DE GRUYTER
OPEN

Journal of ELECTRICAL ENGINEERING, VOL 67 (2016), NO2, 78–86

SPLICING MODEL AND HYPER–CHAOTIC SYSTEM FOR IMAGE ENCRYPTION

Hongye Niu — Changjun Zhou — Bin Wang
Xuedong Zheng — Shihua Zhou *

Encryption is an effective way to protect the image information from attacking by intruders in the transmission applications through the Internet. This study presents an image encryption scheme on the basics of the formal model of DNA computing-splicing system and hyper-chaotic system, which utilizes the instinct properties of hyper-chaotic system and splicing model while programming the method. In our proposed algorithm, the quaternary coding is used to split the plain image into four sub-sections so that we can't get the cipher image without any one sub-section. This new method can be used to change the plain image information drastically. The experimental results and security analysis show that our method not only has a good security but also increases the resistance to common attacks such as exhaustive attacks, statistical attacks and differential attacks.

K e y w o r d s: image encryption, hyper-chaotic system, DNA coding, splicing model

1 INTRODUCTION

With the increasing usage of digital images has been transmitted over Internet, it becomes more and more important to prevent the image informations from disclosing by unknown persons or hackers. As we all know, the most proficient way to protect image information is image encryption. Meanwhile, a large amount of encryption technologies had been published by a large number of researchers [1–3]. Among them, the most widely and highly successful optical encryption schemes are chaos-based image encryption and DNA cryptography-based image encryption because of the distinct characteristics of chaotic map such as sensitivity to the system parameter and initial value [4, 5], respectively, DNA computing 's advantages are the vast parallelism and extraordinary information density and exceptional energy efficiency [6, 7].

Chaos-based image encryption algorithms have ever been popularly used because of the distinct characteristics of chaos system are closely related to the secrecy system. Since chaotic map was firstly used to design a cryptographic algorithm in 1989 [8], various image algorithms had been proposed in the field of cryptography research based on multiple one-dimensional, two-dimensional or higher-dimensional chaotic systems [9–11]. Beldhouche *et al* suggested binary image encoding using one-dimensional chaotic map [12]. And then, Seyedzadeh *et al* proposed a fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map [13]. After that, Chen *et al* pointed out a symmetric image encryption scheme based on 3D chaotic cat maps [14]. Furthermore, Gao *et al* presented an image encryption algorithm based on hyper-chaos [15]. However, the most of them are easy to be attacked by the assailants result from the algorithms concentrated on the chaotic sequence and the pixel grey value from the image to realize encryption.

Nowadays, the hottest encryption method is DNA cryptography, which combines DNA as information carrier with the modern biological technology as implementation tool to realize encryption [16, 17]. Jain *et al* presented adaptive key length based encryption algorithm using DNA approach [18]. Soni *et al* proposed an encryption and decryption algorithm for image based on DNA [19]. Zhou *et al* pointed out image encryption algorithm based on DNA sequences for the big image [20]. Unfortunately, these experiments are theoretically possible but perfect operation is difficult owing to the requirement is a well equipped lab. Recently, DNA sequence operations and chaotic sequences which generated by chaos map were employed in the process of image encryption schemes. In [21], Zhang *et al* used DNA sequence XOR operation and Chen's hyper-chaotic system to scramble and diffuse the pixel values from plain image. Som *et al* proposed a color image encryption based on DNA coding and chaotic sequences, in which the OR operation and 1D Logistic map were employed to producing the cipher image [22]. In the above described methods, there exists a risk of being broken with the rapid development of the parallel computing and cloud computing and quan-

* Key Laboratory of Advanced Design and Intelligent Computing (Dalian University), Ministry of Education, Dalian, 116622, China, zhou-chang231@163.com

DOI: 10.1515/jee-2016-0012, Print (till 2015) ISSN 1335-3632, On-line ISSN 1339-309X

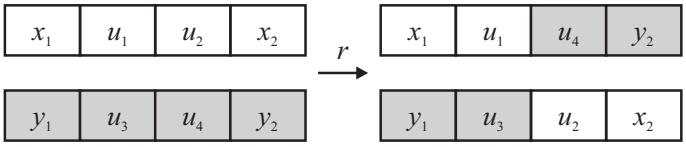

Fig. 1. The splicing operation

tum computing. A mixed image encryption scheme which is composed of the logistic chaotic map and the formal model of DNA computing-splicing system was proposed by Zhou *et al*, which has effectively improved the security of image encryption [23].

In the past decade years, some researchers have been concentrated on DNA computing in image encryption algorithm, where the binary number system is widely implemented to represent the pixel values from plain image. However, the encoding schemes for pixel value are limited since the DNA encoding must satisfy the Watson-Crick complement rule. Simultaneously, the coding speed is lower because the pixel value is transformed into binary first. Therefore, this paper proposes a new method of image encryption using splicing model and hyper-chaotic system to meet the requirements of modern applications with high level of security. This method presents a new way of DNA encoding based on the basic theory of quaternary coding, which expands the encoding schemes and decreases the complexity of computational. Besides, we not only use the DNA sequence operation to diffuse the pixel value from plain image, but also employ the splicing model to take participate in the image encryption procedure. This method has a better encryption effect and resists the common attacks.

2 THE RELATED WORKS

2.1 Chen's hyper-chaotic system

Chaos is a non-linear procedure with the complex structure, whose properties have a natural connection with traditional technologies. Therefore, it is normal to develop image cryptography algorithm by chaos systems. Within the design of the encryption algorithm, the Chen's hyper-chaotic system is employed, which is described as [21]

$$\begin{aligned} \dot{x} &= a(y-x)\,, \\ \dot{y} &= -xz - dx + cy - q\,, \\ \dot{z} &= xy - bz\,, \\ \dot{q} &= x + k\,, \end{aligned} \tag{1}$$

where a, b, c, d, k are the system parameters. when $a = 36$, $b = 3$, $c = 28$, $d = 16$ and $-0.7 \leq k \leq 0.7$, Chen's hyper-chaotic map is full chaotic map and generate four chaotic sequences and we set $k = 0.4$ in this communication.

2.2 The splicing model

In 1987, Tom Head proposed the splicing system which contains two procedures that cutting sequences at specific sites and sticking the fragments with matching end [24]. Generally, the basic splicing system is based on a linear DNA molecule fragments. The formal model of splicing system is as follows:

Consider an abstract alphabet V, and two strings $x = x_1u_1u_2x_2$, $y = y_1u_3u_4y_2$ which composed of symbols of V. It is a splicing operation that converting the array $(x_1u_1u_2x_2, y_1u_3u_4y_2)$ into $(x_1u_1u_4y_2, y_1u_3u_2x_2)$ under the regulation of $r = u_1\#u_2\$u_3\#u_4$, which was illustrated in Figure 1 [25].

In this complementation, the ideas of splicing model which has unique properties such as vast parallelism were employed in the proposed algorithm via simulation experiment in order to speed up encryption speed.

2.3 DNA sequence operations

DNA encoding and decoding based on quaternary

A positive integer X can be represented by a set of N integer constants $\{m_1, m_2, \ldots, m_N\}$ which is defined as

$$\begin{aligned} m_1 &= X \bmod n\,, \\ m_2 &= (X/n) \bmod n\,, \\ m_3 &= (X/n^2) \bmod n\,, \\ &\vdots \\ m_N &= (X/n^{N-1}) \bmod n\,, \end{aligned} \tag{2}$$

where positive integer n is smaller than X.

The above operation is reversible and we can get the value of X according to the inverse of (2) by the following formula

$$X = ((((X/n^N)\times n + m_N)\times n + m_{N-1})\ldots)\times n + m_1\,. \tag{3}$$

In our proposed algorithm, we employ the basic principle of quaternary to divide plain image into four subsections so as to each sub-section can be encoded individually and the cipher image is not complete without any one sub-section because each sub-section is transformed all by itself in the internet. Simultaneously, the DNA sequence operation for each sub-section not only can be done respectively but also can be acted between each other.

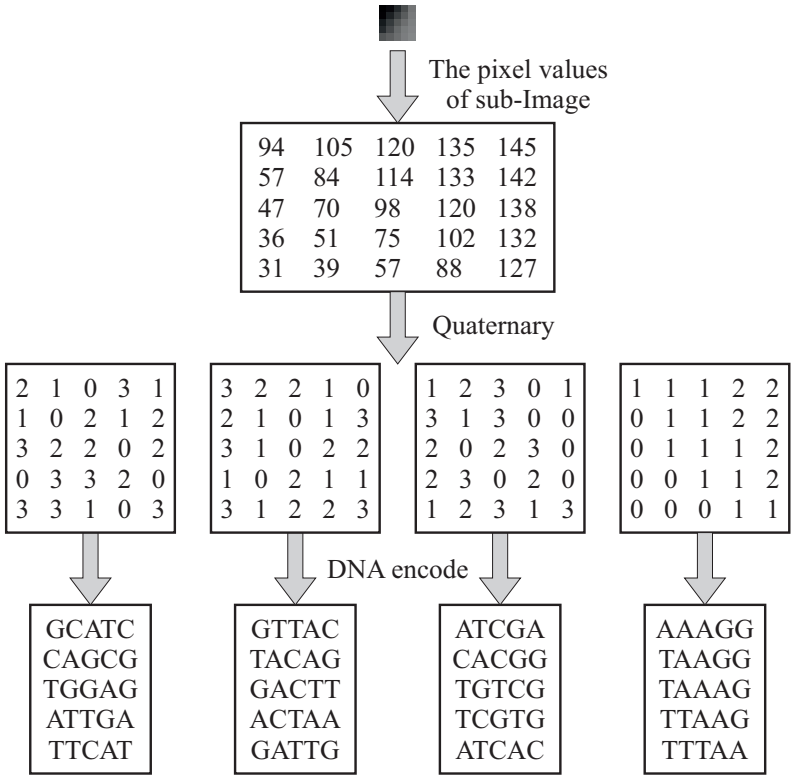

Fig. 2. The process of DNA encode

For example, we assume the first value of plain image is $X = 125$, and choose $n = 4$ in this paper in order to the module is zero after X through four times modular arithmetic. Four position integers $m_1 = 1$, $m_2 = 3$, $m_3 = 3$, $m_4 = 1$ are the results of formula (2), so the first value of each sub-section is m_1, m_2, m_3, m_4 separately and the value of X can be obtained by using (3) that $X = 125 = (((0 \times 4 + 1) \times 4 + 3) \times 4 + 3) \times 4 + 1$.

For the gray-scale image, four sub-sections whose pixel value is $0, 1, 2, 3$ can be obtained by using (2), which can be represented by four nucleic acid bases A (adenine), C (cytosine), G (guanine) and T (thymine). In this circumstance, there are 24 kinds of coding schemes satisfy the regulation, which are shown in Table 1. Therefore, a gray image can convert into four DNA sequence matrixes through split image into four sub-sections with the quaternary and DNA code which the corresponding DNA sequences of values from the four sub-sections are the results of the DNA coding by using the DNA encoding rules. The proposed image encryption transforms the statistical characteristics of plain image information drastically and randomly.

The process of DNA encode is shown in Fig. 2, where we can see the process of DNA encode as follows: we firstly get a sub-image whose size is 5×5 and the pixel values are from the plain image that the position is from $(208, 1)$ to $(212, 5)$. Then the sub-image is expanded to 25×25 and the new image is divided into 25 parts that the pixel values of each part are equal to the values of corresponding position from sub-image. Afterwards, we get the pixel values from sub-image and the values of the four sub-sections which can be gained by utilizing (2). Simultaneously, the DNA sequence matrixes as the results of DNA coding with the DNA encoding schemes. Similarly, the rest pixel values from the plain image could be operated through the above same way.

In this paper, we apply different rules in the DNA encoding process to encode the four sub-sections, and unique rules are employed to decode the four sub-sections in the DNA decoding procedure respectively. So each image can be scrambled and diffused separately.

Addition and subtraction operations for DNA sequences

Some biology operations and algebraic operations based on DNA sequence such as addition operation and subtraction operation have been advanced result from the fast development of DNA computing [29]. In this communication, we transform each pixel value into four integers whose value are from 1 to 4, so addition and subtraction operations for DNA sequences are performed according to the addition operation in the binary. In this way, 24 kinds of DNA addition rules and DNA subtraction rules are existed according to 24 kinds of DNA encoding schemes. For example, we can get a DNA sequence [CCTT] by using one type of addition operation shown in Table 2 to add

Table 1. Twenty-four kinds of encoding and decoding map rules of DNA sequence

	0	1	2	3
(1)	A	C	G	T
(2)	A	C	T	G
(3)	A	G	T	C
(4)	A	G	C	T
(5)	A	T	C	G
(6)	A	T	G	C
(7)	C	A	T	G
(8)	C	A	G	T
(9)	C	G	T	A
(10)	C	G	A	T
(11)	C	T	A	G
(12)	C	T	G	A
(13)	G	A	T	C
(14)	G	A	C	T
(15)	G	C	T	A
(16)	G	C	A	T
(17)	G	T	A	C
(18)	G	T	C	A
(19)	T	A	G	C
(20)	T	A	C	G
(21)	T	C	G	A
(22)	T	C	A	G
(23)	T	G	A	C
(24)	T	G	C	A

Table 2. Addition operation for DNA sequences

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

Table 3. Subtraction operation for DNA sequences

-	A	C	G	T
A	A	T	G	C
C	C	A	T	G
G	G	C	A	T
T	T	G	C	A

DNA sequences [AGCT] and [CTGA]. Otherwise, the sequence [AGCT] was obtained by subtracting the sequence [CTGA] from [CCTT] on the basis of DNA subtraction shown in Table 3.

3 THE PROPOSED IMAGE ENCRYPTION SCHEME

3.1 The basic theory of image encryption

In this section, we perform a detail study on the procedure of image encryption algorithm which composed of splicing model and hyper-chaotic system. Our proposed image encryption scheme includes five phase. First phase, plain image is dividing into four sub-sections whose pixel value is 0,1,2,3 by using quaternary. Afterward, each subsection is encoded into DNA sequences by utilizing DNA encode rules. Second phase, the position of pixel value from plain image has been changed by using chaotic sequences which are the outcomes of hyper-chaotic system with system parameters and initial values. For that result of DNA sequences are achieved by using DNA sequence addition operation to add these sub-sections. And then, DNA sequence is renovating into DNA sub-sequences by regarding a column of DNA sequence matrix as a subsequence and splicing operation are used to scramble them. At the time of decoding the DNA sequence matrixes are complemented and we get the encrypted image after combining the matrixes into one by using quaternary. The process of proposed image encryption algorithm is shown in Fig. 3.

In this paper, we use the rules of DNA addition operation and DNA subtraction operation which are shown in Tables 2 and 3 to scramble the pixel values of gray image in the procedure of encryption and decryption.

3.2 The generation of secret key

A secret key has been performed according to the following steps:

(1) First, we give the initial key "1234567890123456" and calculate the sum of pixel values from plain image which is denoted as *sumMatrix*.

(2) Then, the secret key can be gained by doing addition operation between the initial key and *sumMatrix*.

(3) Finally, the secret key is divided into four same parts which are the values of x_0, y_0, z_0, q_0 that are the initial conditions of hyper-chaotic map.

3.3 Details of the encryption process

According to Fig. 3, the details of the encryption process are described as follows.

Step 1: Divide plain image $A(m, n)$ into four subsections by using formula (2) and convert them into four matrices RA, RB, RC, RD whose size are (m, n);

Step 2: Encode the matrixes RA, RB, RC, RD into DNA sequence matrices EA, EB, EC, ED individually according to the encoding schemes of DNA sequence rule (1), rule (7), rule (13) and rule (19);

Step 3: Generate four chaotic sequences
$x = (x_1, x_2, \ldots, x_n)$, $y = (y_1, y_2, \ldots, y_n)$,
$z = (z_1, z_2, \ldots, z_n)$, $q = (q_1, q_2, \ldots, q_n)$, which are generated from Chen's hyper-chaotic system under the condition that initial values are x_0, y_0, z_0, q_0 and system parameters are a, b, c, d, k.

Step 4: Prepare the chaotic sequences

$$x, y, z, q$$

as follows:

$$\begin{aligned} [lx, fx] &= sort(x); \\ [ly, fy] &= sort(y); \\ [lz, fz] &= sort(z); \\ [lq, fq] &= sort(q); \end{aligned} \tag{4}$$

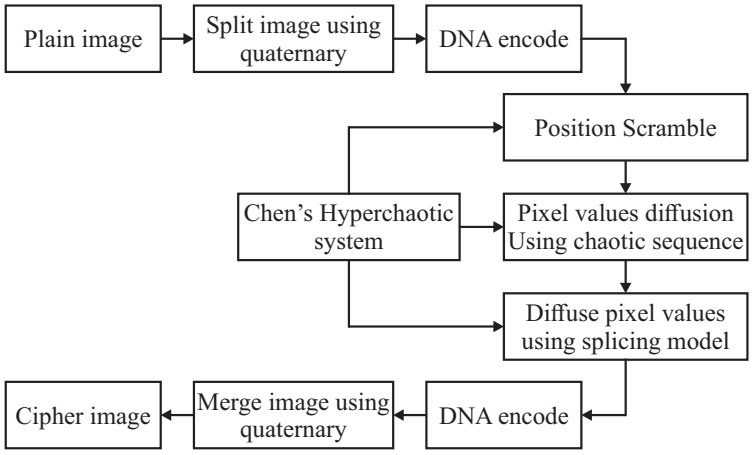

Fig. 3. Process of image encryption

where $[lx, fx] = sort(x)$ sorts the elements of x in ascending order, fx is the new sequence after ascending to x, lx is the index value of fx.

Select (x, y, z, q) to scramble EA, EB, EC, ED, according to

$$\begin{aligned} EA(i,j) &= EA(fx(i), fy(j)); \\ EB(i,j) &= EB(fy(i), fz(j)); \\ EC(i,j) &= EC(fz(i), fq(j)); \\ ED(i,j) &= ED(fq(i), fx(j)); \end{aligned} \tag{5}$$

where $i = 1, 2, \ldots, m$, $j = 1, 2, \ldots, n$, $EA(i,j)$,$EB(i,j)$, $EC(i,j)$, $ED(i,j)$ are the pixel value of the position (i,j) from EA, EB, EC, ED and we can get DNA sequence matrices CA, CB, CC, CD.

Step 5: Prepare the chaotic sequences x, y, z, q as Step 4.

According to DNA sequence addition operation, add CA, CB, CC, CD under the following method:

$$\begin{aligned} CA(i,j) &= CA(i,j) + CB(fx(i), fy(j)); \\ CB(i,j) &= CB(i,j) + SA(fy(i), fz(j)); \\ CC(i,j) &= CC(i,j) + SB(fz(i), fq(j)); \\ CD(i,j) &= CD(i,j) + SC(fq(i), fx(j)); \end{aligned} \tag{6}$$

where $i = 1, 2, \ldots, m$, $j = 1, 2, \ldots, n$ and we get DNA sequence matrices SA, SB, SC, SD.

Step 6: Four one-dimensional arrays MA, MB, MC, MD are obtained by treating a column of SA, SB, SC, SD as a sub-sequence. Scramble MA, MB, MC, MD by using the splicing operation according to

$$\begin{cases} MA\{i\} \leftrightarrow MB\{i\}, & \text{if } x(i) + y(i) < 1, \\ \text{no operation}, & \text{else.} \end{cases} \tag{7}$$

$$\begin{cases} MC\{i\} \leftrightarrow MD\{i\}, & \text{if } z(i) + q(i) < 1, \\ \text{no operation}, & \text{else.} \end{cases} \tag{8}$$

where $i = 1, 2, \ldots, m$; $j = 1, 2, \ldots, n$.

Step 7: Sequence matrices MA, MB, MC, MD are encrypted by using DNA decoding schemes rule (6), rule (12), rule (18), rule (24). Value matrices DA, DB, DC, DD are the results of decoding.

Step 8: Recombine these value matrixes by using formula (3), we get encrypted image.

The decryption algorithm is a reverse procedure of encryption, which the decrypted image is complemented according to contrary operation of above algorithm, where the only change is that the DNA sequence addition operation is replaced by DNA sequence subtraction operation in Step 5.

4 EXPERIMENT AND ANALYSIS

In this session, we discuss the results and consider the security of the proposed image encryption scheme. The security analyses include exhaustive attacks, statistical attacks and differential attacks which are studied to prove that the presented cryptosystem is robust enough to against most kinds of known attacks.

4.1 Exhaustive attacks

Key space

Key space is on behalf of the total number of different keys that are available in the image cipher. In this scheme, key ="1234567898253525" is used as secret key which consists of 128 bits. Therefore, the key space is $2^{128} \approx 3.4028 \times 10^{38}$ that is large enough to resist exhaustive attacks.

Key sensitivity

An ideal image encryption procedure has a large key space to make brute-force attacks infeasible, particularly should be sensitive to the secret keys. The key sensitivity can be tested by using different keys whose have a slight

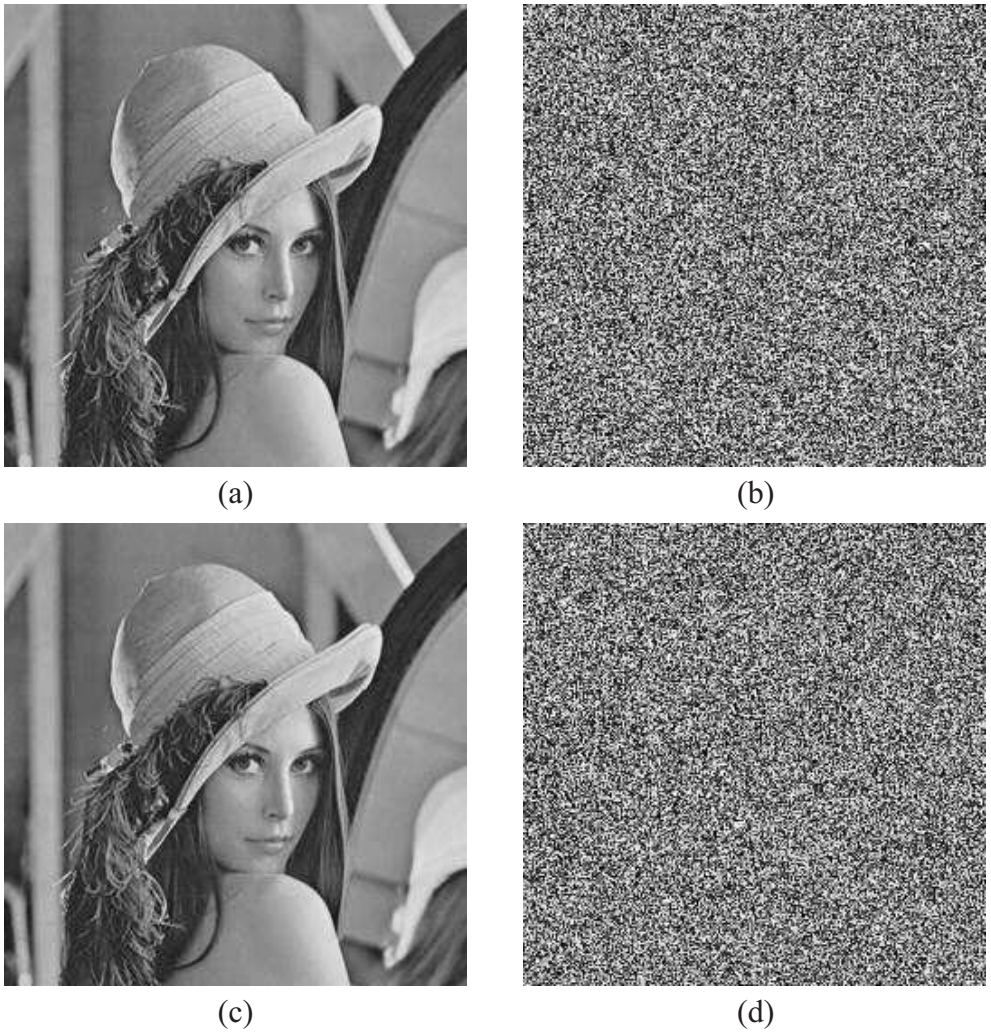

Fig. 4. The results of image encryption and decryption (a) — the plain image, (b) — the cipher image, (c) — the decrypted image with test key, (d) — the decrypted image with wrong key

difference because the Chen's chaotic system is quite sensitive to the initial values.

In this scheme, we use the test key "1234567898253525" to encrypt the plain image which is shown in Fig. 4(a), and the cipher image is shown in Fig. 4(b). Figure 4(c) shows the decrypted image with the correct secret key, Figure 4(d) shows the decrypted image under the worry key "1234567898253526" which is only one bit is different from the test key. This means that the plain image can't be obtained with the slightly different keys no matter that we change the test key a bit from the process of decryption. It is clear that our proposed algorithm is sensitive to the secret keys, and has the ability of resisting exhaustive attacks.

4.2 Statistical attacks

The gray histogram analysis

A gray histogram shows how pixels in an image are distributed by counting the number of pixels at gray intensity level, and the pixel values from cipher image of an ideal image cipher are scattering in the entire pixel value space. The gray scale histograms of plain image and cipher image are given in Figure 5. From Figure 5, we can conclude that the pixel values from plain image are concentrated on some values, while the pixel values from cipher image are very uniform. It illustrates that the proposed image encryption scheme influence the gray distribution, which can against the statistical attacks.

Correlation coefficient analysis

The correlation of adjacent pixels in the cipher image can demonstrate the level of diffusion and confusion which is necessary in the cipher system. As we all known, the image cipher is stronger with the less correlation of two adjacent pixels. The correlation coefficients in horizontal, vertical and diagonal are calculated to analyze the correlations of the adjacent pixels according to the following formulas

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

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

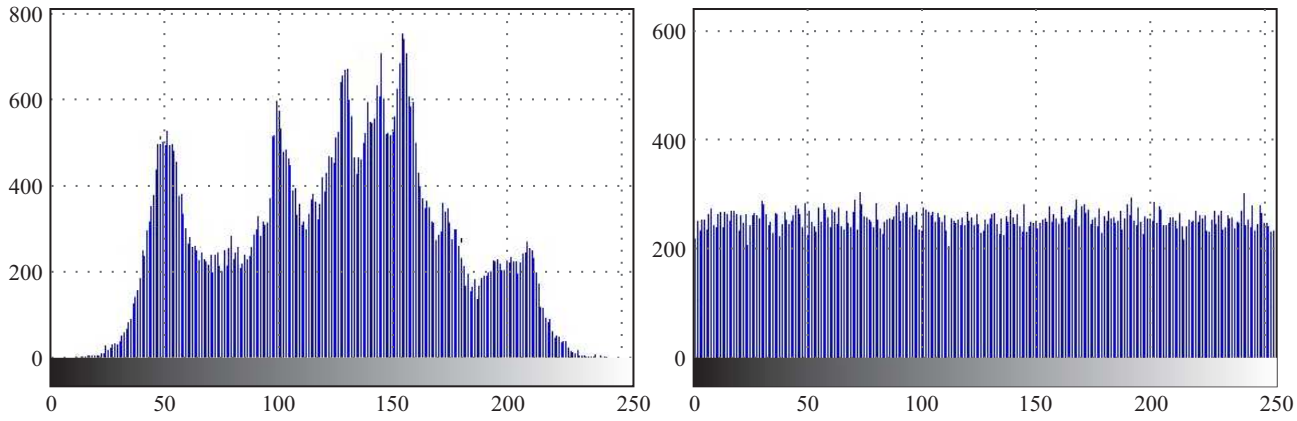

Fig. 5. The gray histogram of (a) — plain image, (b) — cipher image

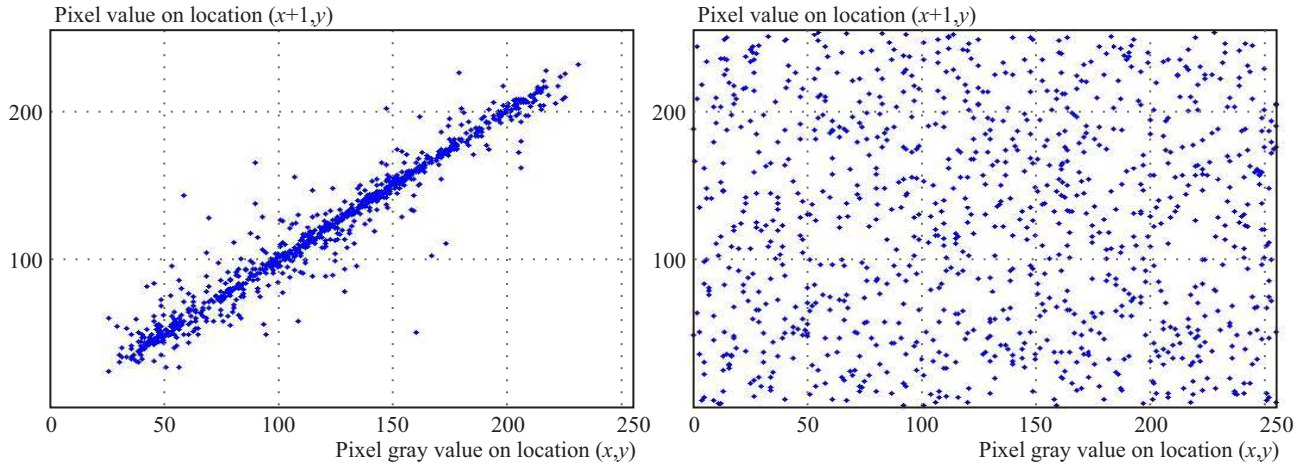

Fig. 6. Correlation of the horizontal in the (a) — plain image and (b) — cipher image

Table 4. Correlation coefficients of two adjacent pixels of the proposed cipher and other schemes

	Plain image			Cipher image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
This work	0.9721	0.9394	0.9159	0.0015	0.0018	0.0018
Ref.[11]	0.9831	0.9689	0.9671	0.0140	0.0092	0.0051
Ref.[16]	0.9707	0.9733	0.9122	0.0024	0.0012	0.0016
Ref.[17]	/	/	/	0.0026	0.0028	0.0036

Table 5. *NPCR* and *UACI* of our proposed cipher and other schemes

	This work	In Ref.[11]	In Ref.[17]
NPCR	99.5712 %	98.563 %	99.64 %
UACI	33.5053 %	33.0813 %	33.25 %

$$\operatorname{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}\big(x_i - E(x)\big)\big(y_i - E(y)\big)\,, \tag{11}$$

$$r_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)} \times \sqrt{D(y)}}\,, \tag{12}$$

where x and y are pixel values of the two adjacent pixels in the image, $E(x)$ is mean, $D(x)$ is variance, $\operatorname{cov}(x,y)$ is covariance.

We randomly select 1000 adjacent pixels from the same location of the plain image and the cipher image respectively in order to calculate the correlation coefficients of the adjacent pixels. The pixel distribution of the horizontal pixel value of images is shown in Fig. 6. Similarly, we run 10 times program for calculating correlation coeffi-

Table 6. The entropy analysis of the proposed cipher and other schemes

	This work	In Ref.[11]	In Ref.[16]
Information entropy	7.9971	7.9939	7.9970

cients of the adjacent pixels in horizontal, vertical and diagonal, and the average values are shown in Table 4.

Table 4 describes the correlation coefficients of two adjacent pixels of the proposed cipher and other schemes. Specially, The results of "lenna" from [16] and the analysis results of "lenna" whose size is 256×256 from [17] are employed to compare with our results. From Table 4, the correlation coefficients of the cipher image of our proposed cipher are close to 0, which far less than the original one. The results show that the presented algorithm has the ability to destroy the relativity effectively, and it is difficulty to obtain any valuable information by using statistical attacks.

4.3 Differential attacks

Generally, the intruder makes a slight change of the plain image, and observes the relationship between the plain image and the cipher image which is obtained by using the proposed algorithm to encrypt the plain image before and after changing. The differential attack of the proposed method is efficient and useful under the condition that one minor change in plain image can result in a great change in the cipher image.

Two common measures of *NPCR* and *UACI* were used to test the differential attack by researchers. The *NPCR* measures the percentage of different pixel numbers and *UACI* measures the average intensity of differences between two images. Assuming that the cipher image of plain image is "test1", the cipher image after changing one pixel value of plain image is "test2". Then we calculate the *NPCR* and *UACI* between "test1" and "test2" using the following formulas.

$$C(i,j) = \begin{cases} 0\,, & \text{if } T_1(i,j) = T_2(i,j)\,, \\ 1\,, & \text{if } T_1(i,j) \neq T_2(i,j)\,, \end{cases} \tag{13}$$

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} C(i,j)}{M \times N} \times 100\,\% \tag{14}$$

$$UACI = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} |T_1(i,j) - T_2(i,j)|}{255 \times M \times N} \times 100\,\% \tag{15}$$

where M and N are the width and height of "test1" or "test2". $T_1(i,j)$ and $T_2(i,j)$ is the pixel value at position (i,j) of "test1" and "test2". Table 5 shows the values of *NPCR* and *UACI* of our proposed cipher and other schemes. Specially, the analysis results of "lenna" whose size is 256×256 from [17] are employed to compare with our results. From Table 5, we can see that our proposed method is sensitive to slight change in the plaintext and can resist differential attack.

4.4 Information entropy

The information entropy is a measure of unpredictability of information content, which is defined as

$$H(X) = -\sum_{i=0}^{n} P(x_i) \log_2 P(x_i) \tag{16}$$

(16) where x_i is the ith gray value of gray image, $P(x_i)$ represents the emergency probability of message x_i, and n is the size of the image. Generally, the information entropy is 8 for an ideal method, and there exists security problem for an image whose information entropy is less than 8. Table 6 shows the information entropy of our encrypted image and other schemes. Specially, the result of "lenna" from [16] is employed to compare with our result. From Table 6, we notice that the value obtained of our scheme is very close to the theoretical value 8 than other schemes. Therefore, the proposed algorithm is difficult to break by entropy attack.

5 CONCLUSION

In this paper, an image encryption scheme based on splicing model and hyper-chaotic system has been introduced. The method on one hand considers the instinct characteristics of hyper-chaotic system and DNA computing, on the other hand employs the splicing model in the process of encrypt image. The image cipher enhances the encryption speed because the plain image is divided into four sub-sections by using quaternary. Simulation results and security analysis show that the proposed algorithm enhances the security and can resist most common attacks, which shows that our encryption technology has a good security.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (Nos. 61402066, 61402067, 61370005), the Basic Research Program of the Key Lab in Liaoning Province Educational Department (LZ2014049, LZ2015004), the Project Supported by Natural Science Foundation of Liaoning Province (No. 2014020132), the Project Supported by Scientific Research Fund of Liaoning Provincial Education (No. L2014499), and by the Program for Liaoning Key Lab of Intelligent Information Processing and Network Technology in University.

References

[1] KWOK, H. S.——TANG, WALLACE, K. S.: A Fast Image Encryption System based on Chaotic Maps with Finite Precision Representation, Chaos Solitons and Fractals **32** (2007), 1518–1529.

[2] GAO HAOJIANG—ZHANG YISHENG—LIANG SHUYUN—LI DEQUN: A New Chaotic Algorithm for Image Encryption, Chaos Solitons and Fractals **29** (2006), 393–399.

[3] LEIER, A.—RICHTER, C.—BANZHAF, W.—RAUHE, H.: Cryptography with DNA Binary Strands, BioSystems **57** (2000), 13–22.

[4] PAREEK, N. K.—PATIDAR, V.—SUD, K. K.: Image Encryption using Chaotic Logistic Map, Image and Vision Computing **24** (2006), 926–934.

[5] WEI XIAOPENG—GUO LING—ZHANG QIANG—ZHANG JIANXIN—LIAN SHIGUO: A Novel Color Image Encryption Algorithm based on DNA Sequence Operation and Hyper-Chaotic System, Journal of Systems and Software **85** (2012), 290–299.

[6] BABAEI, M.: A Novel Text and Image Encryption Method based on Chaos Theory and DNA Computing, Nat Computing **12** (2013), 101–107.

[7] ZHANG YUSHU—WEN WENYING—SU MOTING—LI MING: Cryptanalyzing a Novel Image Fusion Encryption Algorithm based on DNA Sequence Operation and Hyper-Chaotic System, Optik, **125** (2014), 1562–1564.

[8] MATTHEWS, R.: On the Derivation of a "Chaotic" Encryption Algorithm, Cryptologia **8** No. 1 (1989), 29–41.

[9] ALVAREZ, G.—SHUJUN LI: Cryptanalyzing a Nonlinear Chaotic Algorithm (NCA) for Image Encryption, Commun Nonlinear Sci Numer Simulat **14** (2009), 3743–3749.

[10] ARROYO, D.—SHUJUN LI—AMIGÓ, J. M.—ALVAREZ, G.—RHOUMA, R.: Comment on "Image Encryption with Chaotically Coupled Chaotic Maps", Physica D **239** (2010), 1002–1006.

[11] WANG XINGYUAN—WANG XIAOJUN—ZHAO JIANFENG—ZHANG ZHENFENG: Chaotic Encryption Algorithm based on Alternant of Stream Cipher and Block Cipher, Nonlinear Dynamics **63** (2011), 587–597.

[12] BELDHOUCHE, F.—QIDWAI, U.: Binary Image Encoding using 1D Chaotic Map, Proceedings of the IEEE Annual Technical Conference, 2003, pp. 39–43.

[13] SEYEDZADEH, S. M.—MIRZAKUCHAKI, S.: A Fast Color Image Encryption Algorithm based on Coupled Two-Dimensional Piecewise Chaotic Map, Signal Processing **92** (2012), 1202–1215.

[14] CHEN GUANRONG—MAO YAOBIN—CHUI, C. F.: A Symmetric Image Encryption Scheme based on 3D Chaotic Cat Maps, Chaos Solitons and Fractals **21** (2004), 749–761.

[15] GAO TIEGANG—CHEN ZENGQIANG: A New Image Encryption Algorithm based on Hyper-Chaos, Physics Letters A **372** (2008), 394–400.

[16] ZHANG QIANG—WEI XIAOPENG: A Novel Couple Images Encryption Algorithm based on DNA Subsequence Operation and Chaotic System, Optik **124** (2013), 6276–6281.

[17] WANG BIN—ZHENG XUEDONG—ZHOU SHIHUA—ZHOU CHANGJUN—WEI XIAOPENG—ZHANG QIANG—CHE CHAO: Encryption the Compressed Image by Chaotic Map Arithmetic Coding, Optik **125** (2014), 6117–6122.

[18] ANCHAL JAIN—NAVIN RAJPAL: Adaptive Key Length based Encryption Algorithm using DNA Approach, International Conference on Machine Intelligence Research and Advancement, 2013, pp. 140–144.

[19] RANU SONI—ARUN JOHAR—VISHAKHA SONI: An Encryption and Decryption Algorithm for Image based on DNA, 2013 International Conference on Communication Systems and Network Technologies, 2013, pp. 478–481.

[20] ZHOUSHIHUA, ZHANGQIANG, WEIXIAOPENG: Image Encryption Algorithm based on DNA Sequences for the Big Image, International Conference on Multimedia Information Networking and Security, 2010, pp. 884–888.

[21] ZHANG QIANG—GUO LING—WEI XIAOPENG: A Novel Image Fusion Encryption Algorithm based on DNA Sequence Operation and Hyper-Chaotic System, Optik **124** (2013), 3596–3600.

[22] SUKALYAN SOM—ATANU KOTAL—AYANTIKA CHATTERJEE—SOUMISTA DEY—SARBANI PALIT: A Colour Image Encryption Based On DNA Coding and Chaotic Sequences, International Conference on Emerging Trends and Applications in Computer Science, 2013, pp. 108–114.

[23] ZHOU CHANGJUN—WEI XIAOPENG—ZHANG QIANG—LIU RUI: DNA Sequence Splicing with Chaotic Maps for Image Encryption, Journal of Computational and Theoretical Nanoscience **7** (2010), 1–7.

[24] TOMHEAD: Splicing and Regularity, Bulletin of Mathematical Biology **49** (1987), 737.

[25] XU JIN—WANG SHUDONG—PAN LINQIANG: DNA Computing New Computing paradigms, Tsinghua University Press, 2004.

Received 3 September 2015

Hongye Niu was born in Shangdong, 1989. Currently, he is a student at Key Laboratory of Advanced Design and Intelligent Computing (Dalian University), Ministry of Education. His research interests include DNA Computing, Image encryption.

Changjun Zhou was born in Jiangxi, 1977. He received the PhD Degree in Dalian University of Technology, Dalian, in 2008. Currently, he is a Professor at Key Laboratory of Advanced Design and Intelligent Computing (Dalian University), Ministry of Education. His research interests include pattern recognition, artificial intelligence and computer animation.

Bin Wang was born in Dalian, 1983. He received the PhD Degree in Dalian University of Technology, Dalian, in 2013. Currently, he is a Lecture at Key Laboratory of Advanced Design and Intelligent Computing (Dalian University), Ministry of Education. His research interests include DNA computing, DNA coding, Image encryption, and Image watermarking.

Shihua Zhou was born in Dalian, 1982. She received the PhD Degree in Dalian University of Technology, Dalian, in 2013. Currently, she is a Lecture at Key Laboratory of Advanced Design and Intelligent Computing (Dalian University), Ministry of Education. Her research interests include DNA computing, DNA coding and Image encryption.

Xuedong Zheng was born in Liaoning, 1977. He received the PhD Degree in Huazhong University of Science and Technology, Wuhan, in 2010. Currently, he is a lecture at Key Laboratory of Advanced Design and Intelligent Computing (Dalian University), Ministry of Education. His research interests include DNA computing, artificial intelligence and coding theory.