Optik 124 (2013) 3329–3334

Contents lists available at SciVerse ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

# An image encryption scheme based on new spatiotemporal chaos

Chun-Yan Song [a], Yu-Long Qiao [b,*], Xing-Zhou Zhang [b]

[a] College of Mechanical and Electrical Engineering, Northeast Forestry University, Harbin 150001, China
[b] College of Information and Communication Engineering, Harbin Engineering University, Harbin 150001, China

ARTICLE INFO

*Article history:*
Received 19 May 2012
Accepted 16 October 2012

*Keywords:*
Spatiotemporal chaos
Coupled map lattices
Nonlinear chaotic algorithm
Image encryption

ABSTRACT

Spatiotemporal chaos is chaotic dynamics in spatially extended system, which has attracted much attention in the image encryption field. The spatiotemporal chaos is often created by local nonlinearity dynamics and spatial diffusion, and modeled by coupled map lattices (CML). This paper introduces a new spatiotemporal chaotic system by defining the local nonlinear map in the CML with the nonlinear chaotic algorithm (NCA) chaotic map, and proposes an image encryption scheme with the permutation-diffusion mechanism based on these chaotic maps. The encryption algorithm diffuses the plain image with the bitwise XOR operation between itself pixels, and uses the chaotic sequence generated by the NCA map to permute the pixels of the resulting image. Finally, the constructed spatiotemporal chaotic sequence is employed to diffuse the shuffled image. The experiments demonstrate that the proposed encryption scheme is of high key sensitivity and large key space. In addition, the scheme is secure enough to resist the brute-force attack, entropy attack, differential attack, chosen-plaintext attack, known-plaintext attack and statistical attack.



## 1. Introduction

Multimedia communication, especially image communication becomes more and more important because of the development of the Internet and digital multimedia techniques. Digital technology can bring us much convenience, but also bring attackers and illegal users the opportunity, so the image encryption method has become a major concern. Different from texts, images have their intrinsic properties, such as bulk data capacity and strong correlation among pixels, and some traditional data encryption techniques such as DES, AES, IDEA and RSA cannot meet the demand for digital image encryption [1,2]. Because chaos has the good properties such as high security, low computational complexity and high sensitivity to the initial conditions and system parameters, the chaos based encryption algorithm provides a new way for digital image encryption.

Since Matthews [3] suggested that a one-dimensional chaotic map could be used as one time pad for encrypting messages, the researchers have proposed various image encryption algorithms based on the low dimensional chaotic systems [4–7], hyper-chaotic systems [8–10] and spatiotemporal chaotic systems [11–15]. Because the advantages of high efficiency and simplicity of low dimensional chaotic systems, some typical low dimensional chaotic maps, such as logistic map, Arnold map and baker map, have been used to encrypt the images. Pareek [4] introduced an image encryption approach based on two chaotic logistic maps, in which the initial condition of the second logistic map was modified from the numbers generated by the first logistic map. However, there are well-known weaknesses for the logistic map, such as small key space and weak security. To overcome the drawback, Gao and Zhang [5] introduced a new chaotic map, the nonlinear chaotic algorithm (NCA) map, and proposed an image encryption algorithm based on the new chaotic map. Although the scheme is of larger key space and acceptable efficiency, it can not resist the known-plaintext attack and chosen-plaintext attack. Fridrich [6] proposed an image encryption scheme based on a two-dimensional chaotic map. In Akhshani's work [7], two-dimensional piecewise nonlinear chaotic maps were generalized for designing an image encryption scheme. Chen [9] extended the two-dimensional chaotic cat map to 3D for designing a real-time secure symmetric encryption scheme. Gao [10] proposed a new encryption scheme based on hyper-chaotic system. In the scheme, an image total shuffling matrix is adopted to shuffle the positions of image pixels, and then a hyper-chaotic system is used to confuse the relationship between the plain image and the cipher image.

Recently, the coupled map lattices (CML) based spatiotemporal chaotic system was proposed for self-synchronizing stream cipher [11–13]. Wang et al. [12] have shown that the communication with CML is more secure than the communication with a single map. Lian [14] proposed an image or video encryption system based on the spatiotemporal chaos, but Eun-Jun Yoon [15] has demonstrated

* Corresponding author. Tel.: +86 13199479017.
*E-mail addresses:* qiaoyulong@hrbeu.edu.cn, yulongqiao@hotmail.com (Y.-L. Qiao).

0030-4026/$ – see front matter © 2012 Elsevier GmbH. All rights reserved.
http://dx.doi.org/10.1016/j.ijleo.2012.11.002

that the scheme is not secure and introduced an improved scheme. The spatiotemporal chaotic system possesses much better properties than simple chaotic system. First, due to the finite computing precision, there are problems of short period and small number of periodic orbits for low-dimensional chaotic systems. However, it is found that the spatiotemporal chaos can solve the problems satisfactorily [16,17]. Second, the spatiotemporal systems have larger parameter space, more positive Lyapunov exponents, higher randomness and more chaotic sequences, so it is more difficult to predict the chaotic series generated by the spatiotemporal systems. Considering of this, the spatiotemporal chaos is more suitable for data protection. In this paper, we construct a spatiotemporal chaos based on the nonlinear chaotic algorithm (NCA) map introduced in [5], and then propose an image encryption scheme based on the new spatiotemporal chaotic map.

The rest of this paper is organized as follows. Section 2 introduces the new spatiotemporal chaotic system. The spatiotemporal chaos based image encryption scheme is presented in Section 3. The experimental results and analysis are conducted in Section 4. Finally, the conclusions are drawn in the last section.

## 2. Proposed spatiotemporal chaotic system

Spatiotemporal chaos is chaotic dynamics in spatially extended system. Comparing with the low-dimensional chaotic system, the spatiotemporal chaos has more complex behavior and more abundant characteristics. Spatiotemporal chaotic systems are often modeled by partial differential equations (PDE), coupled ordinary differential equations (CODE), or coupled map lattices (CML) [17]. In the paper, CML is employed as the model of the spatiotemporal chaotic systems.

### 2.1. NCA map

The NCA map is constructed on the basis of logistic map. It is well known that the logistic map is defined as follows,

$$x_{n+1} = \mu x_n(1 - x_n), \quad n = 1, 2, \ldots \tag{1}$$

where $0 < \mu \le 4$, $x_n \in (0, 1)$. When $3.57 \le \mu \le 4$, the logistic map appears the chaotic behavior and becomes a chaotic system. The cryptosystem based on the logistic map has small key space and weak security. To overcome the limitation, Gao et al. [5] have proposed a new nonlinear chaotic algorithm (NCA) based on the logistic map as follows:

$$x_{n+1} = (1 - \beta^{-4}) \cdot ctg\left(\frac{\alpha}{1+\beta}\right) \cdot \left(1 + \frac{1}{\beta}\right)^{\beta} \cdot tg(\alpha x_n) \cdot (1 - x_n)^{\beta} \tag{2}$$

where $x_n \in (0, 1)$, $\alpha \in (0, 1.4]$, $\beta \in [5, 43]$, or $x_n \in (0, 1)$, $\alpha \in (1.4, 1.5]$, $\beta \in [9, 38]$, or $x_n \in (0, 1)$, $\alpha \in (1.5, 1.57]$, $\beta \in [3, 15]$. The NCA map is a chaotic system with good properties of balanced 0–1 ratio, zero co-correlation and ideal nonlinearity.

### 2.2. Spatiotemporal chaotic map

A CML is a dynamical system with discrete time, discrete space and continuous state. It always serves as a prototype model of the spatiotemporal chaos to study the chaotic dynamics.

The double-way coupled map lattice system can be defined as

$$\begin{cases} x_{n+1}(i) = (1 - \varepsilon) f(x_n(i)) + \dfrac{\varepsilon}{2}\{f[x_n(i-1)] + f[x_n(i+1)]\} \\ f(x) = \mu x(1 - x) \end{cases} \tag{3}$$

where $i = 1,2, \ldots, L$ is the lattice site index, $n = 1,2, \ldots$ is the time index, $\varepsilon \in (0, 1)$ is a coupling constant, and $x_n(i) \in (0, 1)$. Here $f(x)$ is the logistic map with $3.57 \le \mu < 4$, $0 < x < 1$ and $0 < f(x) < 1$. The periodic boundary condition is $x_n(0) = x_n(L)$, where $L$ is the length of CML.

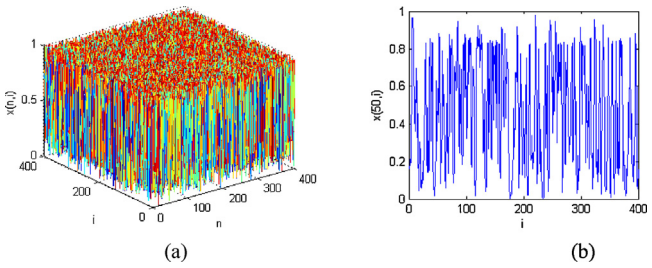


**Fig. 1.** Proposed spatiotemporal chaos: (a) constructed spatiotemporal chaos $x_n(i)$ and (b) $x_{50}(i)$.

Taking the advantages of the NCA map into account, we substitute the logistic map in Eq. (3) with the NCA map Eq. (2), and then the CML is defined as follows:

$$\begin{cases} x_{n+1}(i) = (1 - \varepsilon) f(x_n(i)) + \dfrac{\varepsilon}{2}\{f[x_n(i-1)] + f[x_n(i+1)]\} \\ f(x) = (1 - \beta^{-4}) \cdot ctg\left(\dfrac{\alpha}{1+\beta}\right) \cdot \left(1 + \dfrac{1}{\beta}\right)^{\beta} \cdot tg(\alpha x_n) \cdot (1 - x)^{\beta} \end{cases} \tag{4}$$

where $\varepsilon \in (0, 1)$, and $x_n(i) \in (0, 1)$. The other parameters are explained in Eq. (2).

Fig. 1(a) shows the spatiotemporal chaos with $L = 400$, $\varepsilon = 0.3$, $\alpha = 1.57$ and $\beta = 3.5$. For a given $n = 50$, the state value $x_{50}(i)$ is plotted in Fig. 1(b). We can see from Fig. 1 that the system exhibits chaotic properties both in the time and space domains.

## 3. Spatiotemporal chaos based image encryption scheme

Generally speaking, image encryption schemes are composed of two processes, confusion process and diffusion process. In the paper, we present an image encryption scheme based on two chaotic systems. The NCA map is used to permute the positions of the image pixels, and the constructed spatiotemporal chaotic sequence is adopted to diffuse the shuffled image.

Without loss of generality, we assume the size of a plain image is $256 \times 256$. The proposed image encryption algorithm is summarized as follows.

**Step 1:** Convert the plain image into a one-dimensional array $M = \{m_1, m_2, \ldots, m_{256\times256}\}$.

**Step 2:** Diffuse the array $M$ according to the following formula:

$$\begin{cases} m'_1 = m_1 \oplus m_{256\times256} \\ m'_{j+1} = m_j \oplus m'_j, \quad j = 1, 2, \ldots, 256 \times 255 \end{cases}$$

where $\oplus$ is the bitwise Exclusive-OR (XOR) operation. Then we get the diffused array $M' = \{m'_1, m'_2, \ldots, m'_{256\times256}\}$.

**Step 3:** Calculate the sum of the elements of $M$, and transform it into (0, 1). For example, if the sum is 6434179, we convert it to 0.6434179. This transformed sum value is adopted as the initial value of the NCA map, and the NCA chaotic sequence is generated according to Eq. (2). Choose the $(N_0 + 1)$th element to the $(N_0 + 256 \times 256)$th element from the chaotic sequence ($N_0 = 100$ in the proposed algorithm) in order to avoid the harmful effect of the transition procedure, and form a new sequence $A = \{a_1, a_2, \ldots, a_{256\times256}\}$ for the following encryption.

**Step 4:** Sort $\boldsymbol{A}$ in ascending order, and we obtain a position sequence $\boldsymbol{IX}$, whose element $IX(i)$ is the position where the $i$th sorted element is located in the original sequence $\boldsymbol{A}$. Permute the sequence $M'$ with $\boldsymbol{IX}$, and get $M'' = \{m'_{IX(1)}, m'_{IX(2)}, \ldots, m'_{IX(256\times256)}\}$. Then convert $M''$ into a matrix $MM = \{mm_{i,n} | i, n = 1, 2, \ldots, 256\}$.