Optics and Lasers in Engineering 78 (2016) 17–25

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

A novel bit-level image encryption algorithm based on chaotic maps

Lu Xu, Zhi Li*, Jian Li, Wei Hua

School of Electronic and Information Engineering, Sichuan University, Chengdu 610065, China

ARTICLE INFO

Article history:
Received 1 April 2015
Received in revised form
6 September 2015
Accepted 7 September 2015

Keywords:
Image encryption
Bit-level
Chaotic maps
Cyclic shift
Swapping

ABSTRACT

Recently, a number of chaos-based image encryption algorithms have been proposed at the pixel level, but little research at the bit level has been conducted. This paper presents a novel bit-level image encryption algorithm that is based on piecewise linear chaotic maps (PWLCM). First, the plain image is transformed into two binary sequences of the same size. Second, a new diffusion strategy is introduced to diffuse the two sequences mutually. Then, we swap the binary elements in the two sequences by the control of a chaotic map, which can permute the bits in one bitplane into any other bitplane. The proposed algorithm has excellent encryption performance with only one round. The simulation results and performance analysis show that the proposed algorithm is both secure and reliable for image encryption.

1. Introduction

Security problems have become more and more serious with the rapid development of the Internet and the advent of smart phones that utilize a large amount of private information, especially images, which are exposed to the network. However, because of the data size and high redundancy among the raw pixels of a digital image, traditional encryption algorithms, such as the data encryption standard (DES), international data encryption algorithm (IDEA) and advanced encryption standard (AES) might not be suitable for image encryption [1]. To prevent image information leakage, many new image encryption algorithms have been proposed by using different techniques, including chaos theory [2–13,25–33], optical transform [14–17], random grids [18], DNA coding [19–22] and compressed sensing [23,24].

Chaotic systems have many excellent intrinsic properties, such as periodicity, ergodicity and pseudo-randomness, and high sensitivity to initial conditions and control parameters. These properties have led researchers to consider the use of chaotic systems for image encryption. Liu et al. [3] presented an image encryption method that is based on one-time keys and robust chaotic maps. In [4], Wang et al. proposed a novel color image encryption algorithm that is based on a logistic map. These authors used a combined permutation and diffusion strategy to reduce the correlations between the R, G, B components and enhance the performance of the encryption. In [5–10], the generalized Arnold map, multiple chaotic map, hyper-chaos, quantum logistic map, coupled map lattices and fractional-order chaotic system were employed to design a secure cryptosystem, respectively. Recently, Zhang and Wang proposed many good encryption algorithms [11–13]. In [11], a new block image encryption scheme based on hybrid chaotic maps and a dynamic random growth technique were proposed, which can eliminate cyclical phenomena and effectively resist a chosen plain-text attack. In [12,13], spatiotemporal non-adjacent coupled map lattices and spatiotemporal mixed linear–nonlinear coupled map lattices were introduced, which have more outstanding cryptography features in terms of their dynamics compared with the logistic map or coupled map lattices. The simulation results in their paper demonstrated the superior security and high efficiency of their algorithms.

Because of the advantages of bit-level permutations, which can change the position and value of a pixel simultaneously, a variety of bit-level image encryption algorithms have been proposed [25–33]. In [25], 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. In [29], Zhu et al. proposed a bit-level permutation scheme for image encryption that is based on the Arnold cat map and logistic map. The parameters of the Arnold cat map are produced by a logistic map. Because the higher four-bit planes contain almost all of the information in the image, they are confused independently, while the lower four-bit planes are permuted as a whole. Nevertheless, in [13,30,31], Zhang and Wang et al. noted that Zhu's algorithm had several weaknesses. First, they permute the bits by the Arnold cat map, which requires the plain image to have an $N \times N$ size. Second, the bits in one bit group cannot be permuted into the other bit groups. Therefore, the statistical information that is in each bitplane remains unmodified. Finally, Zhu's algorithm employed a logistic map for the diffusion phase. The parameter u of

* Corresponding author.
E-mail address: lizhi@scu.edu.cn (Z. Li).

http://dx.doi.org/10.1016/j.optlaseng.2015.09.007
0143-8166/© 2015 Elsevier Ltd. All rights reserved.

the logistic map has periodic windows in its bifurcation diagrams, which indicates that the keystream that is generated from the chaotic sequences in the logistic map is vulnerable. In [33], Teng et al. proposed a bit-level image encryption algorithm that is based on a spatiotemporal chaotic system and is self-adaptive. However, their permutation algorithm has the same weakness as Zhu's algorithm.

To overcome the weaknesses above, this paper proposes a novel bit-level image encryption scheme that is based on cyclic shift, swapping and PWLCM chaotic maps. The PWLCM system has a uniform invariant distribution, good ergodicity and few periodic windows in its bifurcation diagrams. Considering these properties, PWLCM chaotic maps are employed for the proposed algorithm. Additionally, the proposed algorithm can encrypt an image that has the size $M \times N$. Before diffusion and confusion, using the bitplane decomposition method, the plain image is transformed into two binary sequences of the same size. In the diffusion phase, a mutual diffusion strategy between the sequences is introduced. The strategy diffuses these two binary sequences effectively and ensures that a slight modification of the plain image can cause a large number of binary values to be changed in the cipher sequences. In the confusion phase, we swap the binary elements between the two sequences by the control of the PWLCM map, which can make the bits in one bitplane permuted into any other bitplane. Moreover, the proposed confusion algorithm is highly related to the two sequences, which will lead to the cryptosystem effectively resisting differential attacks. The experimental results and simulations have shown that the proposed scheme can achieve excellent encryption performance with only one round, unlike many other bit-level image encryption algorithms.

The remainder of this paper is organized as follows. In Section 2, the basic theory of binary bitplane decomposition and PWLCM chaotic maps is briefly introduced. In Section 3, we describe the proposed algorithm in detail. The simulation results and security analysis are presented in Section 4. Then, the conclusions are given in the last section.

2. Binary bitplane decomposition and PWLCW chaotic map

2.1. Binary bitplane decomposition

In [28], three bitplane decomposition methods were introduced in detail by Zhou. We adopt binary bitplane decomposition (BBD) in our encryption algorithm. In a grayscale image, each pixel value is a decimal number between 0 and 255, which can be represented by an 8-bit binary sequence. BBD can divide a grayscale image into 8 binary bitplanes, and the *i*th bit of the binary representation of each pixel is used to compose the *i*th bitplane.

2.2. The PWLCM chaotic map

The piecewise linear chaotic map (PWLCM) is a map that is composed of multiple linear segments, which are described as in Eq. (1).

$$x_i = F(x_{i-1}, \eta) = \begin{cases} x_{i-1}/\eta, & 0 < x_{i-1} < \eta \\ (x_{i-1} - \eta)/(0.5 - \eta), & \eta \le x_{i-1} < 0.5, \\ F(1 - x_{i-1}, \eta), & 0.5 \le x_{i-1} < 1. \end{cases} \qquad (1)$$

Where the positive control parameter and initial condition are $\eta \in (0, 0.5)$and $x_i \in (0, 1)$, respectively. The map is chaotic when it is in the whole range of parameter of η and has no window in its bifurcation diagram [31]. The logistic map has poor dynamic behavior [31], while PWLCM has better balance and is much closer to being uniform [34].

3. The proposed image encryption system

The block diagram of the proposed image encryption algorithm is given in Fig. 1. First, the plain image is decomposed into eight bitplanes using BBD. Second, the bitplanes are arbitrarily divided into two groups equally. As an example, we choose the four higher bitplanes as one group and the four lower bitplanes as the other group. Then, we transform the two groups into two binary sequences, A_1 and A_2. The elements of the bitplanes are arranged in order from top to bottom, left to right and higher bitplane to lower bitplane, to form A_1 and A_2. In the diffusion phase, chaos, cyclic shifts and the XOR operation are employed to change the bit value in A_1 and A_2, and then B_1 and B_2 are produced. In the confusion phase, we swap the binary elements in B_1 and B_2 by using control from the chaotic map, and then we obtain C_1 and C_2. Finally, through transforming C_1 and C_2 into bitplanes and combining all of the bitplanes, we obtain the cipher image. Round *n* is used to further improve the security of the proposed system. The initial parameters and conditions of the chaotic maps serve as the secret keys.

Before the confusion and diffusion phase, we also need to produce two binary keystream sequences using a secret key, $key_1(x_0, \mu_1)$. Suppose that the size of the plain image is $M \times N$. Then, we set the initial parameter μ_1 and initial value x_0 to iterate the PWLCM map (Eq. (1)) $N_0 + MN$ times and discard the former N_0 values to avoid harmful effects. The chaotic sequence has MN elements, $X = \{x_1, x_2, \cdots, x_{MN}\}$. We use the following formula to convert $X(i)$ to the integer sequence $X_1(i)$.

$$X_1 = \ \mathrm{mod}(floor(X \times 10^{14}), 256). \qquad (2)$$

The elements in $X_1(i)$ range from 0 to 255. We decompose X into eight bitplanes using BBD. In fact, there are eight binary sequences. Then, the sequences are flexibly divided into two groups equally. As an example, we choose four odd bitplanes as one group and four even bitplanes as the other group. Through transforming the two groups into two binary sequences b1 and b2, respectively, we obtain the binary keystream sequences. The elements of the bitplanes are arranged in order from left to right and higher bitplane to lower bitplane to form b1 and b2. Below, the confusion and diffusion phase will be described in detail.

3.1. Diffusion phase

Step 1. Calculate the sum of the elements in A_2, according to Eq. (3).

$$sum_1 = \sum_{i=1}^{L} A_2(i) \qquad (3)$$

where L is the size of A_1 and A_2, and L=4MN.
Step 2. Obtain A_{11} using the cycle shift operation. Here,
A_{11} is the cyclic shift of the A_1 matrix to the right by sum_1 bits.

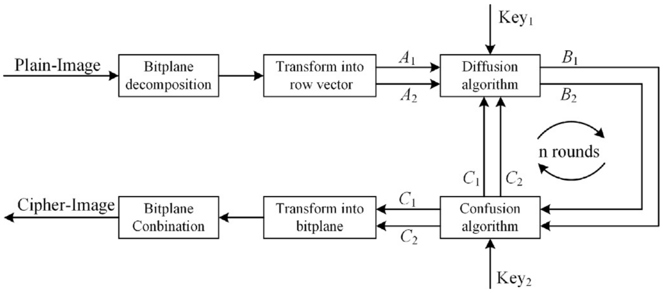

Fig. 1. Block diagram of the proposed image cryptosystem.