Applied Soft Computing 22 (2014) 351–357

Contents lists available at ScienceDirect

Applied Soft Computing

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

A block chaotic image encryption scheme based on self-adaptive modelling

Guodong Ye [a,b], Junwei Zhou [b,*]

[a] College of Science, Guangdong Ocean University, Zhanjiang 524088, Guangdong, China
[b] Department of Electronic Engineering, City University of Hong Kong, 83 Tat Chee Avenue, Kowloon Tong, Hong Kong

ARTICLE INFO

Article history:
Received 16 October 2012
Received in revised form 25 May 2014
Accepted 25 May 2014
Available online 2 June 2014

Keywords:
Error
Division
Hyper-chaos
Logistic map
Modular function

ABSTRACT

In this paper, we suggest a block image encryption algorithm which can give us an efficient scheme to hide and encrypt image data. Only the diffusion function, instead of classical permutation plus diffusion operations, is adopted. The plain-image is firstly divided into two equal parts randomly by vertical, horizontal, or diagonal directions. Then encryption of one part depends on the other part, in which the keystream is generated by the plain-image, i.e., one of the two parts. An error concept is added in the initial conditions in every round. It means that the keystreams are different in the process of encryption steps. The error may be positive or negative decided by a rule of sign function. Experiment results show that the proposed method can provide a high security of cryptosystem, and can reduce the computation redundancy compared with that of the traditional architectures such as Arnold map based method, and totally shuffling based method.

1. Introduction

Chaos-based image encryption has been a keen issue in nowadays. On one hand, traditional methods, such as AES and DES, can not be suitable for digital image because of bulk data capacities, high redundancy, and strong correlations among pixels [1]. On the other hand, it is due to the superior properties of security and complexity, for example, nonlinear equation, sensitivity to initial conditions, control parameters, ergodicity, and random-like behaviour, in the chaotic system [2,3]. Therefore, it has been drawn more and more attentions recently using chaos which has been successfully applied to the image encryption algorithm.

As early as year 1989, Matthew [4] presented a chaotic encryption algorithm, he derived firstly such a chaotic function, and then showed that it was suitable for cryptography. In [5], Shannon pointed out a classical encryption structure, i.e., the confusion plus diffusion functions, which has been adopted in image encryption algorithms [6–10] till now. For simplicity, Logistics map, Chebyshev map and other one-dimensional chaotic maps are widely employed to produce random sequence. However, we know it is not secure enough if low-dimensional chaos is used only, and it has been proved to be weak under brute-force attack. As a result, hyper-chaos based image encryption scheme is naturally brought into our eyes. For example, Gangadhar and Rao [11] proposed hyper-chaotic key based algorithm using hyper-chaos to enhance the security of CKBA. Gao [12] employed an image total shuffling matrix to shuffle the positions of image pixels, and used a four-dimensional hyper-chaotic system to confuse the relationship between the plain-image and the cipher-image. Some other algorithms [13–19] were also suggested to improve the security.

However, the whole permutation-diffusion process should be repeated many rounds to achieve a satisfactory level of security. Permutation based image encryption algorithm has been broken [20] with known-plaintext and chosen-plaintext attack. Additionally, many algorithms [6,8,11,14,21,22] have been found to be insecure in [23–28] respectively. After the security analysis, the main reason is found, i.e., key-dependent problem in the generation of keystream in permutation, or diffusion, or both. However, can we apply the diffusion only to implement the encryption? In this paper, we propose an encryption algorithm using a hyper-chaos system and Logistic map, in which we divide the plain-image into two parts and achieve the diffusion function with modular operation. It can satisfy the rules given by Shannon, i.e., (1) any small value changed in initial conditions should bring us an entirely different cipher-image, (2) a slight change to the plaintext should cause almost all

* Corresponding author at: Department of Electronic Engineering, City University of Hong Kong, 83 Tat Chee Avenue, Kowloon Tong, Hong Kong. Tel.: +852 34429917; fax: +852 3442 0437.
E-mail addresses: guodongye@gmail.com (G. Ye), junweizhou@msn.com (J. Zhou).

http://dx.doi.org/10.1016/j.asoc.2014.05.025
1568-4946/

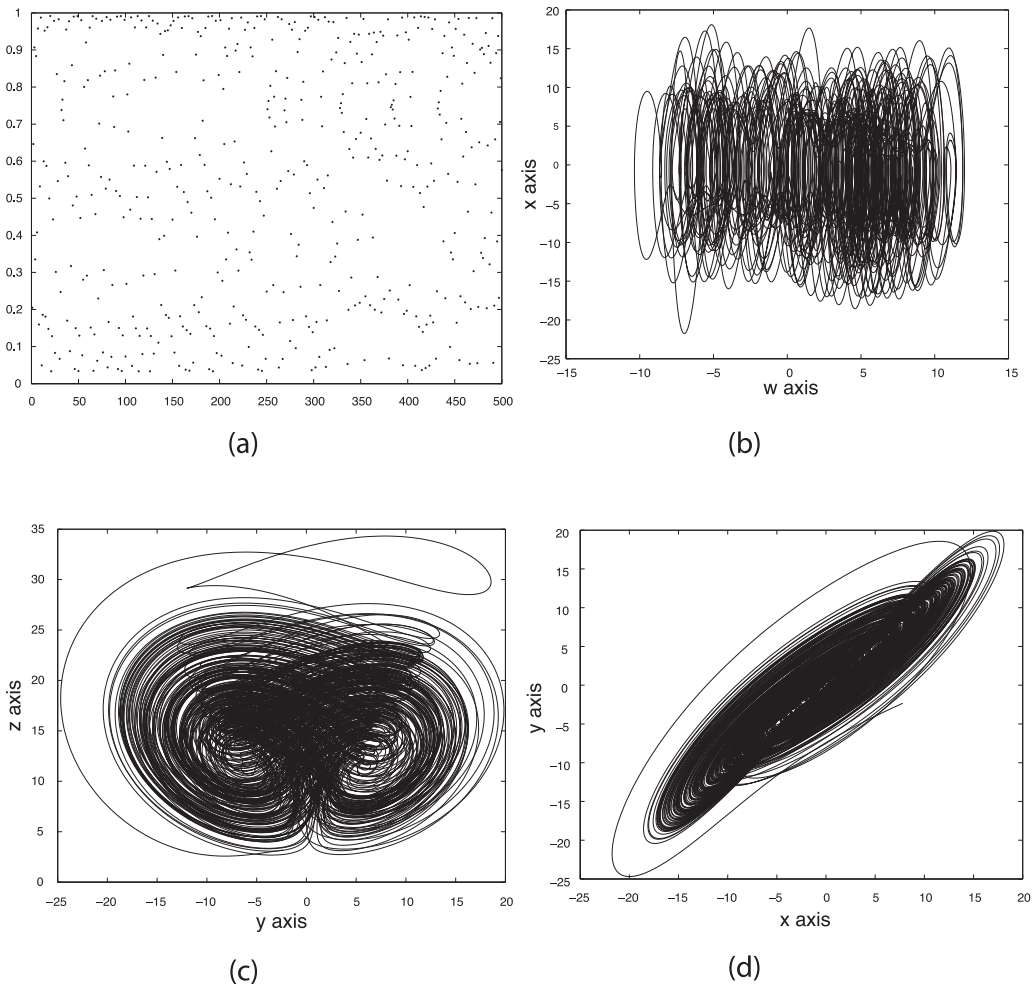

Fig. 1. (a) Logistic map; Hyper-chaos: (b) w–x, (c) y–z, (d) x–y.

the pixel values modified. We produce keystream according to error concept which is dependent on the plain-image. Here, a rule used to judge the sign of error is constructed at the same time.

This paper is organized as follows, double chaotic systems, four methods to divide the plain-image matrix, and error concept are introduced in Section 2. Section 3 lists the steps of the proposed encryption scheme with the encryption and decryption process in detail. The simulation results and performance analyses are shown in Section 4.Finally, Section 5 draws a conclusion for this paper.

2. The preparation for encryption scheme

2.1. Chaotic system

Logistic map is a famous one-dimensional chaotic system with single control parameter. It has been adopted widely to image encryption due to its simple structure. It is described as following Eq. (1).

$$f(x_k) = \mu x_{k-1}(1 - x_{k-1}), \quad k = 1, 2, 3, \ldots. \tag{1}$$

where, $x_k \in (0, 1)$ is time series while μ is the control parameter, and x_0 is the initial value. The parameter μ should be dropped into the field of [3.9,4] to ensure good chaotic properties [9]. Fig. 1(a) shows the chaotic phenomenon of Logistic map.

However, using low-dimensional system solely can not guarantee security, since it can be easily broken by brute-force attack actually. Therefore, the study of high-dimensional system is a general trend. Function (2) is a four-dimensional chaotic system named as hyper-chaotic system [12] with four control parameters and four initial conditions.

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = -xz + dx + cy - w \\ \dot{z} = xy - bz \\ \dot{w} = x + k \end{cases} \tag{2}$$

Here, $a = 36$, $b = 3$, $c = 28$, $d = -16$, and $k \in [-0.7, 0.7]$, the system can be in chaotic state (Fig. 1(b–d) display the chaotic attractor). These two systems (1) and (2) are used in the proposed image encryption scheme.

2.2. Image division and error concept

To reduce the computation of handling with method pixel-by-pixel, we treat the preprocessed image matrix by blocks. The plain-image of size $m \times n$ is shown in Fig. 2. The matrix can be divided into two parts in vertical or horizontal direction [13]. These two parts are decomposed equally according to practical use. Here, we design a new division by diagonal and anti-diagonal lines. In Fig. 2(a) and (b), we use the mid-row and mid-column to depart the image matrix into two parts vertically and horizontally respectively. Fig. 2(c) and (d) shows two parts in upper triangle and lower triangle, of which is divided by diagonal and anti-diagonal line respectively. For simple expression, we take the case of Fig. 2(a) for consideration in this