Optics and Lasers in Engineering 000 (2017) 1–10

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Image encryption algorithm based on multiple mixed hash functions and cyclic shift

Xingyuan Wang [a,*], Xiaoqiang Zhu [a], Xiangjun Wu [b], Yingqian Zhang [c]

[a] School of Electronic & Information Engineering, Dalian University of Technology, Dalian 116024, China
[b] College of Software, Henan University, Kaifeng 475004, China
[c] School of Information Science & Technology, Xiamen University Tan Kah Kee College, Zhangzhou, China

ARTICLE INFO

Keywords:
Hash function
Cyclic shift
Chaotic sequences
PWLCM
Image encryption

ABSTRACT

This paper proposes a new one-time pad scheme for chaotic image encryption that is based on the multiple mixed hash functions and the cyclic-shift function. The initial value is generated using both information of the plaintext image and the chaotic sequences, which are calculated from the SHA1 and MD5 hash algorithms. The scrambling sequences are generated by the nonlinear equations and logistic map. This paper aims to improve the deficiencies of traditional Baptista algorithms and its improved algorithms. We employ the cyclic-shift function and piece-wise linear chaotic maps (PWLCM), which give each shift number the characteristics of chaos, to diffuse the image. Experimental results and security analysis show that the new scheme has better security and can resist common attacks.

1. Introduction

The rapid development of Internet and computer technologies greatly facilitates the transmission of digital multimedia content over various communication networks. Information security against illegal copying and distribution has become an urgent and significant topic. Cryptography has the mission to solve the secure transmission of information. Considering the excellent characteristics of chaotic systems, e.g., ergodicity, non-predictability, and high sensitivity to parameters and initial conditions, chaotic image encryption has attracted extensive attention throughout academia and industry. There are many papers that have researched chaotic cryptology, proposed and analysed chaotic cryptosystems, and gradually formed a new research area from nonlinear science. In recent years, chaotic cryptography has been extensively utilized in image encryption [1–8].

A good encryption system should have a large key space, and be sensitive to the plaintext image and key. The histogram of the ciphertext image should be uniformly distributed. The correlation between adjacent pixels should be relatively low. In the past decade, many works in the literature achieved outstanding results. However, some of them are not secure. The most representative is Baptista's scheme, which pioneered the chaotic image encryption [9]. Since using a smaller number of iterations leads to a non-uniform histogram of the ciphertext [10], Baptista's scheme takes much longer to process [11]. Aiming at these flaws, some researchers analysed and proposed the improved algorithms [12–14]. However, such deficiencies remain in most of the improved Baptista algorithms [15–17]. In addition, Norouzi et al. successfully cracked a greyscale image encryption system by chosen plaintext attack [18]; Bechikh et al. utilized a spatiotemporal chaotic system to crack an image encryption scheme [19].

Aiming at the deficiencies of the above cryptosystem, we proposed another one-time-pad image encryption scheme. In this paper, the initial conditions are generated by utilizing multiple mixed hash functions and chaotic maps. We design a novel image scrambling algorithm based on nonlinear equations, which greatly improve the efficiency of this algorithm. We also employ the PWLCM system to replace the logistic map used in the traditional Baptista cryptosystem. The cyclic-shift function with the characteristics of chaos is used to diffuse the image. Simulation results and security analysis show that the new algorithm has high security and can be used to implement an image encryption system.

2. Baptista's system and related chaotic systems

Baptista's cryptosystem usually uses the logistic map as its chaotic map. When parameter $\mu \in (3.5699456, 4)$ and initial $x_n \in (0, 1)$, the system is chaotic.

$$x_{n+1} = \mu x_n(1 - x_n). \quad (1)$$

There are periodic windows in the bifurcation diagram of the logistic map. When $\mu > 3.63$, the behaviours of the chaotic system appear

* Corresponding author.
E-mail addresses: wangxy@dlut.edu.cn (X. Wang), abc2611617@mail.dlut.edu.cn (X. Zhu), wuhsiang@yeah.net (X. Wu), zhangyq@xujc.com (Y. Zhang).

http://dx.doi.org/10.1016/j.optlaseng.2017.06.015
Received 14 December 2016; Received in revised form 19 June 2017; Accepted 20 June 2017
Available online xxx
0143-8166/

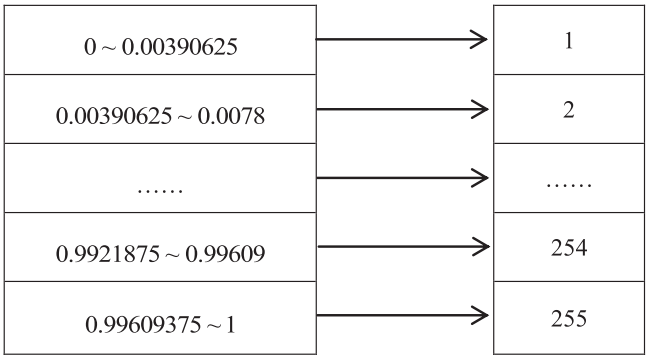

Fig. 1. Subintervals and corresponding integer domain.

similar in strength; when $\mu=3.74$ and $\varepsilon=0.2$, the system exhibits periodic behaviour [20]. To avoid the periodic windows, this paper uses parameters within the range of $\mu \in (3.89, 4]$. In addition, when $a \neq 4$, some subintervals of the trajectory cannot be accessed through iteration. Therefore, the Baptista cryptosystem can only select a part of the attractor, inter alia, and only the interval [0.2, 0.8] can be selected as an encryption interval. If the chaotic trajectories are outside of the interval[0.2, 0.8], the efficiency is very low because the chaotic system requires additional iterations [21].

This paper utilizes the PWLCM system to avoid the deficiencies of the logistic map in the traditional Baptista cryptosystem. The PWLCM system has been extensively used in image encryption schemes because of its good chaotic characteristics [22–24]; its description is as follows:

$$x_n = F(x_{n-1}, \eta) = \begin{cases} \frac{x_{n-1}}{\eta}, & 0 < x_{n-1} < \eta \\ \frac{x_{n-1}-\eta}{2-\eta}, & \eta \le x_{n-1} < 0.5 \\ F(1-x_{n-1}, \eta), & 0.5 \le x_{n-1} < 1 \end{cases}. \tag{2}$$

When $\eta \in (0, 0.5)$, the PWLCM system exhibits chaotic behaviours [25], and the output chaotic sequence distributes uniformly over the entire range of [0, 1]. Therefore, this effective range can avoid invalid iterations and improve the efficiency of the scheme.

The vital difference between a chaotic system and cryptography is in that a chaotic system is defined on the real number field while cryptography is defined on a finite integer domain [26]. Thus, the division of the attractors in this chaotic system divides chaotic sequences into subintervals. The initial value of the PWLCM system is generated by utilizing plaintext information, and then these generated subintervals are associated with the plaintext. This means that if a discrete value in the chaotic trajectory is in a subinterval, it will become an integer value. The interval [0, 1] will be divided into 256 subintervals in this paper, and they correspond to a list of integers in the ascending order, which is shown in Fig. 1.

3. Scheme description

3.1. Generating initial values and control parameters

Hash functions play a major role in image encryption systems. Due to the irreversibility of hash functions, they can resist the known-plaintext attack, chosen-plaintext attack and chosen-ciphertext attack [27]. This paper mixes the SHA1 function and the MD5 function for applications. The SHA1 function can generate a hash value of 160 bits, and the MD5 function can generate a hash value of 128 bits. To enhance the security of the scheme, we proposed an algorithm that utilized multiple mixed hash functions. The formula is as follows:

$$R = \mathrm{SHA1}(\mathrm{hex2dec}(\mathrm{MD5}(a)) \oplus \mathrm{hex2dec}(\mathrm{MD5}(key))), \tag{3}$$

where $\oplus$ represents the XOR operation, and the function hex2dec(·) converts a hexadecimal number to a decimal number. The *key* is set to a very complex string, and a is a part of the plaintext information. Then, the plaintext is associated with hash functions. It is almost impossible for the attacker to track the value of R through an exhaustive method without knowing the *key*. In addition, a hash value of 40 bits can be expressed as a hexadecimal array H:

$$H = [h_1, h_2, ..., h_{40}]. \tag{4}$$

The initial conditions and control parameters are generated by the following method:

First, for a plaintext image P with a size of $M \times N$, where P_i represents pixel value i, we randomly select 16 points and 8 points of the plaintext image and calculate their average pixel value by Eqs. (5) and (6), respectfully:

$$a_1 = \mathrm{floor}\left(\sum_{i=1}^{16} P_i/16\right), \tag{5}$$

$$a_2 = \mathrm{floor}\left(\sum_{i=1}^{8} P_i/8\right), \tag{6}$$

where floor(·) represents the greatest integer less than or equal to the argument. This paper gives the values of key_1 and key_2, which are used as the keys, and calculates two hash values R_1 and R_2. In particular, if the MD5(a) is calculated, we abnegated the first 5-bit hash value of its result; if MD5(*key*)is calculated, we abnegated the last 5-bit hash value of its result. Next, we calculate the R_1' and R_2' by Eqs. (7) and (8):

$$R_1' = \mathrm{hex2dec}(H(h_{11} : h_{15})) \oplus \mathrm{hex2dec}(R_1(r_{11} : r_{15}))/M \times N, \tag{7}$$

$$R_2' = \mathrm{hex2dec}(H(h_{16} : h_{20})) \oplus \mathrm{hex2dec}(R_2(r_{16} : r_{20}))/M \times N. \tag{8}$$

As described earlier, there are periodic windows in the Logistic map. Therefore, we use parameters within the range of $\mu \in (3.89, 4]$, and we calculate the control parameter μ_0 through the linear transformation shown in Eq. (9):

$$\begin{cases} \mu = \mathrm{hex2dec}(H(h_1 : h_8))/10^{10} \\ \mu_0 = 0.11 \times \mu + 3.89 \end{cases}. \tag{9}$$

Finally, we use R_1' and R_2' to calculate the initial value x_0 and control parameter η of the PWLCM system and Logistic map by Eqs. (10) and (11):

$$x_0 = (1/(a_1 + b) + R_1') \bmod 1, \tag{10}$$

$$\eta = (1/(a_2 + b) + R_2') \bmod 1, \tag{11}$$

where mod(·) is the modulus operator, and the parameter of b is set to a key.

3.2. The proposed image encryption scheme

Suppose a plaintext image P of size $M \times N$ is given, where M is the number of rows and N is the number of columns. The encryption process is as follows:

Step 1. According to the hash array H and pixel values of plaintext P, we calculate the initial value x_0 and control parameters μ_0 and η by the above method. The hash array H and parameter b are used as the keys of this encryption scheme.

Step 2. We use two Logistic maps to calculate a set of chaotic coordinates $f(x_i', y_i')$ by Eq. (12) and iterate $M \times N$ times:

$$\begin{cases} x_{n+1} = 3.965 x_n (1 - x_n) \\ y_{n+1} = 3.965 y_n (1 - y_n) \\ x_i' = \mathrm{floor}(x_{n+1} \times 10^{14}) \bmod M + 1 \\ y_j' = \mathrm{floor}(y_{n+1} \times 10^{14}) \bmod N + 1 \end{cases} \tag{12}$$

where $i=1, 2, ..., M$, $j=1, 2, ..., N$, $x'_i \in [1, M]$, and $y'_j \in [1, N]$. The given initial values of x_{00} and y_{00} of the Logistic map are used as the keys of this encryption scheme.