Signal Processing: *Image Communication* 29 (2014) 902–913

Contents lists available at ScienceDirect

Signal Processing: *Image Communication*

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

Chaotic image encryption based on circular substitution box and key stream buffer

Xuanping Zhang [a], Zhongmeng Zhao [a,*], Jiayin Wang [b]

[a] *Department of Computer Science and Technology, Xi'an Jiaotong University, Xi'an 710049, China*
[b] *The Genome Institute, Washington University in St. Louis, St. Louis, MO 63108, USA*

ARTICLE INFO

Article history:
Received 20 December 2013
Received in revised form
4 June 2014
Accepted 26 June 2014
Available online 3 July 2014

Keywords:
Image encryption
Chaos
S-box
Substitution
Diffusion

ABSTRACT

A new image encryption algorithm based on spatiotemporal chaotic system is proposed, in which the circular S-box and the key stream buffer are introduced to increase the security. This algorithm is comprised of a substitution process and a diffusion process. In the substitution process, the S-box is considered as a circular sequence with a head pointer, and each image pixel is replaced with an element of S-box according to both the pixel value and the head pointer, while the head pointer varies with the previous substituted pixel. In the diffusion process, the key stream buffer is used to cache the random numbers generated by the chaotic system, and each image pixel is then enciphered by incorporating the previous cipher pixel and a random number dependently chosen from the key stream buffer. A series of experiments and security analysis results demonstrate that this new encryption algorithm is highly secure and more efficient for most of the real image encryption practices.

1. Introduction

Digital images have some well-known intrinsic properties such as bulk data capacity, high redundancy, strong correlation among adjacent pixels [1]. Due to these features, traditional text encryption schemes are no longer suitable for image encryptions [2]. Along with the rapid growth of requests for image transmission through open networks, the security of digital image has become an imperative issue [3], and attracted much attention of researchers. Various encryption schemes [4–7] have been developed based on different techniques which are summarized in a comprehensive review in [8]. Among the existing state-of-the-art approaches, chaos-based methods are extensively investigated and a large number of chaos-based encryption algorithms have been proposed [9–13]. This is because chaotic systems have good features of aperiodicity, pseudorandomness, and high sensitivity to initial conditions.

In chaos-based encryption schemes, chaotic maps are generally used as one time pad for encrypting messages. Since image encryption schemes based on low dimensional chaotic map have low computational complexity, they can be analyzed with low computational cost using iteration and correlation functions [14]. Recently, many researchers adopted the high dimensional chaotic maps to improve chaos-based cryptosystems with enlarged key space and long periodicity of chaotic system [15–18]. Nevertheless, some cryptosystems based on high dimensional chaotic maps or spatiotemporal chaotic maps are still not acceptably secure [19–22], where one main reason is that the key stream generated is independent from the plain image and the cipher image [23]. To overcome this weakness, a key stream buffer is introduced in [24] to

* Corresponding author. Tel.: +86 2982668645; fax: +86 2982668971.
E-mail address: zmzhao@mail.xjtu.edu.cn (Z. Zhao).

http://dx.doi.org/10.1016/j.image.2014.06.012
0923-5965/

cache the random numbers generated by the chaotic system, which makes the generated key stream related to the images.

A chaos-based image encryption scheme basically comprises iterations of the confusion and the diffusion [25]. In each iteration, Substitution box (S-box), Permutation box (P-box) or other nonlinear operations are utilized to provide confusion and diffusion. S-box is a type of basic nonlinear components for symmetric key algorithms. Benefiting from its properties, e.g. nonlinearity, differential uniformity and strict avalanche criterion, S-box has been widely used in new encryption strategies. Many researchers have shown attention to utilizing chaotic nonlinear properties to design S-boxes. Lots of S-box construction algorithms [26–29] have been proposed using different chaotic systems. Furthermore, S-box applications in image ciphers become more popular where S-box is progressively considered as a main function for performing substitution. However, it is found that some S-box-only ciphers are vulnerable to chosen plaintext attacks. Zhang and Xiao [30] carefully studied the security issues for the general S-box-only image ciphers and presented a successful cryptanalysis. In order to obtain the secure cipher images, some S-box-based image encryption algorithms either use the dynamic S-boxes [31,32] or incorporate the S-box with other encryption methods [33,34]. For example, in [31], a block cipher with dynamic S-boxes is studied, in which a tent map is chosen to generate S-box that is required in the confusion phase, and then a left-cyclic-shift operation is used for diffusion step. Wang and Wang [32] also proposed a chaotic image encryption algorithm based on dynamic S-boxes, where the image pixels are divided into several groups and each group uses a new S-box generated separately, according to the plain image. In [33,34], image encryption algorithms are proposed by combining S-box transformation with permutation-diffusion scheme, where S-boxes are used for substituting pixels to provide extra confusion.

In this paper we propose a novel secure image encryption scheme based on spatiotemporal chaotic system. The chaotic system constituted by the logistic map and the piecewise linear chaotic map (PWLCM) is adopted to produce random numbers. The proposed scheme consists of a substitution process and a diffusion process. In the substitution process, the S-box is considered as a circular sequence with a head pointer to the start position. For each image pixel, it is replaced with an element of S-box, according to both the pixel value and the head pointer to obtain a cipher pixel. Then the head pointer is reset following the cipher pixel. By this way, each image pixel can be substituted using a different S-box. During the diffusion process, the key stream buffer is used to cache the random numbers generated by the chaotic system. For enciphering an image pixel, a random number is chosen dependently to the previous cipher pixel. Thus, the key stream used in diffusion process is highly dependent on the image. Experimental results on various types of security analysis indicate that the proposed scheme is robust against various common attacks and performs higher encryption speed.

The rest of this paper is organized as follows: Section 2 describes our new image encryption scheme in detail. Section 3 shows results of experiments which demonstrate the performance by various security analysis. We compare our scheme with some existing chaos-based encryption schemes in Section 4, and the conclusion of this paper is given in Section 5.

2. The proposed cryptosystem

The architecture of the proposed scheme is shown in Fig. 1. The pipeline of our scheme is as follows: initially, the external secret key and the size of plain image are utilized to produce the initial states and parameters of the chaotic system. The pseudo-random number generator iterates the chaotic system with the initial states and generates the random numbers for image encryption. Then, the encryption process which consists of substitution and diffusion enciphers each pixel of the image using these random numbers.

2.1. Pseudo-random number generator

The pseudo-random number in encryption process is produced by a spatiotemporal chaotic system. This system is modeled by the Coupled Map Lattice (CML). A CML is an array of states whose values are continuous (usually within the unit interval) or discrete space and time. The CML model adopted in this paper is a two-dimensional dynamical map, which can be described as following [35]:

$$\begin{cases} x_{i+1} = (1-\beta) f_1(x_i) + \beta f_2(y_i) \\ y_{i+1} = (1-\beta) f_1(y_i) + \beta f_2(x_i) \end{cases} \tag{1}$$

where the parameter β controls the strength of the coupling, while the functions f_1 and f_2 are the chaotic maps. Let f_1 be the logistic map and f_2 be the piece-wise linear chaotic map (PWLCM), which are represented as follows, separately:

$$f_1(x) = \alpha x(1-x) \tag{2}$$

$$f_2(x) = \begin{cases} x/\gamma, & 0 \le x < \gamma \\ (x-\gamma)/(0.5-\gamma), & \gamma \le x < 0.5 \\ f_2(1-x), & 0.5 \le x < 1 \end{cases} \tag{3}$$

where $x \in [0,1]$ is the state variable, both $\alpha \in (0,4]$ and $\gamma \in (0,0.5)$ are control parameters.

The initial conditions of the above chaotic system include initial state denoted by (x_0, y_0) and three parameter

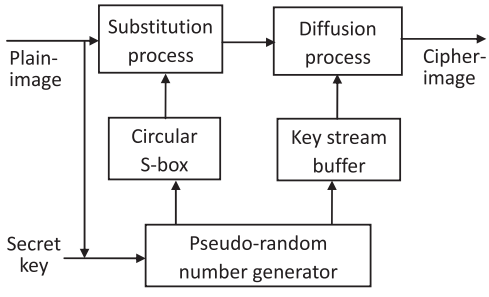

Fig. 1. Architecture of the proposed cryptosystem.