Commun Nonlinear Sci Numer Simulat 20 (2015) 506–515

Contents lists available at ScienceDirect

Commun Nonlinear Sci Numer Simulat

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

A novel image encryption algorithm based on chaos maps with Markov properties

Liu Quan [a,b,*], Li Pei-yue [a], Zhang Ming-chao [a], Sui Yong-xin [a], Yang Huai-jiang [a]

[a] *State Key Laboratory of Applied Optics, Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Sciences, Changchun 130033, China*
[b] *University of Chinese Academy of Sciences, Beijing 100039,China*

ARTICLE INFO

Article history:
Received 2 September 2013
Received in revised form 17 April 2014
Accepted 1 June 2014
Available online 16 June 2014

Keywords:
Chaos
Markov
Complexity
Cipher

ABSTRACT

In order to construct high complexity, secure and low cost image encryption algorithm, a class of chaos with Markov properties was researched and such algorithm was also proposed. The kind of chaos has higher complexity than the Logistic map and Tent map, which keeps the uniformity and low autocorrelation. An improved couple map lattice based on the chaos with Markov properties is also employed to cover the phase space of the chaos and enlarge the key space, which has better performance than the original one. A novel image encryption algorithm is constructed on the new couple map lattice, which is used as a key stream generator. A true random number is used to disturb the key which can dynamically change the permutation matrix and the key stream. From the experiments, it is known that the key stream can pass SP800-22 test. The novel image encryption can resist CPA and CCA attack and differential attack. The algorithm is sensitive to the initial key and can change the distribution the pixel values of the image. The correlation of the adjacent pixels can also be eliminated. When compared with the algorithm based on Logistic map, it has higher complexity and better uniformity, which is nearer to the true random number. It is also efficient to realize which showed its value in common use.

1. Introduction

In recent years, more and more images are transmitted and stored on the internet. The confidentiality of the information becomes a prominent problem. While, the encryption algorithm make only the authorized users can access the image, which is considered a good solution to the problem. As the traditional encryption algorithms (DES, AES, IDEA and so on) were designed based on text-structure data, they were thought inappropriate applied on image encryption [1,2]. The traditional algorithms have an obvious drawback that the code image is still perceived after encryption. The main reason is that the image data has a special structure that the adjacent pixels have a strong correlation, which is different from text data.

To solve this problem, the chaotic encryption algorithm is attracting more and more attention [3–8]. According to the classification of chaotic systems, the chaotic encryption schemes, which have being proposed, can be divided into analog chaotic cryptosystems utilizing continuous dynamical systems [6,19] and digital chaotic cryptosystems utilizing discrete dynamical systems[3–5,7,8]. In 1998, Baptista [3] proposed a chaotic block cipher based on a lookup table which seemed simply and efficiency attracts many attentions. As the cipher-text may become longer than the plain-text and would not

[*] Corresponding author at: State Key Laboratory of Applied Optics, Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Sciences, Changchun 130033, China. Tel.: +86 13654373620.

E-mail address: lovefirespread@gmail.com (Q. Liu).

http://dx.doi.org/10.1016/j.cnsns.2014.06.005
1007-5704/© 2014 Elsevier B.V. All rights reserved.

distribute uniformly, the algorithm is not widely used. At the same time, Fridrich proposed an image encryption algorithm structure model [4]. He divided the entire algorithm into two stages: permutation and diffusion. The permutation stage is used to rearrange the positions of pixels in the image. It will change the image structure and weaken the correlation of adjacent pixels. The diffusion stage is used to replace the image pixel values with random values so that the distribution of the cipher-text will not depend on the plain-text. The designs of image encryption algorithms almost always followed this model nowadays [4–8]. However, the proposed algorithm is broken [9] by Ercan Solak et al in 2010. The main drawback of Fridrich's algorithm is the diffusion function may be too simple to break. The image encryption algorithms similar to Fridrich's may have the same problem. The weaknesses of the existing chaotic image encryption algorithms are summarized as follows: poor statistical properties of chaotic maps, weak resistance to the CCA attack and CPA attacks, not sensitive enough to the plaintext and the keys, small key space, poor diffusion function and so on.

In this paper, a novel class of chaotic maps with Markov properties is proposed. It can be proved that the map generates a uniformly distributed sequence whose autocorrelation function is δ-like. It has no fixed point which can weaken the weak-key's affect. Through the selection of the parameters, it can avoid finite precision degradation problem similar to Tent map. By compared with Logistic map and Tent map on the complexity analysis, it shows that the sequence is closer to true random number [10]. In order to enlarge the key space, an improved coupled map lattice is proposed, which has better statistical properties. Finally, the diffusion function is redesigned to resist the CCA and CPA attacks.

This paper is organized as follows: firstly, a novel chaos is proposed and its properties are analyzed in Section 2. Then, the image encryption algorithm is described in Section 3. Thirdly, the system is tested in Section 4. Finally, the conclusion is drawn.

2. The chaotic system and its properties

2.1. A novel class of chaotic map with Markov properties

The chaotic map used in the paper is described as formula (1).

$$T(x,p,\sigma)=\begin{cases}\sigma x+\frac{(i+1)-i\sigma}{p}mod1, x\in[\frac{i}{p},\frac{i+1}{p}), & i=0,1,\ldots,p-2\\ \sigma x+\frac{p-(p-1)\sigma}{p}mod1, & x\in\left[\frac{p-1}{p},1\right]\end{cases}\qquad(1)$$

The parameter $p(\mathrm{p}\geqslant 7)$ is a prime number and $\sigma(2\leqslant\sigma\leqslant p-1)$ is a positive integer. The x-domain is divided into p parts uniformly (denoted as $I_1,I_2,I_3,\ldots,I_p$) while each part can goes into the other parts after one step iteration which can construct a certain graph. When the parameter changed, the transition modes of the system states would change as shown in Fig. 1.

The chaotic system proposed above have some useful properties [11] as shown in the following four theorems.

Theorem 1. *$T(x,p,\sigma)$ is sensitive to the initial value x.*

Proof. Let $\mathrm{L}(\mathrm{x},\mathrm{f})$ denote the Lyapunov exponent of $T(x,p,\sigma)$. The set A denote the first class of break points of the map,

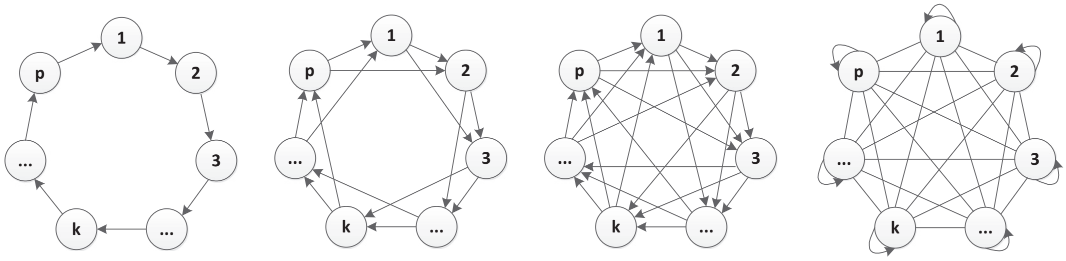
$$\mathrm{A}=\{\mathrm{x}:\lim_{x\to x^-}T(x,p,\sigma)\neq\lim_{x\to x^+}T(x,p,\sigma),\ \text{the left and right limit of }\mathrm{T}(x,p,\sigma)\text{ on x exists}\},$$

If $\mathrm{x}\notin\mathrm{A}$, then $|\mathrm{T}'(\mathrm{x})|=\sigma$.

So that if $x^j=f^j(x_0)\notin\mathrm{A}$, then $\mathrm{L}(\mathrm{x},\mathrm{f})=\ln(\sigma)\geqslant\ln(2)>0$. The map has a positive Lyapunov exponent, which means it is sensitive to the initial value of x. □

Theorem 2. *$I_1,I_2,I_3,\ldots,I_p$ is a Markov portion of $T(x,p,\sigma)$.*

Proof. According to the formula (1), $I_1,I_2,I_3,\ldots,I_p$ is a portion of the x-domain.



(a) $\sigma=1$ (b) $\sigma=2$ (c) $\sigma=3$ (d) $\sigma=p$

Fig. 1. System states transition models with different parameters.