Applied Soft Computing 26 (2015) 10–20

Contents lists available at ScienceDirect

Applied Soft Computing

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

A new image encryption algorithm based on non-adjacent coupled map lattices

Zhang Ying-Qian[a,b], Wang Xing-Yuan[a,*]

[a] Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian 116024, China
[b] City Institute, Dalian University of Technology, Dalian 116600, China

ARTICLE INFO

Article history:
Received 29 January 2013
Received in revised form 26 August 2014
Accepted 23 September 2014
Available online 2 October 2014

Keywords:
Non-adjacent
Coupled map lattices
Image encryption
Bit-level permutation

ABSTRACT

We propose a new image encryption algorithm which is based on the spatiotemporal non-adjacent coupled map lattices. The system of non-adjacent coupled map lattices has more outstanding cryptography features in dynamics than the logistic map or coupled map lattices does. In the proposed image encryption, we employ a bit-level pixel permutation strategy which enables bit planes of pixels permute mutually without any extra storage space. Simulations have been carried out and the results demonstrate the superior security and high efficiency of the proposed algorithm.

1. Introduction

With the rapid development of computer network, the number of image files transmitted over Internet keeps increasing. As a result, the secure transmission of confidential digital images over public channels has become a common interest in both research and application fields. The image symmetric encryption is different from the text symmetric encryption such as DES and AES [1]. The intrinsic properties of images such as bulk data volume, high redundancy and high pixel correlation between adjacent pixels require more efficient permutations and diffusions algorithms of image encryptions than that of text encryptions. In recent years, chaos-based encryption algorithms that rely on dynamicity have been regarded as a promising research for image encryptions. Since Fridrich [2] suggested that a chaos-based image encryption scheme should compose of the iteration of two processes: permutation and diffusion. Presently, various schemes [2–21] have been proposed.

For the permutation phase, bit-level permutation of images is superior to pixel-level permutation due to both the positions and values of pixels changed. In [18], Xiang et al. proposed a selective image encryption scheme that encrypts the higher four bits of each pixel and leaves the lower four bits unchanged. This scheme initiated bit-level permutations in chaos-based image encryptions. Zhu et al. [21] developed a symmetric image encryption scheme using a bit-level permutation. Zhu's method of separation each pixel into groups of bits by calculating percentages of pixel information contributed by different bits is suggested. However, the bits in one bit group cannot be permuted into other bit groups in Zhu's algorithm [21]. Therefore, the statistical information in each bit plane remains unmodified. To avoid this problem, Zhang et al. [20] proposed expand-and-shrink strategy in the permutation phase to significantly reduce the high correlation among the bit planes. However, the expand-and-shrink strategy needs four times extra space for bit-level permutations for breaking the limit of the bit plane. In addition, Zhang's algorithm [20] can only encrypt images of $N \times N$ pixels.

For the diffusion phase, Kanso et al. [8] employed the well known 3D cat map for diffusion phase. However, Xiao et al. [19] presented in advance that the lack of cat map for encryptions is (0, 0)-pixel value unchanged. Zhu's algorithm [21] and Zhang's algorithm [20] employed logistic map for diffusion phase. Nevertheless, the parameter μ of the logistic map has periodic windows in its bifurcation diagrams. Most of chaos-based encryptions such as Zhu's algorithm and Zhang's algorithm assign the parameter μ of the logistic map close to 4 ($\mu = 3.99999$), which can ensure the chaotic behavior of the logistic map. Thus, the limitation in the range of μ indicates that the keystream generated from the chaotic sequences in the logistic map is vulnerable. Besides, in comparison with one dimensional chaotic system, the NCML system contains stronger chaotic behavior, better pseudo random chaotic sequences, wider range of parameters and less periodic

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

http://dx.doi.org/10.1016/j.asoc.2014.09.039
1568-4946/

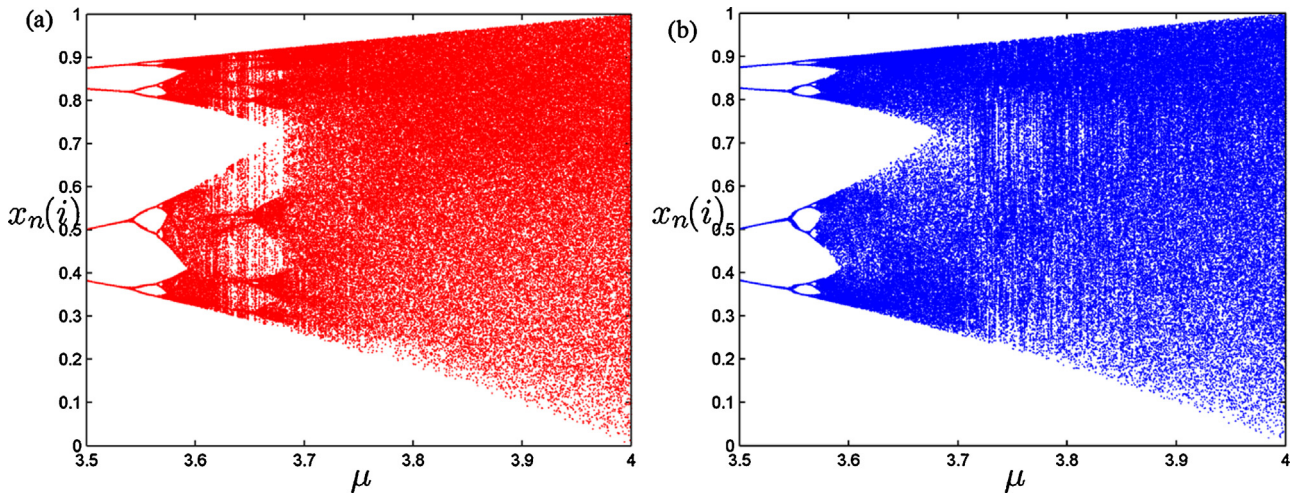

Fig. 1. Bifurcation diagrams. (a) the NCML system, (b) the CML system.

windows in bifurcation diagrams. Therefore, the pseudo random chaotic sequences generated from the NCML system is more secure than that from one dimensional chaotic system. Furthermore, it has been verified that spatiotemporal chaotic systems maintain much longer periodicity in digitalization of the computer than one dimensional chaotic systems [22]. Therefore, spatiotemporal chaotic system is gradually regarded with better properties suitable for image encryptions than one dimension chaotic system, such as larger parameter space, better randomness and more chaotic sequences. The researches [3,6,7,9,10,13–18,26] are based on the coupled map lattices (CML) [23] 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 bifurcation diagram of some lattice. Due to the adjacent lattices coupling, when parameter $\mu \in (3.87, 3.925)$ and $\varepsilon = 0.1$ the system can only generate local chaotic behavior [24] which means that some of lattices are not in chaotic behavior. The number of lattices should be selected carefully for image encryptions. Additionally, the mutual information of chaotic sequences between any two lattices are not zero which indicates that some chaotic sequence of a lattice may be substituted by that of other lattice for potential attacks.

In this paper, we propose a new permutation scheme of the aforementioned image encryption algorithm. The permutation in the proposed algorithm makes it possible for any bit in pixels to break the limit of its bit plane without extra space. Additionally, the new permutation scheme can permute the image in size of $N \times M$. Nevertheless, we employ the chaotic system of the non-adjacent coupled map lattices for diffusion in image encryption. We also develop the dynamics of spatiotemporal system of non-adjacent coupled map lattices. Our work also indicates that the spatiotemporal system of non-adjacent coupled map lattices is more suitable for image encryptions than CML system due to its space non-linear coupling between lattices, less periodic windows in bifurcations and larger range of parameters in chaotic dynamics, when the scheme of non-adjacent coupling is properly chosen. Furthermore, the wide range of choices for the initial conditions and control parameters lead to a large key space. The experimental results presented in this paper show the effectiveness of the proposed image encryption algorithm.

2. Non-adjacent coupled map lattices

The logistic map was originally proposed by May [25]. It is a first-order difference equation represented by $f(x) = \mu x(1-x)$. Non-adjacent coupled map lattices (NCML) that we proposed considers L logistic maps coupled as follows:

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

where i, j, k are the lattices $(1 \le i, j, k \le L)$, ε is the coupling parameter $(0 \le \varepsilon \le 1)$, 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 and k are calculated by a non-adjacent map usually described in non-linear maps such as Arnold cat map, tent map and standard map without loss of generality, The relations of i, j, k are defined by Arnold cat map as follows:

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

where p and q are the parameters of cat map.

The difference between NCML and CML equations resides in the variables j and k in Eq. (2) which are instead of $i-1$ and $i+1$ in Eq. (1), respectively. The CML system is coupled in adjacent lattices, which is a sort of space regular coupling behavior. The parameters p and q turn NCML into diverse dynamics systems due to the use space non-linear map for lattices coupling. When p and q are properly assigned with fixed values, most of these dynamical systems even hold chaotic features while continuously varying the value of μ in the logistic map.

One dimension logistic map is not suitable for data encryptions due to its periodic windows in bifurcation diagrams. The CML system are suggested for data encryptions [3,6,7,9,13–18,26] in recent years partially because periodic windows in bifurcation diagrams of the CML system are fewer than that of logistic map. The NCML system is suitable for data encryptions for the same reason. There are less periodic windows in the bifurcation diagram with $\mu > 3.70$ for the NCML system than that of CML system for $\varepsilon = 0.1$, $p = 23$ and $q = 12$, which is shown in Fig. 1. In addition, the NCML system has a positive value of h (Kolmogorov–Sinai entropy density) for a wider range of values of μ which means the Lyapunov exponents density of NCML system is positive, which is shown in Fig. 2. The bifurcation diagram without periodic windows and Kolmogorov-Sinai entropy density diagram in the NCML system when $\mu > 3.70$ show the new feature for cryptography that the parameter μ which is used as a secret key has a larger key space than logistic map or the CML system.