Optics and Laser Technology 108 (2018) 558–573

Contents lists available at ScienceDirect

Optics and Laser Technology

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

Full length article

A novel chaotic encryption scheme based on image segmentation and multiple diffusion models

Mingxu Wang [a], Xingyuan Wang [a,b,*], Yingqian Zhang [c], Zhenguo Gao [a]

[a] School of Electronic & Information Engineering, Dalian University of Technology, Dalian 116024, China
[b] School of Information Science and Technology, Dalian Maritime University, Dalian 116026, China
[c] School of Information Science & Technology, Xiamen University Tan Kah Kee College, Zhangzhou 363105, China

ARTICLE INFO

Article history:
Received 12 March 2018
Received in revised form 23 June 2018
Accepted 20 July 2018

Keywords:
Chaotic map
Hash algorithm
Permutation and diffusion
Security analysis
Image encryption

ABSTRACT

Based on image segmentation and multiple diffusion models, a novel chaotic encryption scheme is proposed in this paper. Firstly, a random key is generated to calculate the initial value and control parameter of chaotic map. Secondly, the SHA-512 hash algorithm is used to compute a hash array based on plain image, which is used as secret keys. Finally, according to parts values of that array, an image are divide into sub-blocks and some diffusion model are selected respectively. It is proved by simulation results and security analysis that the proposed scheme has a better security and can withstand common attacks.

1. Introduction

Due to the rapid progress of transmission media, people put forward higher requirements on the security and accuracy of the information. Digital image which is a typical two-dimensional data [1] possessed the inherent features of large size, bulk data capacities, high redundancy, and high correlation among adjacent pixels becomes one of the important forms of multimedia information and has come to occupy a dominant position worldwide. These features both reduce the speed of encryption and decrease the universality of traditional encryption algorithms [2]. Researchers have proposed some image encryption schemes based on a variety of methods and technologies [3–7].

Over the last two decades, chaotic system has been caught researchers' attention due to its tremendous inherent features, such as initial sensitivity, unpredictability and pseudo randomness [8]. Its randomness depend on the initial conditions hence the characteristic is difficult to predict. If we just change initial state of system slightly, a different sequence will output. Based on those properties, extensive studies have been done in this direction [9–11] and have been found that it is similar to the counterparts of cryptography and is quite suitable for cryptography. The obtained chaotic sequence are used to realize the chaotic-based cryptography with the architecture of confusion and diffusion. In the process of confusion, the positions of pixels are randomly scramble. All pixels values are modified in the process of diffusion. After these two operation, the plain image will cannot be recognized correctly.

Nowadays, lots of chaos-based image encryption schemes have been introduced [12–25]. Zhou [13] proposes a simple and effective chaotic system using a combination of two existing one-dimension chaotic maps with larger chaotic ranges and better chaotic behaviors compared with their seed maps. Mollaeefar [15] designs a new scheme for image encryption based on two new chaotic maps with high Lyapunov exponents. Zhou [17] proposes a new two-dimension chaotic map, called the 2d Logistic-adjusted-Sine map, which uses the logistic map to adjust the input of the sine map and then extends its phase plane from one-dimension to two-dimension. Based on existing chaotic systems, other researchers have designed some encryption algorithms [18–25]. Our team have proposed three image encryption schemes by combining spatiotemporal chaos with DNA sequence operations [26], and based on the cryptography characteristics of space-time non-adjacent coupled map lattice [27] and mixed linear-nonlinear coupled map lattice [28] respectively. An effective image encryption scheme can withstand the common attacks, such as brute-force attacks, plaintext attacks, statistical analysis attacks, differential attacks, noise attacks, occlusion attacks. But, there are some schemes which cannot against chosen-plaintext attacks

* Corresponding author at: School of Electronic & Information Engineering, Dalian University of Technology, Dalian 116024, China.
E-mail addresses: wangxy@dlut.edu.cn (X. Wang), zhangyq@xujc.com (Y. Zhang), gzg2012@dlut.edu.cn (Z. Gao).

https://doi.org/10.1016/j.optlastec.2018.07.052
0030-3992/

[2,29–38] and some of these [2,33–38] have been cracked by [39–43]. There are two mainly problems in these schemes: encryption process is not associated with plain image, and the same chaotic sequence is used multiple times.

To overcome the above shortcomings and improve encryption capacity, here we design a novel image encryption scheme based on chaotic system. It is divided into three phase: secret keys generation, image permutation and diffusion. Secret keys consist of two parts: random keys and hash array keys, which will be specifically described in the first phase. Random keys are used to initialize the initial values and control parameters of chaotic system. Hash array keys which are mainly generated by using SHA-512 hash function to compute plain image are carried out to permute the coordinates of the image pixels and to make a confusing relationship between the encrypted and the original image. In the last two phases, we design a segmentation-based image permutation and an effective image diffusion strategy containing three models respectively. In the encryption process, the positions of the image block and the selected diffusion model is determined by part values of hash array.

The remainder of the paper is organized as follows: Section 2 briefly introduces chaotic system and SHA-512 hash function. Section 3 presents the proposed scheme. In Section 4, we organized the obtained simulation results. Section 5 evaluates the security performance of the proposed scheme. Section 6 finally reaches a conclusion.

2. Preliminaries

2.1. Chaotic system

Chaotic systems are extremely sensitive to the initial parameter values and their related evolution function due to their inherent characteristics. This means that a slight change in input parameter value causes huge changes in the value that is generated by the evolution function. Logistic map is one of the most popular chaotic maps, particularly, in image encryption. Logistic map is mathematically described in Eq. (1):

$$x_{n+1} = rx_n(1 - x_n), \tag{1}$$

where the control parameter $r \in (0, 4]$, and x_n represents the output chaotic sequence. Logistic map has a good chaotic behavior when $3.5699456 < r \leqslant 4$. As r gradually close to 4, the chaotic behavior is obviously improved, and the output chaotic sequence x_n is also better. In this paper, we use logistic map three times and define three pairs of parameters $(x_1(0),r_1)$, $(x_2(0),r_2)$ and $(x_3(0),r_3)$. Here $x_3(0)(i = 1, 2, 3)$ represents the initial value, and the control parameter is r_i (i = 1, 2, 3).

2.2. Hash function SHA-512

Hash function can compress the message to a certain fixed length, which is often used in cryptography to protect against brute-force attacks. As broken some hash functions such as SHA-1 are, some encryption schemes are no longer safe. At present, SHA-2 function has not been cracked yet. SHA-512, one of hash function SHA-2, is used to compress plain image P, and obtain a 128-bit hash array. In the encryption progress, we use that array as secret keys to permute the coordinates of the image pixels and to make a confusing relationship between the encrypted and the original image. Even if we change 1-bit value of a pixel of P, the generated hash array is completely different. The complexity of that array is 2^{512}, which is sufficient to withstand brute-force attacks. That array achieves the purpose of one-time pad. For the convenience of description, we give a 128-bit hexadecimal array and denoted as H:

$$H = [h_1, h_2, \cdots, h_{128}]. \tag{2}$$

3. The proposed image encryption scheme

This section introduces a novel image encryption scheme. It consists of three phases: secret keys generation, block-based image permutation, image diffusion based on three models. After this progress, P is encrypted into a totally different image and cannot be recognized.

3.1. Generating initial values and control parameters

In this part, we present a new strategy about the generation of secret keys. It consists of two parts: random keys and hash array keys.

On the one hand, we use random keys to initialize the initial values and control parameters of logistic map. As mentioned in last section, we need six different keys in the progress of using that map three times. The generation procedures are described by the following five steps.

Step 1: Generate three sequences with the length of 8: *RC*, *CC* and *Binary* respectively. Here both *RC* and *CC* are random integer sequences, and all elements of *Binary* are 0;
Step 2: Traverse all values of *RC* and *CC* one by one separately. If the value of *RC* is not smaller than*CC*, the value of corresponding position in *Binary* is 1. Otherwise, the value is 0.
Step 3: Convert *Binary* into a decimal number;
Step 4: Repeat step 1 to 3 six times and add all those decimal numbers to a sequences which length is 6 in turn. That sequence is defined as Eq. (3):

$$Key = [k_1, k_2, \cdots, k_6]. \tag{3}$$

Step 5: Calculate the values of three parameter pairs according to *Key*, as shown in Eq. (4):

$$\begin{cases} x_1(0) = 0.1 + \ mod\ (0.001Key(1), 0.9) \\ r_1 = 3.7 + \ mod\ (0.001Key(4), 0.3) \\ x_2(0) = 0.1 + \ mod\ (0.001Key(2), 0.9) \\ r_2 = 3.8 + \ mod\ (0.001Key(5), 0.2) \\ x_3(0) = 0.1 + \ mod\ (0.001Key(3), 0.9) \\ r_3 = 3.6 + \ mod\ (0.001Key(6), 0.4) \end{cases}, \tag{4}$$

where $Key(i), 1 \leqslant i \leqslant 6$, and i represents the ith value of *Key*.

On the other hand, we call hash function SHA-512 to compute the plain image, and then output a 128-bit hash array. The obtained hash array is used as secret keys to permute all pixels positions and diffuse the all pixels values.

3.2. Encryption scheme description

Similar to most algorithms, there are also two mainly phase in this section: permutation and diffusion.

3.2.1. Segmentation-based image permutation

In this phase, we scramble all pixels positions based on image block. The specific process is described by the following seven steps: