \right| \times 10^{10} \right), 10 \right) \end{cases} \tag{4.5}$$

$$CC = \left[RR \quad TT \quad TG \quad ZZ \right] \tag{4.6}$$

$$\begin{array}{l} r_i = 0, if\ cc_i \geq 5 \\ r_i = 1, if\ cc_i < 5 \end{array} \tag{4.7}$$

4.4 Encryption process and decryption process

4.4.1 The block diagram of the proposed image encryption algorithm is given in Fig. 3.

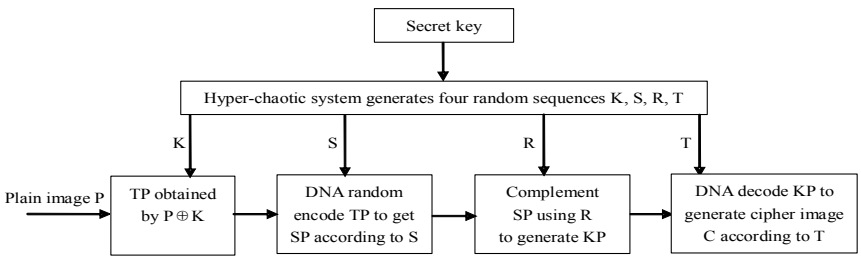

Figure 3: Block Diagram of the Proposed Image Cryptosystem

4.4.2The whole encryption process flow is described as below

1) The image matrix P and random matrix K are used to carry out operations by the following (4.8), then to get the matrix TP.

$$TP = bitxor\left(P, K \right) \tag{4.8}$$

2) Encoding TP according to random matrix *S* and getting *SP* of size $m \times 4n$ with DNA elements.

3) Using DNA complementary rule as suggested in Table 2 to complement matrix SP obtained in Step 2 so as to obtain matrix *KP*. Therefore, Coefficient $kp(i,j)$ of Matrix *KP* is complemented as in (4.9), based on the value of $r(i,j)$ of matrix *R*.

$$\begin{aligned} kp(i,j) &= sp(i,j), if\ r(i,j)=0 \\ kp(i,j) &= comp(sp(i,j)), if\ r(i,j)=1 \end{aligned} \tag{4.9}$$

4) Converting matrix *KP* back to decimal number using DNA decoding according to random sequences *T* to get the final cipher image *C*.

4.4.3Decryption process of the cipher image is parallel to the encryption process.

1) Encoding cipher image *C* according to random matrix *T* to get $KP_{m\times 4n}$ with DNA elements.

2) This step is exactly the same as step 3 of the encryption process, namely, DNA complementary rule as suggested in Table 2 is used to complement matrix *KP*.

Therefore, coefficient *SP* (i,j) of matrix *SP* is complemented as in *Eq*.(4.9), based on the value of $r(i,j)$ of matrix *R*.

3) Converting matrix *SP* back to decimal number by using DNA decoding according to random matrix *S* to get the matrix *TP* of size $m \times n$.

4) The image matrix TP and random matrix K are used to carry out the following operations, and then to get the plain text image matrix *P*

$$P = bitxor(TP, K) \tag{4.10}$$

4.5 Experimental Results

Here we set keys = {10.09845, 9.87657, 10.45768, 8.09457, 6.09478, 234, 256 bit hash value of plain text image} to encrypt three natural image"cameraman". Fig. 4 (b) displays the decrypted image successfully. From Fig. 4(a), information of the plain text image cannot be gained from the encrypted image.

Figure 4: (a) Cipher-text Image; (b) The decrypted image

5. Security analysis

5.1 Sensitivity Analysis and Key Space

Numerical simulation shows that the algorithm is very sensitive to the keys and can reach 10^{-15} or more. That is to say, even if the key value has a slight deviation of 10^{-15}, the original image cannot be decrypted. In Fig. 5(*a*)-(*e*), the Ciphertext image of "cameraman" is decrypted with the wrong keys.

$\{x_0', y_0', z_0', u_0', w_0'\}$={10.09845+$10^{-15}$, 9.87657, 10.45768, 8.09457, 6.09478},

$\{x_0', y_0', z_0', u_0', w_0'\}$ ={10.09845, 9.87657+10^{-15}, 10.45768, 8.09457, 6.09478},

$\{x_0', y_0', z_0', u_0', w_0'\}$ ={10.09845, 9.87657, 10.45768+10^{-15}, 8.09457, 6.09478},

$\{x_0', y_0', z_0', u_0', w_0'\} = \{10.09845, 9.87657, 10.45768, 8.09457+10^{-15}, 6.09478\}$,

$\{x_0', y_0', z_0', u_0', w_0'\} = \{10.09845, 9.87657, 10.45768, 8.09457, 6.09478+10^{-15}\}$.

Information of the original image of "cameraman" from the Fig.5cannot be derived.

If the precision of 10^{-15} is chosen for each parameter, the size of secret key space will be 10^{75}. Furthermore, the key space of SHA-256 is up to 2^{256}, so the total key space can be up to $10^{75} * 2^{256}$. Therefore, the algorithm can resist brute-force attack.

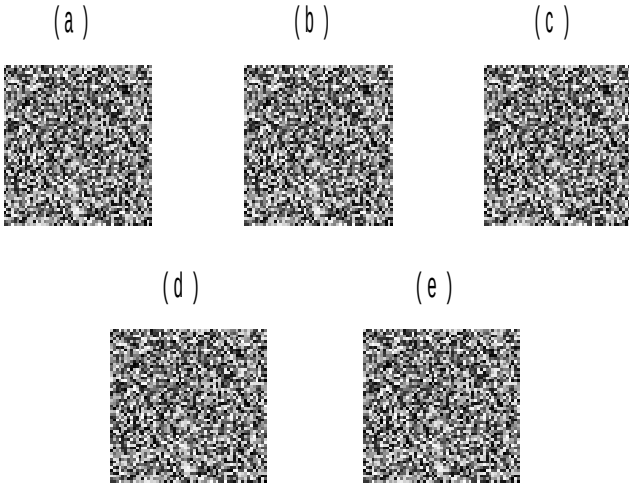

Figure 5: Decryption image using error key

5.2 Statistical Histogram

The histogram of encrypted image can reflect the quality of encryption. In general, the histogram presents a uniform distribution or normal distribution, indicating better encryption effect.

Fig. 6(a)and Fig. 6(b) are respectively for the statistical histograms of cipher-text images and plain text images. The histograms of the plaintext images are bimodal has and have obvious statistical characteristics, while the histograms of the ciphertext images present a uniform distribution without obvious statistical characteristics. Thus, the new encryption scheme can resist statistical attacks.

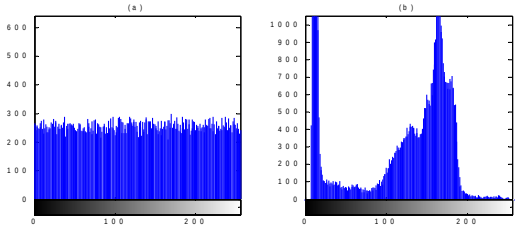

Figure 6: (a) Histogram for Ciphertext image; (b) Histogram for plain text image "cameraman"

5.3 Correlation Analysis

There is a strong correlation between the adjacent pixels of a natural image, and the purpose of encryption is to remove this correlation, strengthen the resistance to statistical analysis. 1,000 pairs of adjacent pixels are selected from plaintext and ciphertext respectively, including vertical, horizontal, and diagonal directions to test the correlation between adjacent pixels of plaintext and ciphertext. Formula of correlation coefficient, such as formula (5.1)-(5.4), as Akhshani did [18].

$$r_{XY} = cov(X, Y) / \sqrt{D(X) D(Y)} \tag{5.1}$$

$$E(X)=\frac{1}{N}\sum_{i=1}^{N}x_i \tag{5.2}$$

$$D(X)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(X))^2 \tag{5.3}$$

$$cov(X,Y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(X))(y_i-E(Y)) \tag{5.4}$$

Here, X and Y represent the gray values of the two adjacent pixels in the image. The correlation of the two adjacent pixels in the vertical, horizontal, and diagonal directions of the "cameraman" plaintext image and the ciphertext image is shown in Figures 7 and 8. The correlation coefficients of two adjacent pixels in some cipher images are indicated in Table 3, the lowcorrelation and positive encryption effect.

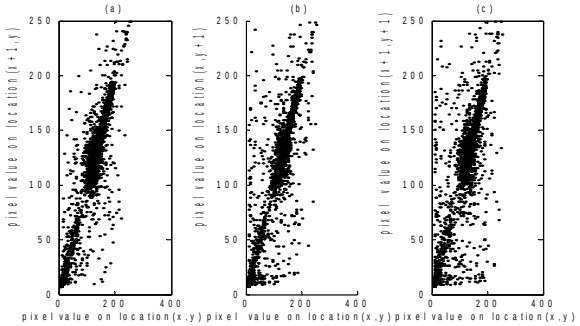

Figure 7: Adjacent pixels correlation graph of plaintext image "cameraman": (a) horizontal direction correlation; (b) vertical direction correlation; (c) diagonal direction correlation

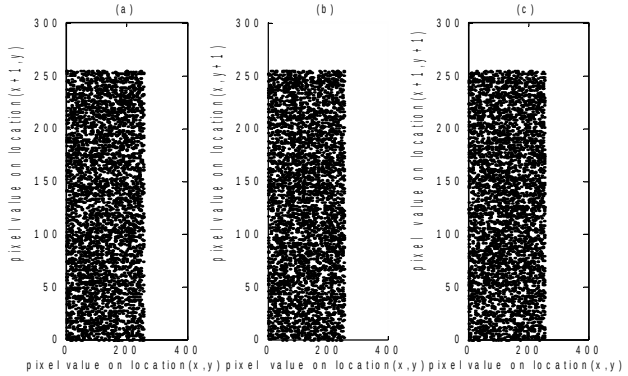

Figure 8: Adjacent pixels correlation graph of Ciphertext Image "cameraman": (a) horizontal direction correlation; (b) vertical direction correlation; (c) diagonal direction correlation

Image	Cameraman	trees	peppers
Horizontal	0.0654	0.0128	0.0834
diagonal	0.0065	0.0324	0.0166
vertical	-0.0438	-0.0035	0.0036

Table 3: Correlation coefficients of two adjacent pixels in the cipher-images

5.4 Information Entropy Analysis

Image entropy is a concept to measure the amount of image information. The larger the image entropy is, the less the information is carried by the image [19]. The formula of information entropy is calculated as (5.5)

$$H=\sum_{i=1}^{n} p(s_i)\log_2(p(s_i)) \tag{5.5}$$

where $p(s_i)$ denotes the probability of symbol s_i. For 256 gray images, the ideal information entropy is 8. Table 4 shows the entropy of the cipher-images. The obtained values are very close to 8, which concludes that the encrypted images are random and unpredictable.

Image	Cameraman	Trees	Peppers
Entropy	7.9890	7.9894	7.9920

Table 4: Information Entropy of the Cipher-images

5.5 Plaint Text Sensitivity

The algorithm is sensitive to plaintext, which means that a small change to plaintext will greatly affect the corresponding ciphertext. The algorithm is more sensitive to plaintext, with greater ability to resist differential attack. The NPCR and UACI [18] are usually used to measure the ability of the algorithm to resist differential attack, and its formulas are shown in Formula (5.6)-(5.7)

$$NPCR=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D_{ij}}{MN} \tag{5.6}$$

$$UACI=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{c_1(i,j)-c_2(i,j)}{255}}{MN} \tag{5.7}$$

where C_1 and C_2 are two ciphertext images, and their corresponding plaintext images have different pixel values . M and N are the width and height of the image respectively. $D(i, j)$ is determined as formula (5.8).

$$\begin{aligned} D(i,j)&=0, if\ c_1(i,j)=c_2(i,j)\\ D(i,j)&=1, if\ c_1(i,j)\neq c_2(i,j)\end{aligned} \tag{5.8}$$

10 pixels in the the plain-image “cameraman” are randomly selected, and the gray value is adjusted with the difference 1. For example, the gray value - 58 of the pixel at position (101, 200) is replaced by 59. Therefore, 10 images with slight difference from the plaintext images are received, and the 10 encrypted images can be obtained via encryption. Therefore, the NPCR and UACI values of the 10 ciphertext images and the original ciphertext can be calcu lated respectively, which are shown in Table 5. The mean values of the 10 NPCR and UACI values are 99.4453% and 34.4973% respectively. They are close to the ideal values (about 0.996 and 0.334).

Position	(101,200)	(161,210)	(11,22)	(81,20)	(210,89)
NPCR(%)	99.8093	98.4416	99.1906	98.3011	99.5611
UACI(%)	45.6606	40.3064	33.6844	34.5754	27.4453
Position	(151,208)	(19,208)	(71,109)	(67,88)	(189,123)
NPCR(%)	99.8201	99.0876	99.1926	98.1906	99.8451
UACI(%)	33.2842	26.9481	39.7866	36.9054	46.3763

Table 5: Results of NPCR and UACI tests of "cameraman"

5.6 Resistance to Chosen-plaintext Attacks

The key streams of this paper are four random sequences: K, S, T, R, which are related to the plain text image. The chaotic sequences - K, S, T, R used by the encryption system are different per images. Attackers cannot obtain random sequences K, S, T, R by using the chosen-plaintext attacks.

6. Summary

This study presents a novel hyperchaos-based image encryption algorithm using dynamic DNA coding and SHA-256.The safety of the encryption algorithm depends on the four random sequences, which are produced by the five-dimension hyper-chaos system with the initial value related to the SHA-256 hash of the explicit image. Therefore, the encryption algorithm can resist the attacks by both known-plaintext and chosen- plaintext. Furthermore, to improve the security of the encryption algorithm, different DNA coding rules are adopted for the pixel values of different positions, according to random matrix S produced by the five-dimension hyper-chaos system. Experiment results and the security analysis show that the new algorithm can also resist the entropy attack and statistical attack.

References

[1] Y. Li, W. Tang and G. Chen, *"Hyperchaos evolved from the generalized Lorenz equation," Int. J.* Circuit Theory Appl. vol. 33, Apr. 2005, pp. 235–251.

[2] K. Murali, E. Lindberg and H. Leung, *"Design principles of hyperchaotic circuits," In. AIP Conf.* Proc. 622 (2001) 15–26

[3] J. C. Sprott, X. Wang and G. R. Chen, *"Coexistence point, periodic and strange attractors," Int. J.* Bifurc. Chaos. vol. 23, May. 2013, pp. 1350093–1350097

[4] Q. Lai and S. Chen, *"Research on a new 3D autonomous chaotic system with coexisting attractors,"* Optik. vol. 127, Mar. 2016, pp. 3000–3004.

[5] E. Chen and L. Q. Min, *"Discrete Chaotic Systems with One-Line Equilibria and Their Application to Image Encryption,"* International Journal of Bifurcation and Chaos. vol. 27, Mar. 2017, pp. 1750046–1750062.

[6] S. Q. Pang and Y. J. Liu, *"A new hyperchaotic system from the Lü system and its control,"* J.Comput. Appl. Math. vol. 235, Feb. 2011, pp. 2775–2789.

[7] C. Zhu, *"A novel image encryption scheme based on improved hyperchaotic sequences,"* Opt. Commun. vol. 285, Jan. 2012, pp. 29–37.

[8] O. Mirzaei, M. Yaghoobi and H. Irani, *"A new image encryption method: parallel sub-image encryption with hyper chaos,"* Nonlinear Dyn. vol. 67, Jan. 2012, pp. 557–566

[9] X.Huang, *"Image encryption algorithm using chaotic chebyshev generator,"* Nonlinear Dyn. vol. 67, Mar. 2012, pp. 2411–2417,

[10] C. Li, S. Li and K. T. Lo, *"Breaking a modified substitution–diffusion image cipher based on chaotic standard and logistic maps,"* Commun. Nonlinear Sci. Numer. Simul. vol. 16, Feb. 2011, pp. 837–843,

[11] H. J. Liu and X. Y. Wang, *"Color image encryption using spatial bit-level permutation and high-dimension chaotic system,"* Optics Communications. vol. 284, Aug. 2011, pp. 3895-3903,

[12] A. Gehani, T. LaBean and J. Reif, *"DNA based cryptography,"* Discrete Math. Theor. 54 (2000) 233–249.

[13] H. Liu, X. Wang and A. Kadir, *"Image encryption using DNA complementary rule and chaotic maps,"* Appl. Soft. Comput. vol. 12, May. 2012, pp. 1457–1466.

[14] Q. Zhang, L. Guo and X. Wei, *"Image encryption using DNA addition combining with chaotic maps,"* Math. Comput. Model. vol. 52, Dec. 2010, pp. 2028–2035.

[15] H. Hermassi, A. Belazi, R. Rhouma and S. Belghith, *"Security analysis of an image encryption algorithm based on a DNA addition combining with chaotic maps,"* Multimed. Tools Appl. vol. 72, Oct. 2014, pp. 2211–2224.

[16] J. Anchal and R. Navin, *"A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps,"* Multimed. Tools Appl. vol. 75, May. 2016, pp. 5455–5472,

[17] X. L. Huang and G. D. Ye, *"An image encryption algorithm based on hyper-chaos and DNA sequence,"* Multimed. Tools Appl. vol. 72, Sep. 2014, pp. 57–70.

[18] S. Behnia, A. Akhshani, H. Mahmodi and A. Akhavan, *"A novel algorithm for image encryption based on mixture of chaotic maps,"* Chaos Soliton Fract. vol. 35, Jan. 2008, pp. 408–419.

[19] F. Y. Sun, Z. W. Lu and S. T. Liu, *"A new cryptosystem based on spatial chaotic system,"* Opt. Commun. vol. 283, May. 2010, pp. 2066–2073.