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