Optics and Lasers in Engineering 82 (2016) 95–103

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

journal homepage: www.elsevier.com/locate/optlaseng

An image encryption scheme based on the MLNCML system using DNA sequences

Ying-Qian Zhang [a,*], Xing-Yuan Wang [b], Jia Liu [a], Ze-Lin Chi [a]

[a] City Institute, Dalian University of Technology, 31 Tieshanxi Road, Dalian 116600, PR China
[b] Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, 2 Linggong Road, Dalian 116024, PR China

ARTICLE INFO

Article history:
Received 21 December 2015
Received in revised form
30 January 2016
Accepted 1 February 2016

Keywords:
Image
Spatiotemporal chaos
DNA
Encryption

ABSTRACT

We propose a new image scheme based on the spatiotemporal chaos of the Mixed Linear–Nonlinear Coupled Map Lattices (MLNCML). This spatiotemporal chaotic system has more cryptographic features in dynamics than the system of Coupled Map Lattices (CML). In the proposed scheme, we employ the strategy of DNA computing and one time pad encryption policy, which can enhance the sensitivity to the plaintext and resist differential attack, brute-force attack, statistical attack and plaintext attack. Simulation results and theoretical analysis indicate that the proposed scheme has superior high security.

1. Introduction

Chaos based optical encoding and image encryptions [1–5] have attracted considerable attention due to their superiority [6,7]. Spatiotemporal chaotic systems are gradually regarded with better properties suitable for optical image encryptions than one dimension chaotic system, such as larger parameter range, better randomness and more chaotic sequences. The researches [8–14] are based on the CML system [15] which enhances the security of the encryption algorithms. However, the CML system is coupled by adjacent lattices, which is defined as follows:

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

where ε is the coupling parameter, the mapping function $f(x)=\mu x(1-x)$, and $\mu \in (0,4]$. The parameter μ still has periodic windows in the bifurcation diagram of some lattice. Due to the adjacent coupling between lattices, parameters $\mu \in (3.87, 3.925)$ and $\varepsilon = 0.1$ can only generate local chaotic behavior of the CML system, which implies some of lattices are not in chaotic behavior. Such space regular coupling of the adjacent coupling in the CML system is a linear coupling in the space. The lattice should be selected carefully for image encryptions. The MLNCML system can overcome the above drawbacks [16] because the chaotic system that employs the spatial nonlinear coupling can generate better pseudo-random sequences than that employs adjacent coupling.

DNA computing is applied in cryptography for massive parallelism, huge storage and ultra-low power consumption [17,18]. Therefore, the DNA-based schemes [19–27] have been well studied and achieved good results in recent years. In these DNA based the schemes, the ideas are focused on two main approaches. The first consists of applying different DNA operations, like DNA addition and DNA subtraction, on DNA coefficients after transforming the decimal matrixes values [19,23]. The second consist of adopting a dynamic DNA encoding rules depending on a secret key [20,25]. However, some of the schemes [22,25] in the both approaches are not satisfied in the security performance. The scheme in [25] employs XOR operations and the DNA encoding rules to calculate the ciphered image, which leads equivalent keys in its key space [24]. The scheme in [21] applied a fixed DNA encoding rule and the ciphered pixel values only depend on the key of the algorithm, which can be cracked in chosen plaintext attacks [26,28]. The proposed scheme in this paper avoids using XOR operations, which breaks the reduction of key space. To prevent such loopholes of the fixed DNA encoding rule, the proposed scheme employs the DNA encoding/decoding rule as a part of secret key and one-time pad encryption policy to enhance the sensitivity of the plaintext. Besides, the superior approach to the former DNA based schemes is that the DNA matrix is calculated and determined by the index lattice of the MLNCML system which depends on the plaintext image. Since the spatiotemporal chaos has $L=100$ lattices, each lattice can be selected as the potential one for

* Corresponding author.
E-mail addresses: zhangyq@dlut.edu.cn (Y.-Q. Zhang), wangxy@dlut.edu.cn (X.-Y. Wang).

http://dx.doi.org/10.1016/j.optlaseng.2016.02.002
0143-8166/

generating the corresponding DNA matrices in the specific encryption procedure by the plaintext image.

In addition, the former DNA based encryption schemes [21,22] are based on low dimension chaotic maps. The drawback of periodic degrading with finite precision in digital computers still remains. In order to overcome the above drawbacks, high dimensions spatiotemporal chaotic system is employed in the proposed scheme, which can alleviate the dynamical degradation and provide multiple chaotic sequences for encryptions in the proposed scheme. The motivation of the work is to avoid such vulnerabilities and obtain a high level security encryption scheme.

In this paper, the merits of the DNA method and the MLNCML system are combined together. In addition, one time pad encryption policy enhances the security of the proposed scheme. The spatial lattice index for generating time series for encryptions is determined by the plaintext image, which enhances the sensitivity of the plaintext image. Experimental results and theoretical analysis indicate that the proposed scheme has superior high security.

2. Preliminary materials

2.1. The MLNCML system

The logistic map was originally proposed by May [29]. It is a first-order difference equation represented by $f(x)=\mu x(1-x)$. The system considers L logistic maps coupled by neighborhood links and Arnold cat map links as follows [14]:

$$x_{n+1}(i)=(1-\varepsilon)f[x_n(i)]+(1-\eta)\frac{\varepsilon}{2}\{f[x_n(i+1)]+f[x_n(i-1)]\},$$
$$+\eta\frac{\varepsilon}{2}\{f[x_n(j)]+f[x_n(k)]\} \quad (2)$$

where i, j, k are the lattices ($1\le i,j,k\le L$), ε is the coupling parameter ($0\le\varepsilon\le 1$), η is the coupling parameter ($0\le\eta\le 1$), n is the time index ($n=1, 2, 3, \ldots$) and $f(x)=\mu x(1-x)$, $\mu\in(0,4]$. The relations of i, j, k are defined by the Arnold cat map described in Eq. (3).

$$\begin{bmatrix} j \\ k \end{bmatrix} = A\begin{bmatrix} i \\ i \end{bmatrix} \bmod L = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix}\begin{bmatrix} i \\ i \end{bmatrix} (\bmod L), \quad (3)$$

where p and q are the parameters of cat map.

The parameters p, q and η make the proposed system into diverse dynamics systems. When p, q and η are assigned with fixed values, most of these dynamical systems even hold chaotic features in continuously varying value of μ in logistic map.

The bifurcation diagram with less periodic windows in the MLNCML system is the new feature for cryptography [30]. The CML system is regarded as a suitable spatiotemporal chaotic system for cryptography partially because it is less periodic windows than low dimension chaotic map. Compared with the CML system, the MLNCML system contains larger range of parameters for the pattern of fully developed turbulence. Thus, the MLNCML system is more suitable for cryptography for the same reason.

2.2. DNA encoding and decoding rules

A DNA sequence is composed of four nucleic acid bases (hereinafter abbreviated to base): A (adenine), C (cytosine), G (guanine), T (thymine), where A and T are complementary, G and C are complementary. Because 0 and 1 are complementary in the binary, so 00 and 11 are complementary, 01 and 10 are also complementary. By using four bases A, C, G and T to encode 00, 01, 10 and 11, there are 24 kinds of encoding rules. But there are only 8 kinds of encoding rules satisfying the Watson–Crick complement rule [31], as listed in Table 1. DNA decoding rules are the reverse of DNA encoding rules.

2.3. DNA addition and subtraction rules

Addition and subtraction operations for DNA sequences are performed according to traditional binary addition and subtraction. Corresponding to 8 kinds of DNA encoding rules, there also exists 8 kinds of DNA addition rules and 8 kinds of DNA subtraction rules. For example, according to DNA encoding Rule 1, the DNA addition Rule 1 and DNA subtraction Rule 1 are shown in Table 2 and Table 3 respectively.

3. Image encryption and decryption scheme

Without loss of generality, the gray images are employed to present the encryption scheme for simplicity. The corresponding encryption algorithm can be presented as follows:

Input: $L=100$ and the source image sp. Secret keys: μ, η,ε, $x_0(1)$, the index of the used DNA encoding rule, the index of the used DNA decoding rule. Generate 128 bits random number R.

Output: Returns ciphered image c.

Step 1. Combine η,ε and $x_0(1)$ with the random number R, and calculate the new sub key η',ε', $x_0'(1)$ and random number R'in the SHA-3 hash algorithm by the equation $(\eta',\varepsilon',x_0'(1),R')=hash(\eta,\varepsilon,x_0(1),R)$.

Step 2. Calculate the initial values in Eq. (2) by using logistic map for as follows:

$$x_0'(i)=\mu x_0'(i-1)(1-x_0'(i-1)), \quad (4)$$

where $i\in[2,L]$. Iterate the MLNCML system $M\times N$ times to obtain sequences in Eq. (2).

Suppose sp is an one-dimensional pixel sequence and the kth pixel of sp is $sp(k)$. For each pixel, implement the following

Table 1
DNA encoding rules.

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

Table 2
DNA addition Rule 1.

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

Table 3
DNA subtraction Rule 1.

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

operation to obtain an $M \times N$ confused image G:

$$G(k) = \mod\{[\mod(\lfloor x_k(\mathrm{mod}(G(k-1), L)) \times 10^{16} \rfloor, 256) + sp(k) + G(k-1)], 256\} \quad (5)$$

where the initial value $G(0)=1$.

Step 3. Encode G by a kind of DNA encoding rule (the index of this DNA encoding rule serves as secret keys) and transform it into an $M \times (N \times 4)$ DNA matrix D, i.e., encode every pixel of G as a 4-base DNA sequence:

$$D_k = D_k^1 D_k^2 D_k^3 D_k^4, (k \in [1, M \times N]).$$

Step 4. Compute z_k from the MLNCML system from

$$X_q = \{x_1(q), \ x_2(q), \ldots, \ x_{M\times N}(q)\},$$

where $q = \left(\frac{1}{M\times N}\sum_{i=1}^{M\times N} sp(i)\right) \mod L$ and each element denoted as $x_k(q)$ $(k \in [1, M \times N])$, implement the following operation:

$$z_k = \mod\left(\lfloor x_k(q) \times 10^{16} \rfloor, \ 256\right). \quad (6)$$

Encode z_k by a kind of DNA encoding rule (the index of this DNA encoding rule serves as secret keys) and transform it into an $M \times (N \times 4)$ DNA matrix D'.

Step 5. Calculate the D'' as follows:

$$D'' = \begin{cases} D_k + D'_k, & \mathrm{mod}(R' \gg (k \bmod 128), 2) = 1 \\ D_k - D'_k, & \mathrm{mod}(R' \gg (k \bmod 128), 2) = 0 \end{cases}, \quad (7)$$

where "+" and "−" are respectively the DNA addition operation and DNA subtraction operation in the proposed algorithm, "$>>$" is the binary left shift operation. The indexes of the used DNA addition rule and DNA subtraction rule serve as secret keys.

Step 6. Decode D'' by a kind of DNA decoding rule (the index of this DNA decoding rule serves as secret keys), and we obtain the ciphered image, denoted by C.

Step 7. If the one round encryption or the complete multi-rounds encryptions are accomplished, the value of (M, N)-pixel in the ciphered image is assigned with the value of q. The encryption process finishes. The flow chart of the encryption is shown in Fig. 1.

The decryption algorithm, shown in Fig. 2, is the reverse process of encryption algorithm as follows:

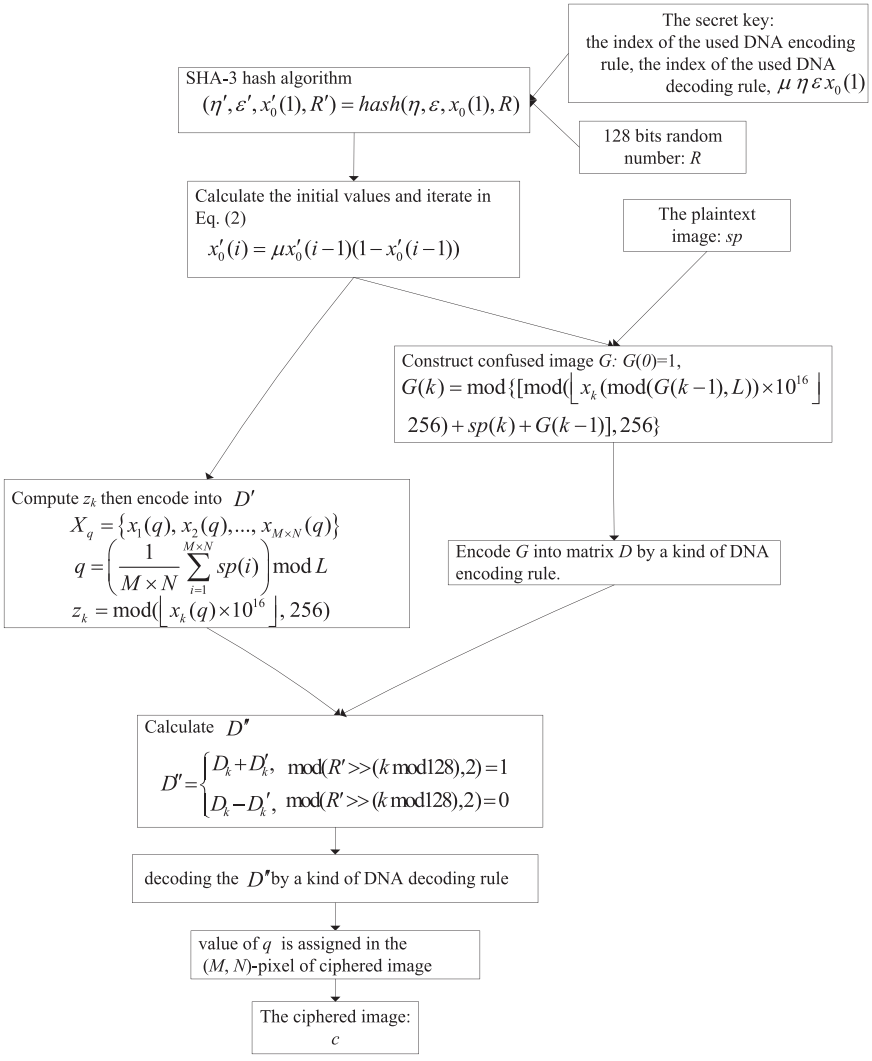

Fig. 1. Encryption flow chart.

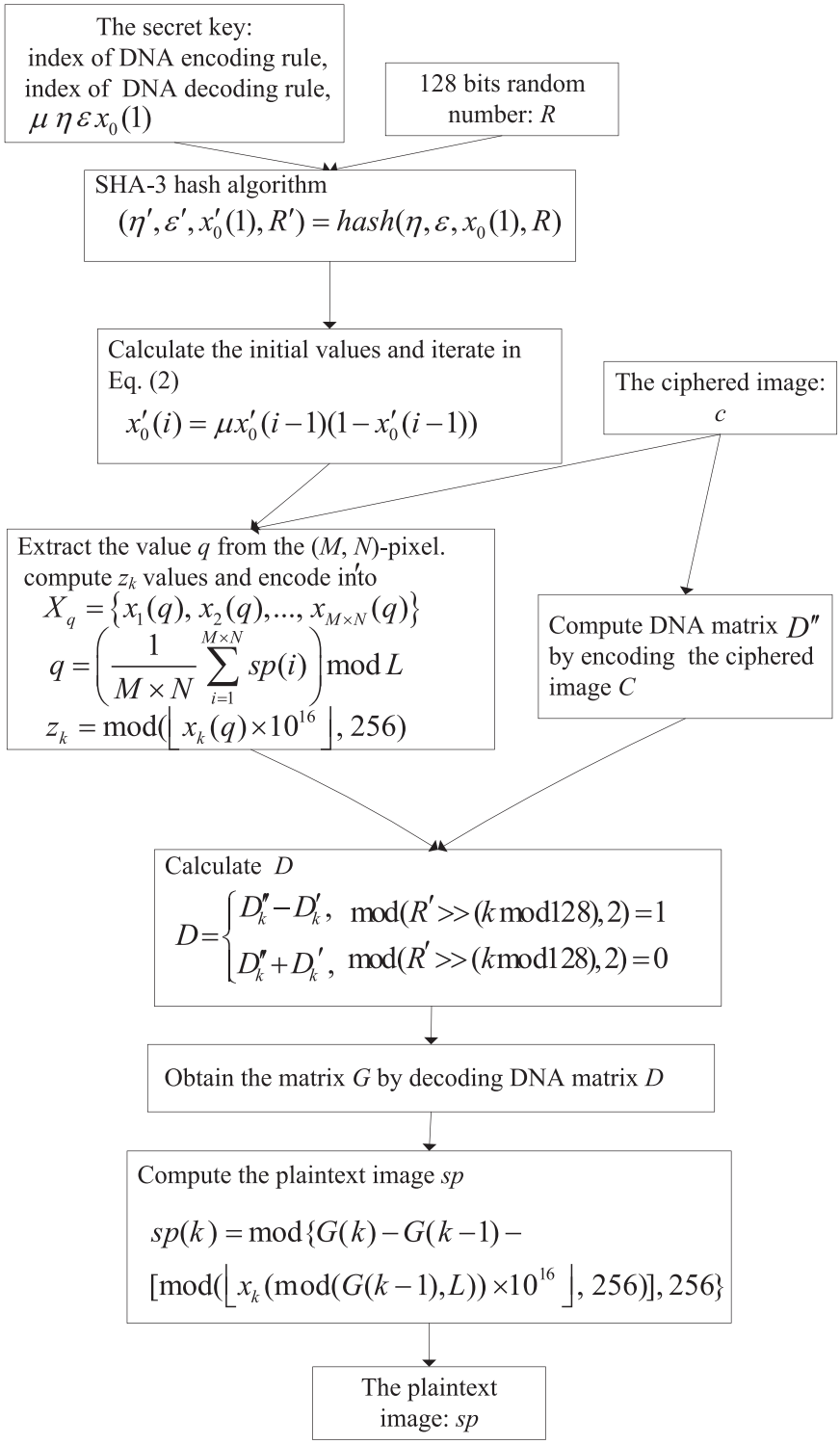

Fig. 2. Decryption flow chart.

Input: $L=100$ and the ciphered image C. Secret keys: μ, η,ε, $x_0(1)$, the index of the used DNA encoding rule, the index of the used DNA decoding rule. Receive 128 bits random number R.

Output: Returns the plaintext image sp.

Step 1. Combineη,ε and $x_0(1)$ with the random number R, and calculate the new sub key η',ε', $x_0'(1)$ and random number R'in the SHA-3 hash algorithm by the equation $(\eta', \varepsilon', x_0'(1), R') = hash(\eta, \varepsilon, x_0(1), R)$.

Step 2. Calculate the initial values in Eq. (2) by using logistic map for as follows:

$$x_0'(i) = \mu x_0'(i-1)(1-x_0'(i-1)), \tag{4}$$

where $i \in [2, L]$. Iterate the MLNCML system $M \times N$ times to obtain sequences in Eq. (2).

Step 3. Extract the value q from the (M, N)-pixel in the ciphered image and compute z_k values by Eq. (6) from

$X_q = \{x_1(q),\ x_2(q), ...,\ x_{M\times N}(q)\}$.

Fig. 3. Encryption results. (a) Original Lena image, (b) Ciphered Lena image, (c) Recovery Lena image, (d) Original Barb image, (e) Ciphered Barb image, (f) Recovery Barb image.

Encode z_k by a kind of DNA encoding rule (the index of this DNA encoding rule serves as secret keys) and transform it into an $M \times (N \times 4)$ DNA matrix D'.

Step 4. Compute DNA matrix D'' by encoding the ciphered image C in a kind of DNA decoding rule (the index of this DNA decoding rule serves as secret keys).

Step 5. Compute DNA matrix D by the equation as follows:

$$D = \begin{cases} D''_k - D'_k, & \mathrm{mod}(R' \gg (k \bmod 128), 2) = 1 \\ D''_k + D'_k, & \mathrm{mod}(R' \gg (k \bmod 128), 2) = 0 \end{cases}. \tag{8}$$

Step 6. Obtain the matrix G by decoding DNA matrix D by the kind of DNA decoding rule.

Step 7. Compute the plaintext image sp by the following equation:

$$sp(k) = \mathrm{mod}\left\{G(k) - G(k-1) - \left[\mathrm{mod}\left(\left\lfloor x_k(\mathrm{mod}(G(k-1), L)) \times 10^{16} \right\rfloor, 256\right)\right], 256\right\}. \tag{9}$$

The plaintext images of Lena and Barb and the corresponding ciphered images, shown in Fig. 3, employ the secret key assignment with $\mu = 3.88$, $\eta = 0.6, \varepsilon = 0.3$, $x_0(1) = 0.30565487923280$, DNA encoding Rule 1 and DNA decoding Rule 1.

4. Simulation results

A good cryptosystem should resist all kinds of known attacks, such as known-plaintext attack, chosen cipher-text attack, statistical

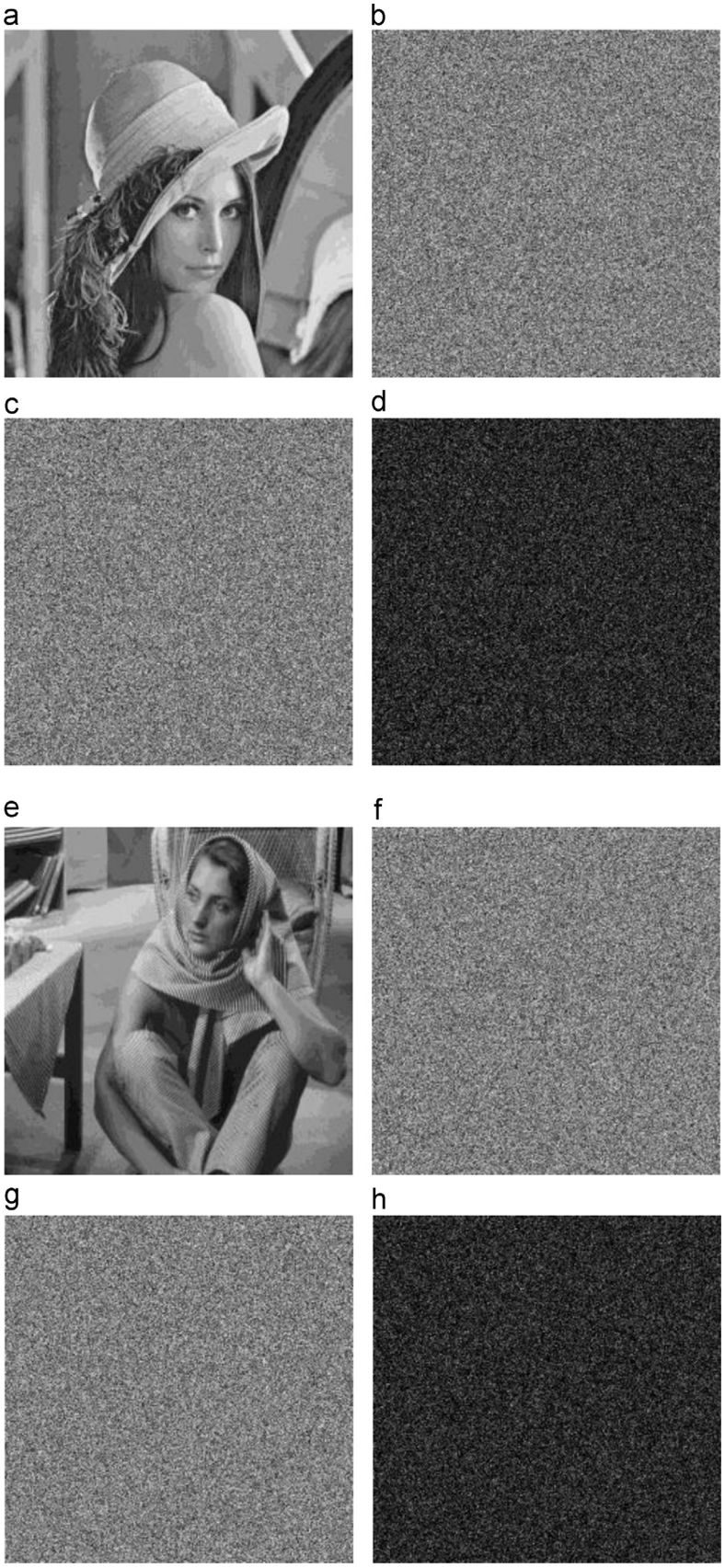

Fig. 4. Key sensitivity. (a) Original Lena image, (b) Ciphered Lena image when $\mu = 3.88$, (c) Ciphered Lena image when $\mu = 3.8800001$, (d) Difference between Fig. 3(b) and Fig. 3(c), (e) Original Barb image, (f) Ciphered Barb image when $\mu = 3.88$, (g) Ciphered Barb image when $\mu = 3.8800001$, (h) Difference between Fig. 3(f) and Fig. 3(g).

attack, differential attack, and various brute-force attacks. The corresponding security analyses have been performed on the proposed algorithm, including key space analysis, key sensitivity analysis, statistical analysis and differential analysis.

4.1. Key space

The key space should be large enough to make brute-force attacks infeasible. Number of control parameters in secret key: μ has a precision of 10^{-14} and $\mu \geq 3.7$, ε has a precision of 10^{-14}, $x_0(1)$ has a precision of 10^{-14} and η has a precision of 10^{-14}. In one-time pad policy, the 128 bits random number will be abandoned; therefore, the 128 bits random number is not counted into the key space. Except the secret key the index of the used DNA encoding rule, the index of the used DNA decoding rule, the key space size is more than 10^{56}. Therefore, the proposed encryption algorithm is good at resisting brute-force attack.

4.2. Key sensitivity

The secret keys include μ, η, ε, $x_0(1)$, the index of the used DNA encoding rule, the index of the used DNA decoding rule. It is time consuming to examine the sensitivity of secret keys by enumerating all the possible combinations of secret key parts. We employ Lena and Barb images for the test the key sensitivity when we randomly change the secret key part a little bit, which is shown in Fig. 4.

4.3. Histogram analysis

The histogram of an image reveals the distribution information of pixel values. An ideal encrypted image should have a uniform and completely different histogram against the plain-image for preventing the adversary from extracting any meaningful information from the fluctuating histogram of the cipher-image.

The histograms of the plain-images and ciphered images of Lena and Barb are shown in Fig. 5. The corresponding ciphered images of Lena and Barb are encrypted by completely different secret keys. The histograms of cipher-images are fairly uniform and are significantly different from that of the plain-images.

4.4. Differential attack

A good encryption scheme is not only sensitive to the secret key but also the plaintext image. In the proposed scheme, the current ciphered pixel value depends on the ciphered value of the previous pixel. The chaotic series for encrypting images do not depend on the specific lattice in the proposed scheme. Since the MLNCML system contains 100 lattices, the specific lattice for the next pixel encrypting is determined dynamically by ciphered pixel value of the previous pixel. Therefore, different plaintext images employ various lattices for their encryptions. In the proposed scheme, different pixel takes different lattices of chaotic series for encryption, which increase the sensitivity of the plaintext image.

For quantity analysis, an adversary may make a slight change (e.g. only one pixel changed) of the original image, and then

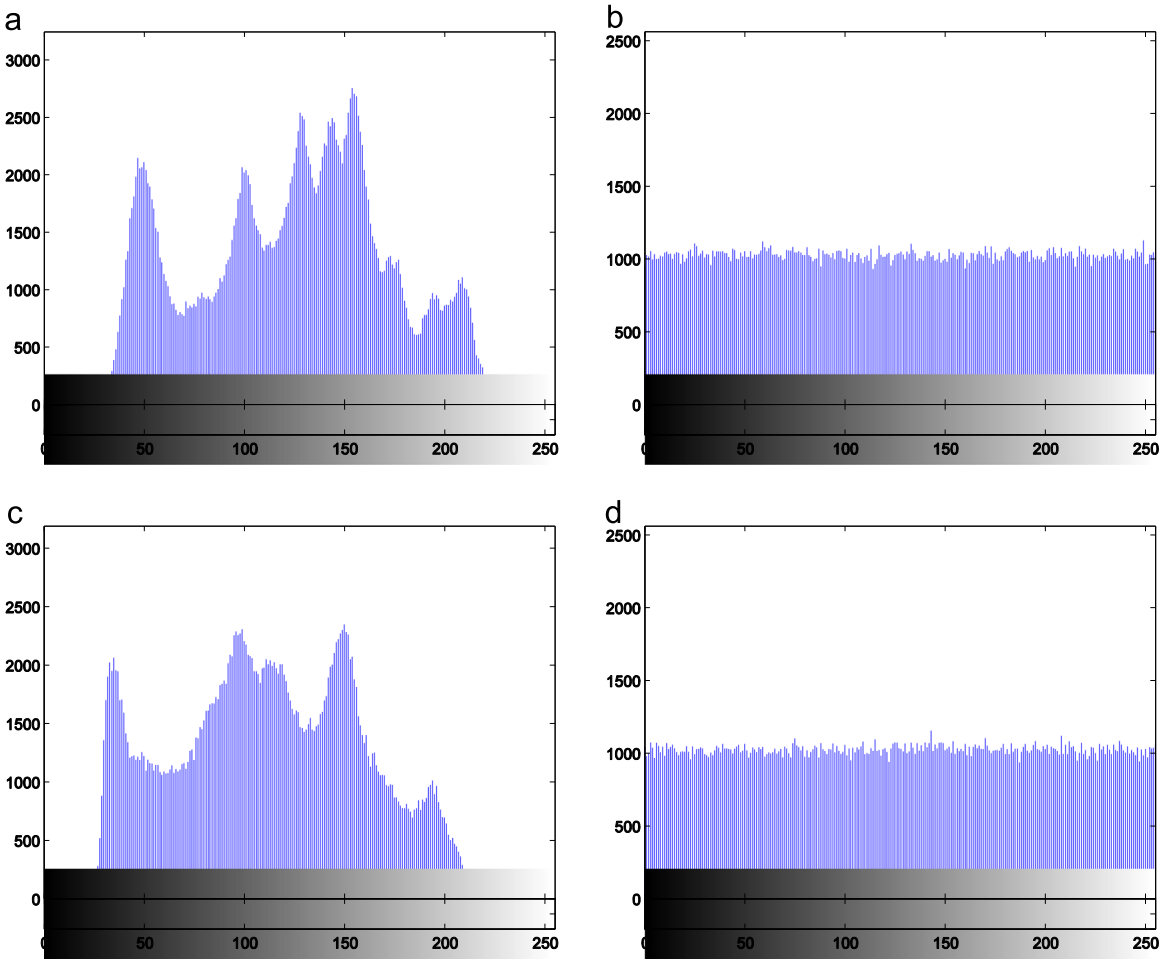

Fig. 5. Histograms for the plain-images and ciphered images. (a) Histogram of Lena, (b) Histogram of ciphered image of Lena, (c) Histogram of Barb, (d) Histogram of ciphered image of Barb.

observes the change of encryption results. In this way, the adversary may be able to find out a meaningful relationship between two ciphered images and the original image. We employ the *NPCR* (number of pixels change rate) and *UACI* (unified average changing intensity) which is defined in Eq. (10) and Eq. (11).

$$\begin{cases} D(i,j) = \begin{cases} 1, c_1(i,j) \neq c_2(i,j) \\ 0, \text{otherwise} \end{cases} \\ NPCR = \frac{\sum_{ij} D(i,j)}{M \times N} \times 100\% \end{cases}, \tag{10}$$

$$UACI = \frac{1}{M \times N}\left[\sum_{ij} \frac{c_1(i,j) - c_2(i,j)}{255}\right] \times 100\%, \tag{11}$$

where c_1 and c_2 are the two ciphered images.

Without loss of generality, we employ two plaintext images for tests which are the Lena image and the Barb image. The images of only adding 1 in the value of the (0,0)-pixel are the corresponding slightly changed images. The *NPCR* and *UACI* values of Lena and Barb for five encryption rounds are listed in Table 4 and Table 5.

4.5. Correlation analysis

It is known that adjacent image pixels are highly correlated either in horizontal, vertical or diagonal directions. The correlation between adjacent pixels should be significantly reduced in the ciphered image. To test the correlation of plain-text image and ciphered image, the following procedures are carried out. First, randomly select 3000 pairs of two adjacent pixels from an image. Then, the correlation coefficients of adjacent pixels in vertical, horizontal and diagonal directions are evaluated using the following formulas:

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

$$E(x) = \frac{1}{S}\sum_{i=1}^{S} x_i, \tag{13}$$

$$D(x) = \frac{1}{S}\sum_{i=1}^{S} (x_i - E(x))^2, \tag{14}$$

$$\mathrm{cov}(x,y) = \frac{1}{S}\sum_{i=1}^{S} (x_i - E(x))(y_i - E(y)), \tag{15}$$

where x and y denote two adjacent pixels and S is the total number of duplets (x, y) obtained from the image. $E(x)$ and $D(x)$ are the expectation and the variance of x, respectively. The calculated correlation coefficients of plaintext images of Lena, Barb and their corresponding ciphered images in the proposed algorithm are listed in Table 6. The average performance for ciphered images of Lena and Barb are compared with that of Lian's algorithm [32] and Zhu's algorithm [33], which is also listed in Table 6.

Table 4
NPCR performance of the proposed algorithm compared with images changed in (0, 0)-pixel

Round	Proposed scheme (Lena)	Proposed scheme (Barb)	Lian's algorithm
1	0.996448516	0.996253967	0.000335693
2	0.995880126	0.996143341	0.033283200
3	0.996840244	0.996285224	0.799290000
4	0.996165251	0.996515762	0.995064000
5	0.996852911	0.996647786	0.995914000

Table 5
UACI performance of the proposed algorithm compared with images changed in (0, 0)-pixel

Round	Proposed scheme (Lena)	Proposed scheme (Barb)	Lian's algorithm
1	0.334036464	0.334926440	0.000087738
2	0.334710798	0.334227259	0.007984160
3	0.334532587	0.334753260	0.218563000
4	0.334643658	0.334868465	0.322368000
5	0.334692570	0.334972605	0.333359000

Table 6
Correlation coefficients of the proposed algorithm compared with that of Zhu's algorithm and Lian's algorithm

	Horizontal	Vertical	Diagonal
The proposed algorithm (Barb)	0.000006321	0.000000769	−0.000007787
The proposed algorithm (Lena)	0.000002971	−0.000001339	−0.000003790
Lian' algorithm	0.062110733	0.003154296	0.002587458
Zhu's algorithm	0.000898142	0.001221932	0.003672757

4.6. Computational and complexity analysis

To evaluate the running speed, tests are performed on the encryption speed of the proposed algorithm in comparison with Lian's algorithm. All the tests are implemented in Visual C++ 6.0 with a Windows XP Professional operating system, and the computer is of an Intel Core 2.4 GHz CPU, 2GB RAM and 500 GB hard disk. The image of Lena, the 512 × 512 image with 256 grey levels, is encrypted by each algorithm for ten times. The total average execution time in the proposed algorithm, Lian's algorithm and Zhu's algorithm are 325 ms, 341 ms and 34 ms respectively. Therefore, the proposed algorithm is slower than Zhu's algorithm but similar to Lian's algorithm.

For analyses of execution time, the time-consuming part in computations is the operation of multiplying floating point numbers for the MLNCML system. The proposed algorithm needs more time than the Zhu's algorithm because the proposed algorithm needs $\Theta(L \times M \times N)$ iterations of multiplying floating point numbers; however the Zhu's algorithm needs $\Theta(M \times N)$ iterations of multiplying floating point numbers. In Lian's algorithm, the time-consuming part in computations is $\Theta(M \times N)$ iterations of calculations of a sine function which needs more time by Taylor series calculations.

Although the proposed algorithm is slower than Zhu's algorithm, the proposed algorithm can be applied into multiple images encryption simultaneously because the spatiotemporal chaotic MLNCML system contains $L = 100$ chaotic series which provide more potential pseudo-random series for encryptions. Multi-images encryptions amortize the computational complexity of the MLNCML system. However, Zhu's algorithm needs to re-calculate chaotic series for another image encryption. Therefore, the proposed scheme is superior to Zhu's and Lian's algorithms in image cloud storage encryption. In addition, when the size of lattices decreases properly, the execution speed of the proposed algorithm can be faster.

4.7. Information entropy

The information entropy can test uncertainty. Entropy reflects whether gray-scale values' distribution is random or equality. The coarser the image is, the larger the entropy is. The minimum and maximum values of entropy are zero and eight respectively. Therefore, the value of entropy of encrypted image should be as higher as possible. Let m be the information source, and the

equation for calculating information entropy is:

$$H(m)=\sum_{i=0}^{2^n-1} p(m_i)\log_2\frac{1}{p(m_i)}, \tag{16}$$

where $p(m_i)$ represents the probability of symbol m_i. Assume that there are 2^8 states of the information source and they appear with the same probability. The ideal information entropy is $H(m)=8$, which indicates that the information is completely random. The information entropy of the ciphered image should be close to 8 after encryption. The values of information entropy of ciphered images in the proposed scheme are 7.999287615, which indicate that the ciphered images obtained by the proposed algorithm could hardly divulge information.

4.8. Known-plaintext and chosen-cipher text attacks analyses

known-plaintext and chosen-cipher text attacks are usually employed to make an analysis on image encryption algorithms [8–10,24,26–28]. According to the Kerckhoffs' principle, assume that the attacker has obtained the encryption and decryption machinery as well as the attacker does not access the intermediate result and the secret key of the cryptosystem and the 128 bits random number R.

In the proposed algorithm, the chaotic sequences in the spatiotemporal chaos have changed entirely, because the parameters for the spatiotemporal chaos is re-calculated by the SHA-3 hash function where the random number R is used only once in the encryption (one time pad). Therefore, when the attacker chooses an image for another attack, the corresponding chaotic sequences have changed. The attacker cannot recovery the former chaotic sequences. In addition, the DNA matrix calculations in steps 4 and 5 depend on the plaintext image and the random number R. Therefore, the proposed scheme has a good feedback mechanism to the plaintext image for the one time pad encryption. The ciphered image obtains only 2% chaotic sequences in the whole MLNCML spatiotemporal chaotic system, which can not supply any information for attackers when they choose special images. As a result, the cryptanalysis methods such as [8–10,24,26–28] will not work properly to our encryption algorithm.

5. Conclusions and future work

In this paper, we proposed a new image encryption scheme by the MLNCML system. This spatiotemporal chaotic system has the features of larger parameter range, better randomness and more chaotic sequences than the CML system. In addition, the DNA computing is suitable in cryptography for massive parallelism, huge storage. Therefore, the proposed scheme has a good significance in chaotic cryptography. The security analyses are given to prove that the key space and sensitivity is better enough to make brute-force attacks infeasible. Simulations results indicate that the proposed scheme leads to a higher security level. As a part of future work, we intend to implement it in parallel and design it into a large number of images cloud computing and storage encryptions.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (Nos: 61370145, 61173183, and 60973152), the Doctoral Program Foundation of Institution of Higher Education of China (No: 20070141014), Program for Liaoning Excellent Talents in University (No: LR2012003), the National Natural Science Foundation of Liaoning province (No: 20082165) and the Fundamental Research Funds for the Central Universities (No: DUT12JB06).

References

[1] Wang XY, Gu SX, Zhang YQ. Novel image encryption algorithm based on cycle shift and chaotic system. Opt Lasers Eng 2015;68:126–34.
[2] Wang XY, Liu LT, Zhang YQ. A novel chaotic block image encryption algorithm based on dynamic random growth technique. Opt Lasers Eng 2015;66:10–8.
[3] Chen JX, Zhu ZL, Fu C, Yu H, Zhang LB. An efficient image encryption scheme using gray code based permutation approach. Opt Lasers Eng 2015;67:191–204.
[4] Xu L, Li Z, Li J, Hua W. A novel bit-level image encryption algorithm based on chaotic maps. Opt Lasers Eng 2016;78:17–25.
[5] Wang L, Song H, Liu P. A novel hybrid color image encryption algorithm using two complex chaotic systems. Opt Lasers Eng 2016;77:118–25.
[6] Chen W. Multiple-wavelength double random phase encoding with CCD-plane sparse-phase multiplexing for optical information verification. Appl Opt 2015;54(36):10711–6.
[7] Chen W, Chen XD. Double random phase encoding using phase reservation and compression. J Opt 2014;16(2):025402.
[8] Arroyo D, Rhouma R, Alvarez G, Li SJ, Fernandez V. On the security of a new image encryption scheme based on chaotic map lattices. Chaos 2008;18:033112.
[9] Ercan S, Cahit C. Algebraic break of image ciphers based on discretized chaotic map lattices. Inform Sci 2011;181:227–33.
[10] Ge X, Liu FL, Lu B, Wang W. Cryptanalysis of a spatiotemporal chaotic image/video cryptosystem and its improved version. Phys Lett A 2011;375:908–13.
[11] Lian SG. Efficient image or video encryption based on spatiotemporal chaos system. Chaos Soliton Fractal 2009;40:2509–19.
[12] Liu HJ, Wang XY. Color image encryption using spatial bit-level permutation and high-dimension chaotic system. Opt Commun 2011;284:3895–903.
[13] Tang Y, Wang ZD, Fang JA. Image encryption using chaotic coupled map lattices with time-varying delays. Commun Nonlinear Sci 2010;15:2456–68.
[14] Xiang T, Wong KW, Liao XF. Selective image encryption using a spatiotemporal chaotic system. Chaos 2007;17:023115.
[15] Kaneko K. Pattern dynamics in spatiotemporal chaos. Physica D 1989;34:1–41.
[16] Zhang YQ, Wang XY. A New Image Encryption Algorithm Based on Non-adjacent Coupled Map Lattices. Appl Soft Comput 2015;vol. 26:10–20.
[17] Head T, Rozenberg G, Bladergroen RS, Breek CKD, Lommerse PHM, Spaink HP. Computing with DNA by operating on plasmids. Biosystems 2000;57(2):87–93.
[18] Zheng XD, Xu J, Li W. DNA arithmetic operation based on n-moduli set. Appl Math Comput 2009;vol. 212:177–84.
[19] Wei XP, Guo L, Zhang Q, Zhang JX, Lian SG. A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. J Syst Softw 2012;85(2):290–9.
[20] Liu HJ, Wang XY, kadir A. Image encryption using DNA complementary rule and chaotic maps. Appl Soft Comput 2012;12(5):1457–66.
[21] Zhang, X. P. Wei Q. A novel couple images encryption algorithm based on DNA subsequence operation and chaotic system. Optik 2013;124(23):6276–81.
[22] Zhang Q, Wei XP. RGB Color Image Encryption Method Based on Lorenz Chaotic System and DNA Computation. IETE Tech Rev 2013;30(5):404–9.
[23] Zhang Q, Guo L, Wei X. Image encryption using DNA addition combining with chaotic maps. Math Comput Model 2010;11–12(52):2028–35.
[24] Belazi A, Hermassi H, Rhouma R, Belghith S. Algebraic analysis of a RGB image encryption algorithm based on DNA encoding and chaotic map. Nonlinear Dyn 2014;76:1989–2004.
[25] Liu L, Zhang Q, Wei X. A RGB image encryption algorithm based on DNA encoding and chaos map. Comput Electr Eng 2012;38(5):1240–8.
[26] Özkaynak F, Yavuz S. Analysis and improvement of a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. Nonlinear Dyn 2014;78:1311–20.
[27] Wang XY, Zhang YQ, Bao XM. A novel chaotic image encryption scheme using DNA sequence operations. Opt Lasers Eng 2015;73:53–61.
[28] Zhang YQ, Wang XY. Analysis and improvement of a chaos-based symmetric image encryption scheme using a bit-level permutation. Nonlinear Dyn 2014;77(3):687–98.
[29] May RM. Simple mathematical models with very complicated dynamics. Nature 1976;261:459–67.
[30] Zhang YQ, Wang XY. A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice. Inform Sci 2014;273:329–51.
[31] Watson JD, Crick FHC. A structure for deoxyribose nucleic acid. Nature 1953;171(4356):737–8.
[32] Lian SG, Sun J, Wang Z. A block cipher based on a suitable use of the chaotic standard map. Chaos Solitons Fractals 2005;26:117–29.
[33] Zhu ZL, Zhang W, Wong KW, Yu H. A chaos-based symmetric image encryption scheme using a bit-level permutation. Inform Sci 2011;181:1171–86.