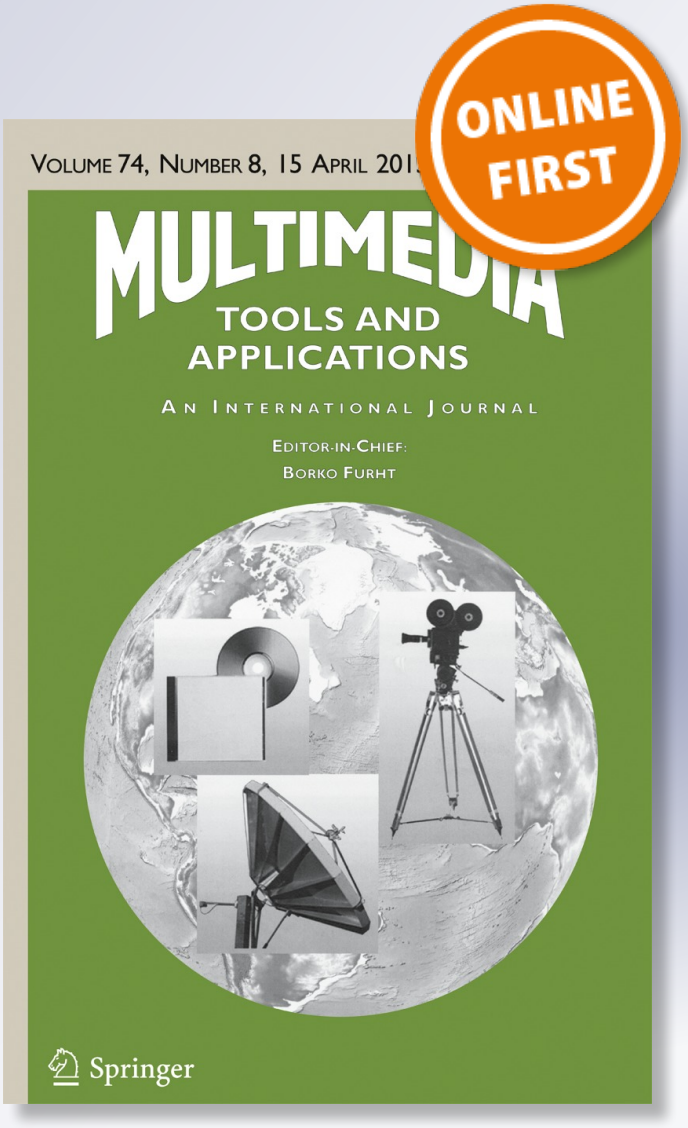
Chaos-based image encryption scheme combining DNA coding and entropy

Ping Zhen, Geng Zhao, Lequan Min & Xin Jin

Multimedia Tools and Applications
An International Journal

ISSN 1380-7501

Multimed Tools Appl
DOI 10.1007/s11042-015-2573-x



Springer

Multimed Tools Appl
DOI 10.1007/s11042-015-2573-x

Chaos-based image encryption scheme combining DNA coding and entropy

Ping Zhen[1] · Geng Zhao[2] · Lequan Min[1] · Xin Jin[2]

Received: 10 August 2014 / Revised: 26 January 2015 / Accepted: 19 March 2015

Abstract Information security has became more and more important issue in modern society, one of which is the digital image protection. In this paper, a secure image encryption scheme based on logistic and spatiotemporal chaotic systems is proposed. The extreme sensitivity of chaotic system can greatly increase the complexity of the proposed scheme. Further more, the scheme also takes advantage of DNA coding and eight DNA coding rules are mixed to enhance the efficiency of image confusion and diffusion. To resist the chosen-plaintext attack, information entropy of DNA coded image is modulated as the parameter of spatiotemporal chaotic system, which can also guarantee the sensitivity of plain image in the encryption process. So even a slight change in plain image can cause the complete change in cipher image. The experimental analysis shows that it can resistant different attacks, such as the brute-force attack, statistical attack and differential attack. What's more, The image encryption scheme can be easily implemented by software and is promising in practical application.

Keywords Image encryption · Spatiotemporal chaotic system · DNA encoding · Information entropy

✉ Ping Zhen
zhenping1989@126.com

Geng Zhao
zg@besti.edu.cn

Lequan Min
minlequan@sina.com

✉ Xin Jin
jinxin@besti.edu.cn

[1] School of Automation and Electrical Engineering, University of Science and Technology Beijing, Beijing, 100083, China

[2] Beijing Electronic Science and Technology Institute, Beijing, 100070, China

Published online: 10 April 2015

1 Introduction

With the development of communication technology, transmission of digital images via the Internet has become more and more popular. However, this exposes the digital images to serious threats in the transmission process. Different from text encryption techniques, image has some special characteristics, such as bulk data capacity and high correlation among pixels. Traditional encryption algorithms, such as Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA) and Advanced Encryption Standard (AES), etc., are not suitable for image encryption. So it is necessary to design new image encryption schemes.

The particular properties of chaos [3, 6], such as sensitivity to initial conditions and system parameters, pseudo-randomness, ergodicity and so on, have granted chaotic dynamics as a promising alternative for the conventional cryptographic algorithms. The inherent properties connect it directly with cryptographic characteristics of confusion and diffusion, which is presented in Shannon's works [1]. Spatiotemporal chaotic system has been widely used in chaotic cryptography [7, 12] in recent years for its excellent chaotic dynamic properties, which could maintain longer periodicity in digitalization and gain good performance in cryptography. Moreover, it could be implemented in parallel by hardware, and has larger key space. Thus, it is also suitable for image encryption [15, 16].

Due to massive parallelism, huge storage, ultra-low power consumption and the massive research on DNA computing [17], DNA cryptography emerged as a new cryptographic field [17, 19, 20]. Recently, DNA-based image encryption has become more and more popular [8, 9, 14, 18, 21]. DNA-based image encryption is generally categorized into two phases: firstly, using DNA theory to encode plain image pixels into DNA sequence. Then a gray pixel value is decomposed into four DNA elements, which can increase the efficiency of image confusion and diffusion. Secondly, the encoded plain image pixels generate a key image based on DNA operation rules and form the cipher image. Zhang et al. [21] presented an image encryption scheme based on DNA sequence addition operation, which was soon analyzed to be invertible and insecure against chosen-plaintext attack [2]. The authors in [22] found that the encryption algorithm proposed in [23] can be broken by choosing the maximum number of $\lceil (m + 4n - 2)/3 \rceil + 1$ plain images, where m and n are the width and height of the plain image. In [11], a RGB image encryption algorithm based on DNA encoding and chaos map was proposed. However, its encryption results are not sensitive with respect to change of the plain image and secret key. Furthermore, the equivalent secret key of the encryption algorithm can be reconstructed as analyzed in [10, 13].

According to the deficiencies of image encryption scheme [11, 21, 23], we have formulated some rules to design secure image encryption scheme as follows:

(1) Cipher image should be sensitive with the changes of the secret key and plain images.
(2) Structural security of image encryption scheme is quite important. Some structural weakness may reveal the equivalent keys instead of searching for secret keys directly.
(3) High-dimensional chaotic system is more reliable to design secure image encryption scheme because of its high complexity. Some cryptosystems, which are based on a low-dimensional chaotic map, have obvious drawbacks, such as short period and small key space.
(4) Secret keys or other secret information should be relevant to the plaintext or ciphertext, which can be necessary to resist chosen-plaintext attack.

Based on these rules, we design a novel image encryption scheme, which utilizes chaotic system, DNA encoding and information entropy. In the proposed scheme, logistic system is iterated to generate the DNA matrix and the image encoding rules. Then the generated DNA matrix performs the DNA addition operation with encoded image. To increase of sensitivity, information entropy of additive DNA image is diffused through the iteration of logistic system, which is used to modulate the parameter of spatiotemporal system and can speed up both the confusion and diffusion process. The adoption of information entropy can cause a 64-bit ciphertext expansion in order to decrypt the cipher image, but it has little influence on the performance of the proposed scheme. Experiment analysis shows that the image encryption scheme can resist various attacks and is suitable for practical image encryption.

This paper is arranged as follows. In Section 2, a brief description of spatiotemporal chaotic system and DNA encoding is introduced. The details of the proposed image encryption and decryption process are described in Sections 3 and 4, respectively. In Section 5, the simulation results are presented. Security and performance analysis will be discussed in Section 6. The last Section presents the conclusions.

2 Preliminaries

2.1 Spatiotemporal chaotic system

The spatiotemporal chaotic system used in our scheme is the typical coupled map lattice(CML). Compared with simple chaotic maps, spatiotemporal chaotic system possesses two additional merits for cryptographic purposes. First, the period is much longer so that the short period problem is practically avoided. Second, the system is high-dimensional and has a number of positive Lyapunov exponents that guarantee the complex dynamical behavior or pseudorandomness. Therefore, it is more impossible to predict the time series generated by this kind of chaotic systems. The CML-based spatiotemporal chaotic system introduced by Kaneko [5] is described as

$$x_{n+1}(i) = (1-\varepsilon) f(x_n(i), u) + \frac{\varepsilon}{2}[f(x_n(i+1), u) + f(x_n(i-1), u)] \tag{1}$$

$$f(x, u) = ux(1-x) \tag{2}$$

where $i = 1, 2, \ldots, N$, N is the number of lattices. $f(x, u)$ is the logistic chaotic map, and $u \in [3.56995, 4]$ is the parameter. ε is the coupling parameter. The periodic boundary condition, i.e., $x_n(j) = x_n(N + j)$ for any valid j, is used in the CML. To balance the complexity and efficiency, N is set to be 3 in the proposed image encryption scheme.

2.2 DNA coding

DNA (Deoxyribonucleic acid) is a molecule that encodes the genetic instructions used in the development and functioning of all known living organisms and many viruses, and it has become indispensable for basic biological research. There are four different nucleic acids in a DNA sequence: A (adenine), T (thymine), C (cytosine), and G (guanine). It can be concluded that A and T are complementary, as well as G and C, according to Watson-Crick base pairing rules [23].

In the binary system, 0 and 1 are complementary. Therefore, it can be inferred that 00(0) and 11(3) are complementary, as well as 01(1) and 10(2). These eight encoding and decoding rules [10] for the DNA sequence are listed in Table 1.

With the development of DNA computing, some algebraic operators are essential. Tables 2 and 3 describe DNA addition and subtraction operation, respectively. The addition and subtraction operation can be properly used for image encryption.

3 The proposed image encryption scheme

This section will present the details about the image encryption scheme, which combines the advantages of spatiotemporal chaotic system and DNA encoding. The process of the encryption process is shown in Fig. 1. It consists of five parts:

(1) Generate the secret key

The secret key includes initial value and parameters of logistic chaotic system (x_0^l, u_0^l), initial value and coupling parameter of spatiotemporal chaotic system $(x_0^s(i), \varepsilon)$, $1 \leq i \leq 3$. The parameter of spatiotemporal chaotic system u^s is derived from information entropy of the image.

(2) Image DNA encoding and substitution

Input the 8-bit gray image I_{input} of size $m \times n$. The gray value of each pixel is v_i, $i = 1, 2, \ldots, mn$. Each $v_i \in \{0, 1, \cdots, 255\}$ can be decomposed into four elements by:

$$v_i = \sum_{k=0}^{3} v_i^{4-k} \cdot 4^k, v_i^k \in \{0, 1, 2, 3\} \tag{3}$$

In this way, convert I_{input} into matrix I' of the size $m \times 4n$. Then iterate the logistic chaotic map (2) with the initial value x_0^l and parameter u_0^l to get the sequence:

$$L_1 = \{x_1, x_2, \cdots, x_{4n}\}$$

Convert L_1 into DNA sequence

$$L_1' = \{d_{1,1}, d_{1,2}, \cdots, d_{1,4n}\}$$

by computing:

$$l_i = \lfloor x_i \times 2^8 \rfloor \mod 4 \tag{4}$$

$$d = \begin{cases} A \ if \ l_i = 0 \\ C \ if \ l_i = 1 \\ G \ if \ l_i = 2 \\ T \ if \ l_i = 3 \end{cases} \tag{5}$$

Table 1 Eight DNA encoding and decoding rules

0	1	2	3	4	5	6	7
A−00	A−00	C−00	C−00	G−00	G−00	T−00	T−00
C−01	G−01	A−01	T−01	A−01	T−01	C−01	G−01
G−10	C−10	T−10	A−10	T−10	A−10	G−10	C−10
T−11	T−11	G−11	G−11	C−11	C−11	A−11	A−11

Table 2 DNA addition operation

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

where $\lfloor x \rfloor$ takes the largest integer less or equal than x. Compute $e_1 = \lfloor x_{4n} \times 2^8 \rfloor \mod 8$ and choose the DNA encoding rule e_1 to encode the elements in the first row of I'. Continue iterating the logistic chaotic map to get the sequence:

$$L_2 = \{x_{4n+1}, x_{4n+2}, \cdots, x_{8n}\}.$$

According to the (4, 5), encode L_2 into DNA sequence

$$L_2' = \{d_{2,1}, d_{2,2}, \cdots, x_{2,4n}\}.$$

Compute $e_2 = \lfloor x_{8n} \times 2^8 \rfloor \mod 8$. For the elements in the second row of I', choose the DNA encoding method e_2.

Continue doing like the above steps, until all the m rows in I' are encoded. Then perform the DNA addition to get the DNA matrix I_{DNA} of size $m \times 4n$ by:

$$I_{DNA} = I' + L' \tag{6}$$

(3) Image entropy computation

Compute the information entropy H of I_{DNA} by:

$$H = \sum_{i \in \{A,T,G,C\}} p(i) \log_2 \frac{1}{p(i)} \tag{7}$$

where $p(i)$ is the occurrence probability of i in I_{DNA}. Then compute:

$$x_0^H = \begin{cases} H - \lfloor H \rfloor & if\ H - \lfloor H \rfloor \neq 0 \\ x_0^l & if\ H - \lfloor H \rfloor = 0 \end{cases} \tag{8}$$

Table 3 DNA subtraction operation

−	A	C	G	T
A	C	A	T	G
C	G	C	A	T
G	T	G	C	A
T	A	T	G	C

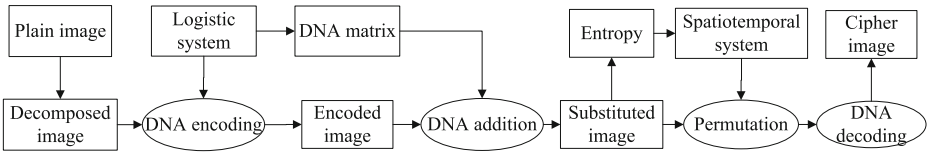


Fig. 1 Block diagram for image encryption process

x_0^H is regarded as initial value of logistic chaotic map and iterate the logistic map with the parameter u^l to get x_{20}^H. Convert decimal x_{20}^H into 64-bit binary sequence H_{binary} as follows:

$$H_{binary} = Dec2Bin\left(x_{20}^H, 64\right) \tag{9}$$

Inversely, convert the binary sequences H_{binary} into decimal $H_{decimal}$ as follows:

$$H_{decimal} = Bin2Dec(H_{binary}) \tag{10}$$

It should be noticed that $H_{decimal}$ may not be equal to x_{20}^H because of the influence of finite computer precision. Iterate the logistic chaotic map with the initial value x_0^l and parameter u_l to get sequence x_{10}^l. Compute

$$H_{cipher} = Dec2Bin\left(x_{10}^l, 64\right) \oplus H_{binary} \tag{11}$$

where $\oplus$ denotes the exclusive or operation, H_{cipher} is regarded as the ciphertext of the entropy.

(4) Image permutation

Compute

$$u^s = 3.75 + 0.25H_{decimal} \tag{12}$$

Iterate the spatiotemporal chaotic map as shown in (1) with the initial value $x_0^s(i), i \in \{1, 2, 3\}$, coupling parameter ε and u^s to get the sequence:

$$R = \{x(1)_1, x(1)_2, \cdots, x(1)_m\}, \quad C = \{x(3)_1, x(3)_2, \cdots, x(3)_{4n}\}$$

Sort R and C in ascending order:

$$R' = \{x(1)'_1, x(1)'_2, \cdots, x(1)'_m\}, \quad Ind_R = \{i_1, i_2, \cdots, i_m\}, \quad x(1)_{i_k} = x(1)'_k$$

$$C' = \{x(3)'_1, x(3)'_2, \cdots, x(3)'_{4n}\}, \quad Ind_R = \{j_1, j_2, \cdots, j_{4n}, \quad x(3)_{j_k} = x(3)'_k$$

According to Ind_R and Ind_C, permute the rows and columns of I_{DNA} by:

$$I'_{DNA}(i, j) = I_{DNA}(Ind_R(i), Ind_C(j)) \tag{13}$$

where $i = 1, 2, \cdots, n, \ \ j = 1, 2, \cdots, 4n$.

(5) Image decoding

According to the first decoding rule in Table 1, decode the DNA matrix I'_{DNA} into the cipher image I_{cipher}. (H_{cipher}, I_{cipher}) is the final ciphertext.

4 Image decryption algorithm

The decryption process is the simple reversion of the above encryption, which is shown in Fig. 2. We will introduce it briefly.

(1) Choose the first DNA encoding rule to encode the cipher image I_{cipher} and get I'_{DNA}.

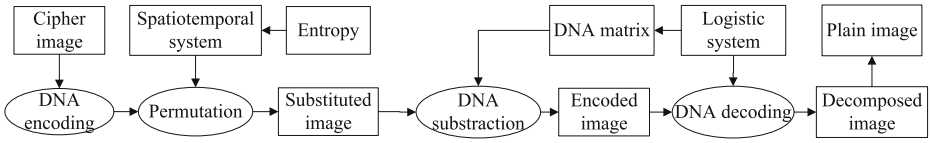


Fig. 2 Block diagram for image decryption process

(2) According to the secret key, iterate the logistic chaotic map and decrypt entropy ciphertext to get $H_{decimal}$.
(3) Iterate the spatiotemporal chaotic map and execute the reverse permutation to get I_{DNA}.
(4) Iterate the logistic map to generate the corresponding sequence, reverse the substitution by DNA subtraction, and decode the DNA image from the first row to the last and get I'.
(5) By (3), it is very convenient to recover the plain image I_{input} from I'.

5 Simulation result

To analyze the performance of image encryption scheme, we implement the algorithm by Matlab 7.14, with the secret key

$$\{x_0^l = 0.437, u^l = 0.785, x_0^s = (0.364, 0.785, 0.293), \varepsilon = 0.2582\}.$$

The "Lena", "black" and color "peppers" images are used as the plain image. The corresponding cipher images and decrypted images are as in Fig. 3. For the color image, the three channels of red, green and blue, are encrypted separately. From the cipher image Fig. 3(b), (e), (h), we can see that the simulation result is quite satisfactory.

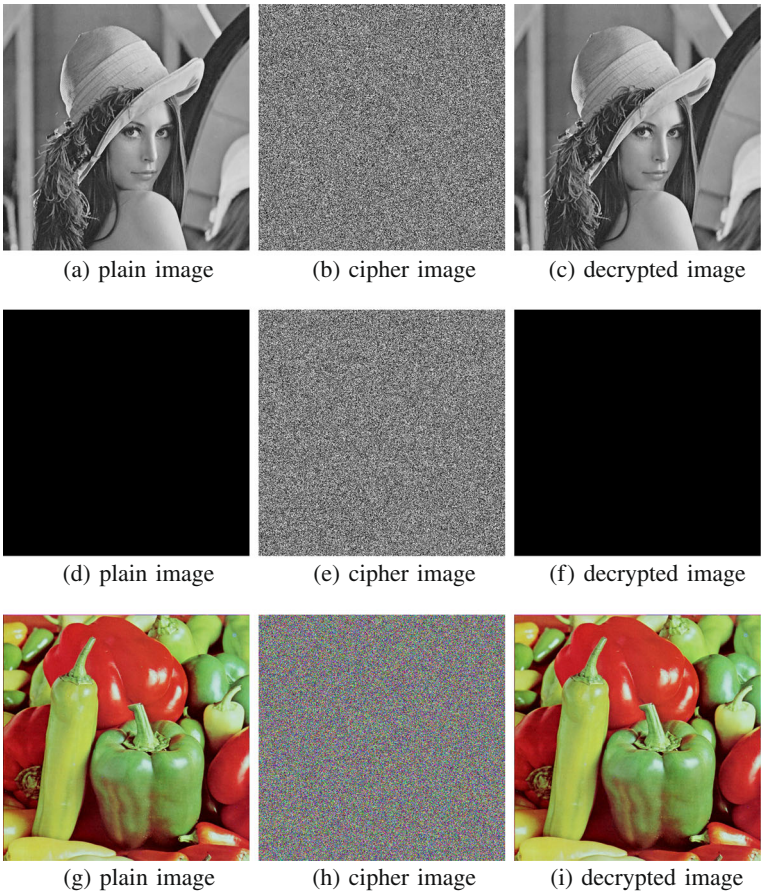
6 Security and performance analysis

A well designed image encryption scheme should be robust against different kinds of attacks, such as brute-force attack, statistical attack, differential attack, and chosen-plaintext attack [15]. In this section, we will analyze the security of the proposed encryption scheme.

6.1 Resistance to the brute-force attack

6.1.1 Key space

The key space of the image encryption scheme should be large enough to resist the brute-force attack, otherwise it will be broken by exhaustive search to get the secret key in a limited amount of time. In the encryption scheme, $\{x_0^l, u^l, x_0^s, \varepsilon\}$ is the secret key and x_0^s consists of three initial values, where $x_0^l, x_0^s, \varepsilon \in (0, 1)$, $u^l \in (3.56995, 4)$. The precision of 64-bit double data is 10^{-15}, so the key space is about $10^{15} \times 10^{14} \times (10^{15})^3 \times 10^{15} = 10^{89} \approx 2^{295}$, which is larger than the max key space (2^{256}) of practical symmetric encryption of AES [4]. So it is large enough to resist brute-force attack.



(a) plain image (b) cipher image (c) decrypted image

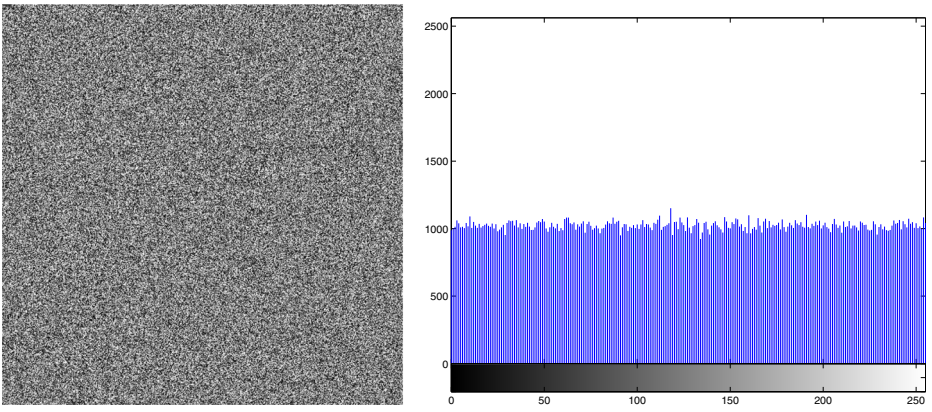
(d) plain image (e) cipher image (f) decrypted image

(g) plain image (h) cipher image (i) decrypted image

Fig. 3 The plain image, cipher image and corresponding decrypted image of "Lena"(**a**-**c**), "black"(**d**-**f**) and "peppers"(**g**-**i**), respectively

6.1.2 Sensitivity of secret key

The logistic and spatiotemporal chaotic system are extremely sensitive to the system parameter and initial value. A light difference can lead to the decryption failure. To test the secret key sensitivity of the image encryption scheme, we change the secret key x_0^l from 0.437 to 0.437000000000001 to decrypt the "Lena" cipher image in Fig. 3(b), while the other secret key $(u^l, x_0^s, \varepsilon)$ remains the same. The decryption result and its corresponding histogram are shown in Fig. 4. We can see that the decrypted image is completely different from the original "Lena" image and its histogram is quite flat. The test results of the other secret key $(u^l, x_0^s, \varepsilon)$ are similar. The experiment shows that the image encryption scheme is quite sensitive to the secret key , which also indicates the strong ability to resist exhaustive attack.



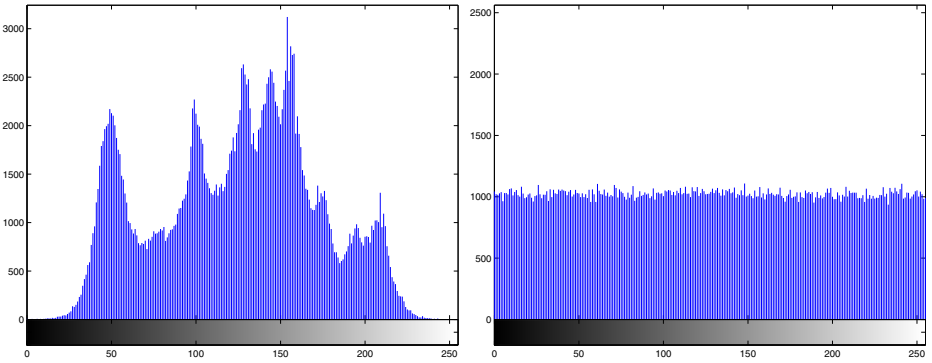
(a) (b)

Fig. 4 The sensitivity to the secret key: (**a**)The decryption result of "Lena" image when x_0^l is changed from 0.437 to 0.437000000000001; (**b**) The histogram of incorrectly decrypted image

6.2 Resistance to the statistic attack

6.2.1 The gray histogram analysis

The histogram is used to show the distribution of pixel values of a gray image. The histogram of cipher image should be flat enough, otherwise some information can be leaked to cause the statistical attack. This makes cipher-only attack possible through analyzing the statistic property of the cipher image. Figure 5. shows the gray-scale histograms of the "Lena" image and its corresponding cipher image, respectively. Comparing the two histograms we can see that the pixel values of the original "Lena" image are concentrated on



(a) (b)

Fig. 5 The gray histogram analysis: (**a**) The gray histogram of the original "Lena" image; (**b**) The gray histogram of its cipher image

some values, but the histogram of its cipher image is very uniform, which makes statistical attacks impossible.

6.2.2 Information entropy

The information entropy [1] is used to express randomness and can measure the distribution of gray values in the image. The more uniform the distribution of pixel gray values, the greater the information entropy is. It is defined as follows:

$$H(m) = -\sum_{i=0}^{L} P(m_i) \log_2 P(m_i) \tag{14}$$

where m_i is the i-th gray value for an L level gray image, $L = 255$. $P(m_i)$ is the probability of m_i in the image and $\sum_{i=1}^{L} P(m_i) = 1$. The information entropy of an ideal random image is 8, which shows that the information is completely random. The information entropy of the cipher image should be close to 8 after encryption. The closer it is to 8, the smaller possibility for the scheme leaks information. We compute the information entropy of "Lena" cipher image $H(m) = 7.9993$, which is very close to 8. It can be seen that the proposed image encryption scheme hardly leaks any information.

6.2.3 The correlation analysis

Correlation indicates the linear relationship between two random variables. In image processing, it is usually employed to investigate the relationship between two adjacent pixels. Usually, the correlation of between adjacent pixels in the plain image is very high. A good encryption scheme should reduce the correlation between adjacent pixels, i.e., the less correlation of two adjacent pixels have, the safer the cipher image is. In order to test the correlation of two adjacent pixels, we randomly select 2000 pairs (horizontal, vertical and diagonal) of adjacent pixels from the original "Lena" image and its corresponding cipher image. Using the following formulas for the correlation computation.

$$r_{xy} = \frac{cov(x, y)}{\sqrt{D(x)} \times \sqrt{D(y)}} \tag{15}$$

$$cov(x, y) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)) \tag{16}$$

$$D(x) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))^2 \tag{17}$$

$$E(x) = \frac{1}{N} \sum_{i=1}^{N} x_i \tag{18}$$

The computation results are shown in the Table 4. It shows that there is strong correlation between adjacent pixels of each direction in original "Lena" image since the correlation coefficients are all close to 1 while the correlation coefficients of the adjacent pixels in the cipher image are very small, which are close to 0. So the image encryption scheme can greatly reduce the correlation of the cipher image.

For the graphical display, Fig. 6(a)–(c)show the strong correlation of (horizontal, vertical and diagonal) adjacent pixels in the original "Lena" image since most dots are distributed along the diagonal and Fig. 6(d)–(f) show that the correlation of adjacent pixels in the

Table 4 Correlation coefficients of the original "Lena" image and its cipher image

	Horizontal	Vertical	Diagonal
Original image	0.9794	0.9646	0.9535
Cipher image	0.0214	0.0465	−0.0090

corresponding cipher image is greatly reduced since the dots are distributed in the entire plane.

6.3 Resistance to differential attack

Differential attack means that attacker makes a slight change to the original image, and use the proposed image encryption scheme to encrypt for the original image before and after changing, to find out the relationship between the original image and the cipher image through comparing two cipher images. Researchers usually adopt NPCR (number of pixels change rate) and UACI (unified average change intensity) as two criterions to examine the performance of resisting differential attack. The following equations are used to compute NPCR and UACI:

$$C(i,j) = \begin{cases} 0 \ if \ P_1(i,j) = P_2(i,j) \\ 1 \ if \ P_1(i,j) \neq P_2(i,j) \end{cases} \tag{19}$$

$$NPCR = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} C(i,j)}{M \times N} \times 100\,\% \tag{20}$$

$$UACI = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} |P_1(i,j) - P_2(i,j)|}{255 \times M \times N} \times 100\,\% \tag{21}$$

where M and N are the height and width of the image, $P_1(i,j)$ and $P_2(i,j)$ denote the pixel gray value of two cipher images in the same position. The closer the NPCR gets to 100 %, the more sensitive the cryptosystem is to the original image, and the more effective the cryptosystem resists differential attack. The greater the UACI is, the better the cryptosystem resists the differential attack. For the 512 × 512 "Lena" image, we choose five pixel from the position of four corners and middle, and then change the pixel gray values to calculate the NPCR and UACI, respectively. From the result in Table 5, the NPCR is very close to 100 % and UACI is about 33 %, which demonstrates that the proposed image encryption scheme has a strong ability to resist differential attack.

6.4 Resistance to chosen-plaintext attack

In the image encryption scheme, we utilize image information entropy to avoid chosen-plaintext attack existing in [2, 23]. The entropy is computed after the original image

Table 5 NPCR and UACI when pixel value changed in different position

Position	Original pixel	Changed pixel	NPCR	UACI
(1,1)	164	165	99.61 %	33.51 %
(1,512)	131	132	99.60 %	33.41 %
(256,256)	94	95	99.58 %	33.44 %
(512,1)	47	48	99.60 %	33.38 %
(512,512)	108	109	99.60 %	33.45 %

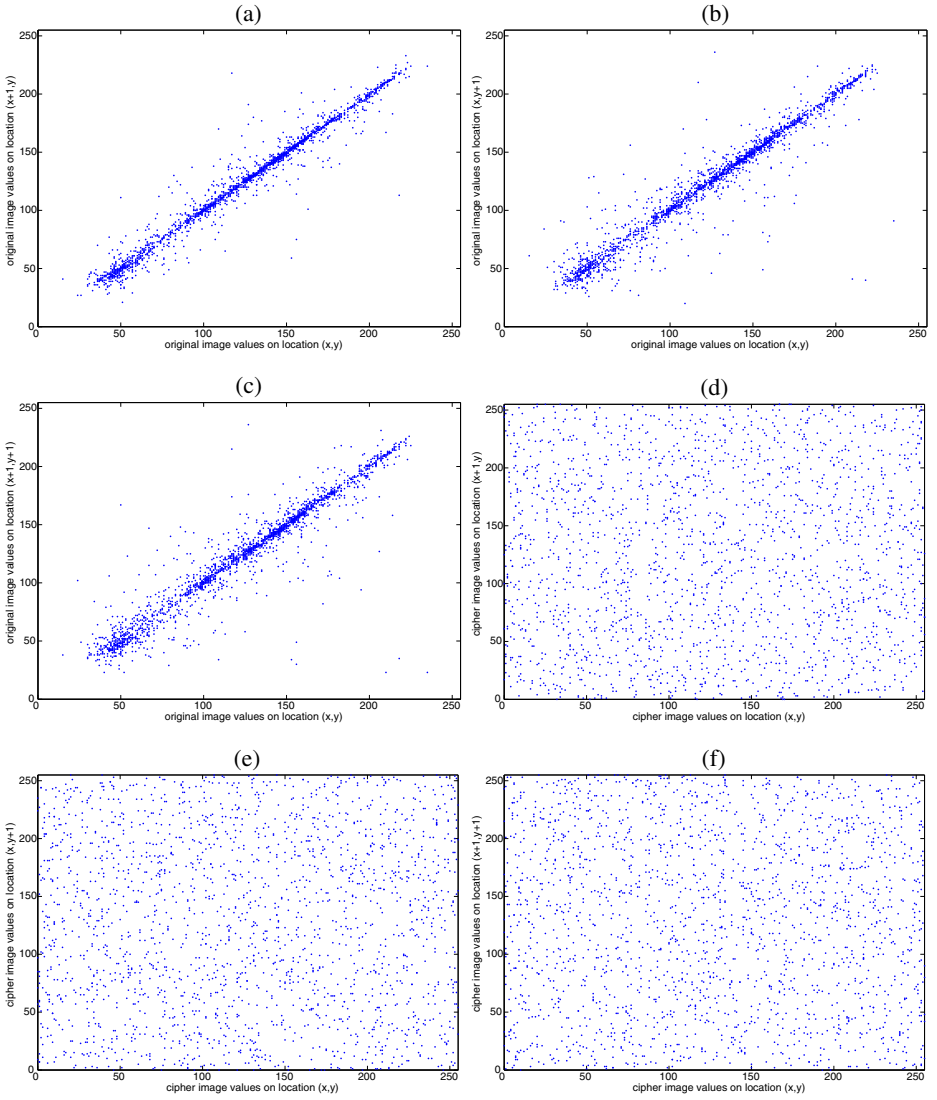


Fig. 6 Correlation analysis: (**a**)-(**c**)correlation among horizontally, vertically, and diagonally adjacent pixels of the original image "Lena"; (**d**)-(**f**)correlation among horizontally, vertically, and diagonally adjacent pixels of its cipher image

processed by DNA encoding and DNA addition. According to (7), the entropy is determined both by the original image and secret key. Then the information entropy is diffused to influence the entire cipher image through the sensitivity of logistic and spatiotemporal chaotic system. From the differential attack test, we can see that even a slight change in plain image can cause a huge change in the cipher image, which satisfies good encryption result. However, the entropy information $H_{decimal}$ is also needed to decrypt cipher image, which can cause a 64-bit ciphertext expansion. In order to avoid being leaked, it is encrypted by exclusive or operation in (11). Even if the entropy information is cracked by brute-force attack,

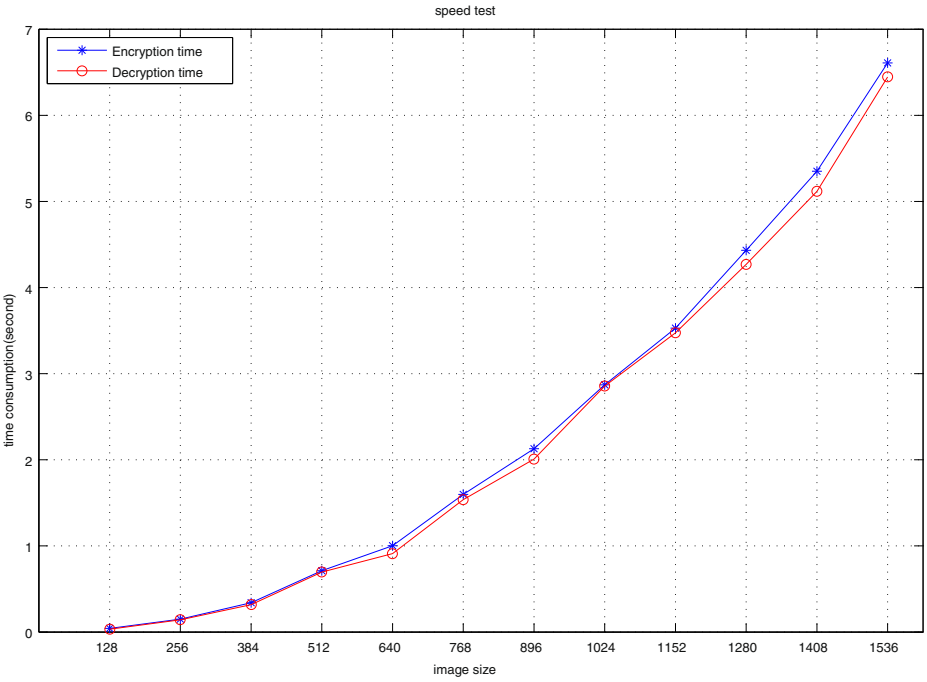


Fig. 7 Image encryption scheme speed test

the attacker still cannot launch any attacks without secret key. The measure can prevent the image encryption scheme from chosen-plaintext attack effectively.

6.5 Image encryption scheme speed test

The image encryption scheme is implemented by Matlab on personal computer with Intel i7-3667U processor and 4.00G RAM. The encryption and decryption consumption time is recorded for the images of different size. The result is shown in Fig. 7.

From Fig. 7, we can see that the larger size of the image, the more time it needs for encryption and decryption. For a general size of image, for example, with the size of 512×512, it consumes less than one second to encryption or decryption. When transplanted to other implement environment, like C/C++, the speed can be much faster, which can satisfy practical demand.

6.6 Comparison with other methods

In this section, we compare statistical performance with three other related image encryption schemes proposed in recent years, namely, Refs. [14, 21, 23].

The statistical results are based on “Lena” image, which are listed in Table 6. From the table, we can see that the information entropy value of the four schemes are all very close to 8, which can guarantee no information leak of cipher image. For the correlation analysis in horizontal, vertical and diagonal direction, the value of our scheme is slightly bigger, but it has little influence since they are all extremely close 0, which show uniform distribution of

Table 6 The performance comparsion of the proposed scheme with other methods

		Ref. [21]	Ref. [23]	Ref. [14]	Our scheme
Information entropy		7.9980	7.9968	7.9992	7.9993
Correlation analysis	Horizontal	0.0036	0.0012	0.0058	0.0214
	Vertical	0.0023	0.0026	0.0022	0.0465
	Diagonal	0.0039	0.0021	0.0031	−0.0090
Differential analysis	NPCR	99.61 %	–	99.71 %	99.60 %
	UACI	38 %	–	33.63 %	33.44 %

cipher image. Compared to Refs. [14, 21, 23], the UACI value of our scheme is more close to the ideal value 33.33 %.

However, Refs. [21, 23] have already been analyzed to be insecure [2, 22]. The scheme in Ref. [14] are constructed by DNA sequences and genetic algorithm, and has quite complex structure, which may lead to side effect for the performance. In contrast, our scheme takes advantage of the logistic and spatiotemporal chaotic system and can achieve high complexity with simple structure. So our proposed image encryption scheme shows some advantage and can be regarded as a candidate for image encryption in practical application.

7 Conclusions

In this paper, a novel image encryption scheme is proposed, which takes the advantage of the chaotic system, DNA encoding and information entropy simultaneously. The sensitivity and unpredictability of logistic and spatiotemporal chaotic system can guarantee the structural complexity of the scheme. Through the DNA encoding, a pixel value can be decomposed into four DNA elements, which can realize both confusion and diffusion efficiently. Information entropy is utilized to resist the chosen-plaintext attack and increase the sensitivity of plain image. In order to decrypt the cipher image, the scheme can cause a 64-bit ciphertext expansion. But this has little influence on the performance. Explicit analysis shows that the proposed scheme is quite secure to resist different attacks, such as brute-force attack, statistical attack, differential attack, and chosen-plaintext attack, etc., and also suitable in practical application.

Acknowledgments The work is supported by the National Natural Science Foundation of China (No.61170037), the Fundamental Research Funds for the Central Universities (No.2014XSYJ01) and the Specialized Research Fund for Doctoral Program of Higher Education of China(No.06198016)

References

1. Claude S (1949) Communication theory of secrecy systems. Bell System Technical Journal 28(4):656–715
2. Hermassi H, Belazi A, Rhouma R, Belghith S (2013) Security analysis of an image encryption algorithm based on a DNA addition combining with chaotic maps. Multimed Tools Appl:1–14
3. Huang C, Nien H (2009) Multi chaotic systems based pixel shuffle for image encryption. Opt Commun 282:2123–2127

4. Joan D, Vincent R (2002) The Design of Rijndael: AES - The Advanced Encryption Standard. Springer. ISBN:3-540-42580-2
5. Kaneko K (1985) Spatiotemporal intermittency in coupled map lattices. Prog Theor Phys 74(5):1033–1044
6. Lian S, Sun J, Wang Z (2005) A block cipher based on a suitable use of the chaotic standard map. Chaos Soliton Fract 26(1):117–129
7. Li P, Li Z, Halang W, Chen G (2010) Cryptography based on spatiotemporal chaotic systems. Evolutionary Algorithms and chaotic systems: part II vol 267: pp 293–328. Springer, Berlin Heidelberg
8. Liu L, Zhang Q, Wei X (2012) A RGB image encryption algorithm based on DNA encoding and chaos map. Comput Electr Eng 38(5):1240–8
9. Liu H, Wang X, kadir A (2012) Image encryption using DNA complementary rule and chaotic maps. Appl Soft Comput 12(5):1457–66
10. Liu Y, Tang J, Xie T (2014) Cryptanalyzing a RGB image encryption algorithm based on DNA encoding and chaos map. Opt Laser Technol 60:111–115
11. Liu L, Zhang Q, Wei X (2012) A RGB image encryption algorithm based on DNA encoding and chaos map. Comput Electr Eng 38(5):1240–8
12. Lü H, Wang S, Li X, Tang G, Kuang J, Ye W, Hu G (2004) A new spatiotemporally chaotic cryptosystem and its security and performance analyses. Chaos 14(3):617–629
13. Özkaynak F, Ozer A, Yavuz S (2013) Security analysis of an image encryption algorithm based on chaos and DNA encoding. Signal processing and communications applications conference(SIU):1–4
14. Rasul E, Abdul HA, Ismail FI (2014) Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. Opt Laser Eng 56:83–93
15. Wang X, Bao X (2013) A novel image block cryptosystem based on a spatiotemporal chaotic system and a chaotic neural network. Chin Phys B 22(3):050508
16. Wang X, Liu L (2013) Cryptanalysis and improvement of a digital image encryption method with chaotic map lattices. Chin Phys B 22:050503
17. Watada J, Binti R (2008) DNA computing and its applications. Eighth international conference on intelligent systems design and applications 2:288–94
18. Wei X, Guo L, Zhang Q, Zhang J, Lian S (2012) A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. J Syst Softw 85:290–9
19. Xiao G, Lu M, Qin L, Lai X (2006) New field of cryptography: DNA cryptography. Chinese Science Bulletion 51(12):1413–1420
20. Zhang Y, He L, Fu B (2012) Research on DNA cryptography. Applied cryptography and network security:357
21. Zhang Q, Guo L, Wei X (2010) Image encryption using DNA addition combining with chaotic maps. Math Comput Model 52(11):2028–35
22. Zhang Y, Wen W, Su M, Li M (2014) Cryptanalyzing a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. Optik-Int J Light Electron Opt 125(4):1562–1564
23. Zhang Q, Guo L, Wei X (2013) A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. Optik-Int J Light Electron Opt 124(18):3596–600

Ping Zhen was born in Henan Province, China. He is a Ph.D. candidate in School of Automation and Electrical Engineering in University of Science and Technology Beijing, China. His research interests include chaos theory, chaos-based cryptography and multimedia encryption.

Geng Zhao was born in Sichuan Province, China. He received the Ph.D. degree from University of Science and Technology Beijing. He is a professor in Beijing Electronic Science and Technology Institute, China. His research interests include chaotic secure communications and computer information security.

Lequan Min was born in Beijing, China. He is a professor in School of Automation and Electrical Engineering in University of Science and Technology Beijing, China. His research interests include complex network and chaos theory and application.

Xin Jin was born in Anhui, China. He received the Ph.D. degree from Beihang University. He is a lecture in Beijing Electronic Science and Technology Institute. His research is focused on visual computing and visual media security.