Optics and Lasers in Engineering 66 (2015) 10–18

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

A novel chaotic block image encryption algorithm based on dynamic random growth technique

Xingyuan Wang *, Lintao Liu [1], Yingqian Zhang [2]

Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian 116024, China

ARTICLE INFO

Article history:
Received 2 April 2014
Received in revised form
1 August 2014
Accepted 4 August 2014
Available online 16 September 2014

Keywords:
Cat map
Dynamic random growth
Chaotic system
Block image encryption

ABSTRACT

This paper proposes a new block image encryption scheme based on hybrid chaotic maps and dynamic random growth technique. Since cat map is periodic and can be easily cracked by chosen plaintext attack, we use cat map in another securer way, which can completely eliminate the cyclical phenomenon and resist chosen plaintext attack. In the diffusion process, an intermediate parameter is calculated according to the image block. The intermediate parameter is used as the initial parameter of chaotic map to generate random data stream. In this way, the generated key streams are dependent on the plaintext image, which can resist the chosen plaintext attack. The experiment results prove that the proposed encryption algorithm is secure enough to be used in image transmission systems.

1. Introduction

Nowadays more and more images and videos are transmitted through Internet. This brings great convenience to people in daily life as they can obtain what they want on the Internet conveniently. But there are some problems: the information transmitted on the Internet can be intercepted, tampered and destroyed illegally. So the secure transmission of images has become urgent. Due to some intrinsic features of images, such as bulk data capacity and high correlation among pixels, traditional encryption methods like DES, IDEA and RSA are not suitable for image encryption. Since chaos has the characters of non-periodicity, non-convergence, ergodicity and sensitive dependence on initial conditions, chaos-based image encryption system attracts more and more people's attentions.

The classic encryption frame is the permutation–diffusion pattern suggested by Shannon. Many encryption methods use Arnold cat map or generalized cat map in the permutation section [1,2]. But since short periodic and easy to be cracked by chosen plaintext attack, cat map is not secure to be used in the common way [3,4]. Some proposed image encryption schemes only do XOR operation on the original or scrambling images [5–8]. It is also easy to be cracked by chosen plaintext attack [9,10], since the key stream only depends on the key not related to the plaintext. Recently, some image encryption schemes using double images are proposed to get a good encryption effect [11,12], while other people proposed method using genetic algorithm and DNA sequence [13].

Many other algorithms are also proposed [14–20], and some of them are analyzed [21,22]. In this paper, a new chaos-based block image encryption method is proposed, which is a two rounds algorithm based on permutation–diffusion architecture. Both theoretical and computer simulations show that the algorithm is secure enough to be used in image transmission system.

This paper is organized as following: Section 2 describes Arnold cat map; Section 3 shows the proposed image encryption scheme; Section 4 presents the computer simulation results; Section 5 discusses the security analyses; finally, Section 6 concludes this paper.

2. Arnold cat map

The classical Arnold cat map is a two-dimensional invertible chaotic map defined by

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod 1. \quad (1)$$

But in permutation process of image encryption scheme, it is more common to use the generalized cat map as following:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & 1+pq \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N. \quad (2)$$

* Corresponding author. Tel.: +86 41184707827.
E-mail addresses: wangxy@dlut.edu.cn (X. Wang), liulintao100@yahoo.cn (L. Liu), zhangyq@dlut.edu.cn (Y. Zhang).
[1] Tel.: +86 18940912432.
[2] Tel.: +86 18940965159.

http://dx.doi.org/10.1016/j.optlaseng.2014.08.005
0143-8166/

Here N is the number of rows or columns. That is to say the image is of the size $N \times N$. (x_n, y_n) is the original position of a pixel, and (x_{n+1}, y_{n+1}) is the new position.

It is very fast to permute an image using cat map, which is very important in real-time data transmission, but there are two fatal drawbacks. The cat map permutation process is periodic and can be easily attacked using chosen plaintext attack.

To show the periodic character of cat map, we choose $p=40$, $q=8$ and Lena image with size (124×124) for instance. The permutation results of Lena.bmp are shown in Fig. 1. It can be seen that after five rounds of permutation, we get the plaintext again. So the cat map cannot be used in image transmission system, since the enemy can get the plaintext image of any cipher image just by iterating cat map to the cipher image.

Except for the periodic drawback, cat map can be easily attacked by chosen plaintext method. Firstly, we choose an image, the pixel gray value of which are all 0 except (1, 0) position. We let the gray value at (1, 0) to be 255. In the cipher permuted by cat map, we can find the position of gray value 255, for example (x, y). Then we select another image whose gray value is 0 except (1, 1) position. The gray value at (1, 1) is also 255. We can then get the position of 255 in the corresponding cipher, for example (u, v). Finally we have

$$\begin{bmatrix} x & u \\ y & v \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & 1+pq \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \bmod N. \tag{3}$$

Here the two images we choose are both of size $N \times N$.

According to Eq. (3) we have

$$\begin{bmatrix} 1 & p \\ q & 1+pq \end{bmatrix} \bmod N = \begin{bmatrix} x & u \\ y & v \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \bmod N. \tag{4}$$

Let

$$\boldsymbol{A} = \begin{bmatrix} 1 & p \\ q & 1+pq \end{bmatrix} \bmod N,$$

then $\boldsymbol{A}$ is the equivalent key of cat map.

As it is not secure to use cat map in the common way, we confuse the image in another way, which can eliminate the periodic drawback and resist chosen plaintext attack.

3. The proposed encryption method

The encryption method consists of two processes: permutation and diffusion.

3.1. Permutation process

In the permutation process, we still use Arnold cat map, but in an uncommon way. For $N \times N$ image P, we use logistic maps in this process

$$f: x_{n+1} = \mu x_n (1 - x_n), \tag{5}$$

where x_n is an independent variable; μ is the control parameter of logistic map; $n=0, 1, 2, \ldots$, when $3.5699456 < \mu \leq 4$, the logistic map is chaotic [23]. To overcome the problem of periodic window of logistic map, we do the following steps: firstly, we choose $\mu \geq 3.9$. When $\mu \geq 3.9$, the periodic window of logistic map is little enough to ensure that we will get a non-periodic point as the key after trying just three or four times. If we choose μ and initial value of logistic which are all periodic after five times, then let $\mu=4$ and choose another initial value of logistic map.

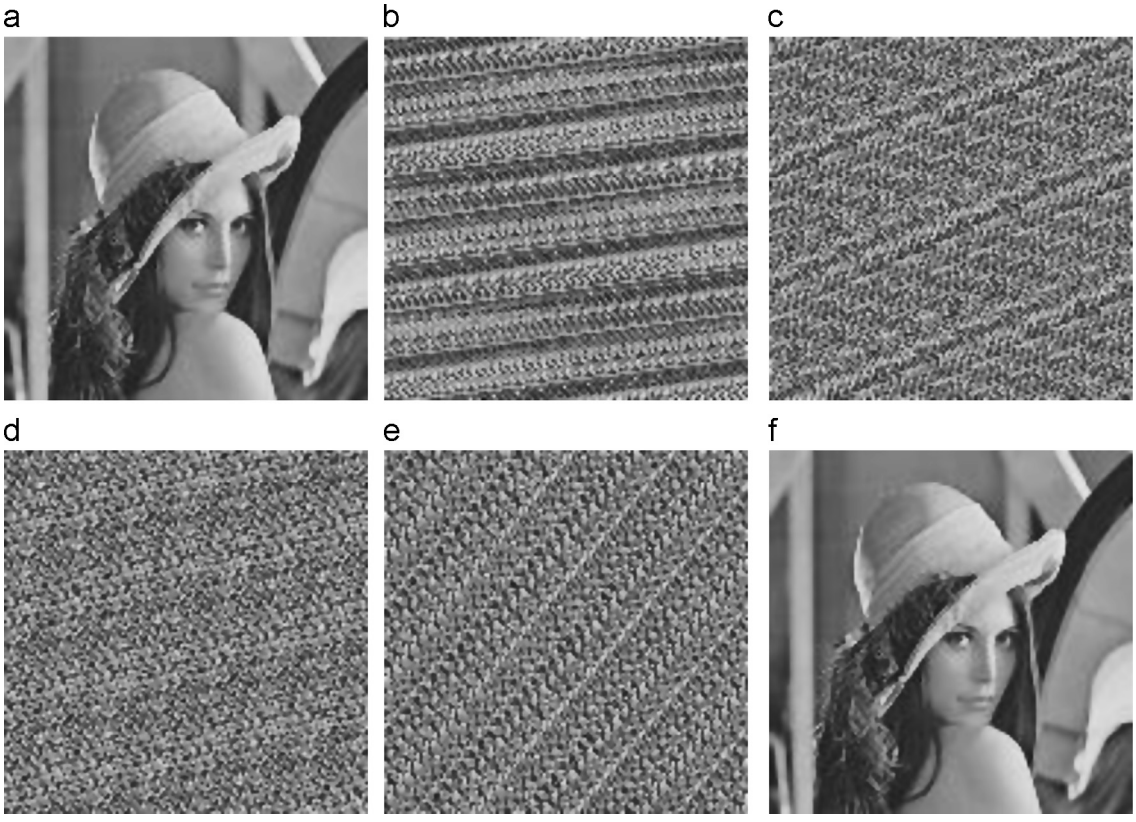

Fig. 1. The periodic feature of Arnold cat map. (a) Original image, (b) 1 round of permutation, (c) 2 rounds of permutations, (d) 3 rounds of permutations, (e) 4 rounds of permutations and (f) 5 rounds of permutations.