Optics Communications 338 (2015) 209–217

Contents lists available at ScienceDirect

Optics Communications

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

A novel image encryption algorithm based on chaotic system and improved Gravity Model

Xing-yuan Wang*, Na Wei, Dou-dou Zhang

Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian 116024, China

ARTICLE INFO

Article history:
Received 8 July 2014
Received in revised form
17 October 2014
Accepted 18 October 2014
Available online 27 October 2014

Keywords:
Image encryption
Logistic map
Improved Gravity Model

ABSTRACT

In this paper, an image encryption based on chaotic system and improved Gravity Model is presented. Firstly, the original image is shuffled according to two chaotic sequences generating by logistic map. Secondly, the shuffled image is diffused using the improved Gravity Model. Thirdly, in order to improve the influences of the encrypted image by changing one-pixel on the plain image, the logistic chaotic system is used to further diffusion once again. Many experiments are done and security analyses are discussed, which show that the novel algorithm has good effect and it can resist common attacks.

1. Introduction

According to Shannon's theory, practical encryption algorithms include bit diffusion and confusion, sensitivity to plain text and keys, and computational unpredictability. These fundamental concepts in cryptology are very similar to corresponding concepts in chaos theory, such as ergodicity and mixing, sensitivity to initial values, Lyapunov exponent and strange attractor. Therefore, cryptography can be thought of as a specific application of chaos theory [1].

Chaotic systems have good features of sensitive dependence on initial conditions, pseudo-randomness, periodicity and reproduction. So the algorithms based on chaos have proved to be superior for encrypting images [2–4]. In recent years, a large numbers of chaotic systems have been employed in cryptosystem in order to get larger key space. But with the increasing ability of the computer calculation, an encryption scheme only with simple chaotic model can cracked easily. So in this paper, In order to improve the complexity and difficulty of decryption, we will use Gravity Model to enhance the property of diffusion [5–7].

The Law of universal gravitation was first proposed by Newton in Philosophiae Naturalis Principia Mathematica in 1687 [8], which states that any two particles are attracted to each other in nature. The formula is $F = GMm/r^2$, where G is the gravity coefficient, M, m are the quality of particle, r is the distance between them. According to this equation, we can find that magnitude of the gravitational force is proportional to quality and is in inverse proportion to the distance between them. In this paper, assuming that there is a particle in the space and it produces force to the pixels of the image. We use the force to change the value of pixel, so as to achieve the purpose of diffusion. Gravity Model is first used to image encryption in by Sun and Chen in 2006 [9]. But there are many problems in this paper, such as: his algorithm has good effect only the Gravity coefficient (G) is very lager, so which may lead to this method failure subjecting to the conditions of computer storage capacity. Except that, his algorithm is not sensitivity to secret keys and the Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) is very poor [10].

Motivated by the above discussion, in our paper we will purpose a new image encryption algorithm based on chaotic system and improved Gravity Model in order to overcome the malpractices. The simulation results show that the proposed algorithm has properties of big key space, high sensitivity to key, resisting differential attacks, and statistical analysis.

The rest of the paper includes: In Section 2, the encryption and decryption algorithm will be presented; Section 3 shows the experimental results and analysis. Finally, Section 4 concludes the paper.

2. The preliminaries

2.1. The logistic map

In the proposed algorithm, logistic map is used to generate chaotic sequences, which is used to shuffle and diffuse the current

* Corresponding author.
E-mail addresses: wangxy@dlut.edu.cn (X.-y. Wang), weina19900925@gmail.com (N. Wei), doudou19890215@126.com (D.-d. Zhang).

http://dx.doi.org/10.1016/j.optcom.2014.10.042
0030-4018/

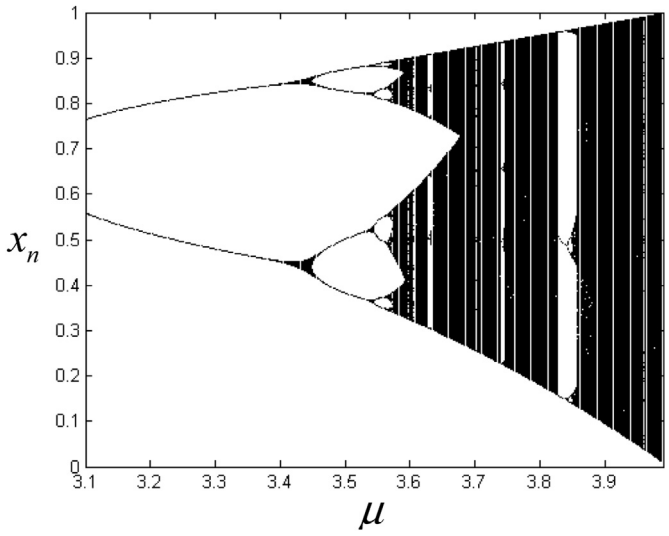

Fig. 1. The bifurcation diagram of logistic map.

pixels. The Logistic map can be presented as Eq. (1) [11,12].

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

where $x_n \in (0, 1)$ and $u \in (0, 4]$. The bifurcation diagram of logistic map is shown in Fig. 1. From Fig. 1 it can be displayed that when $u \in (3.9, 4]$, the system is chaotic and the pseudorandom sequence between 0 and 1 can be got.

2.2. The improved Gravity Model

Suppose a $K \times N$ plain image $I = \{0 \le f(i, j) \le 256; i = 1, 2, \ldots, K; j = 1, 2, \ldots, N\}$ as the $K \times N$ particles in same plane of space. There is a particle (E) in the space of different plane and the quality (m_{ij}) of any pixel is not zero, the location of image as Fig. 2. So gravity exists between particle and pixels. Thus we can use it to change the value of pixel. In order to overcome the malpractice in algorithm purpose by Sun, the Gravity Model can be represented as follows:

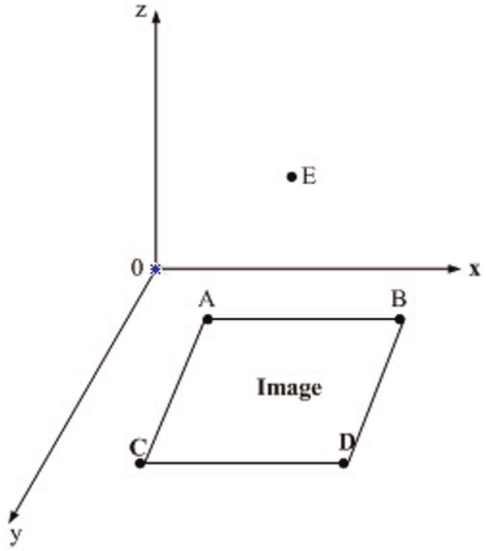

Fig. 2. Sketch map of image in the *XOYZ* plane.

$$B'_{ij} = \left[\frac{Gm(x, y, z)m_{ij}(i, j)}{(x - i)^2 + (y - j)^2 + z^2}\right] \bmod 256 \oplus B_{ij} \tag{2}$$

where G is gravity coefficient, $m(x, y, z)$ is the quality of particle (E), (x, y, z) is the location of particle. In order to guarantee the denominator isn't zero, in this paper we stipulate $z \neq 0$. $m(i, j)$ is the quality of pixel, (i, j) is the location of pixel. B_{ij} is the pixel value of plain image, B'_{ij} is changed value of pixel by Eq. (2), mod: returns the remainder after division. In theory, G,$m(x, y, z)$ and $m(i, j)$ must larger than zero, and $Gm(x, y, z)m_{ij}(i, j)$â^a¢$(x - i)^2 + (y - j)^2 + z^2$. In following, we use different G,$m(i, j)$, $m(x, y, z)$ to express the information hiding using by this model remaining $x = 100$, $y = 300$, $z = 100$ unchanged.

From Fig. 3 We can find that when $m(x, y, z) = 1$, $m(i, j) = 1$, G is very small, the effect of information hiding is very poor, which can be used in Digital Watermarking. So, we should adjust G in the application, but which may lead to G exceed the storage capacity of the computer, and the key less sensitivity to G. From Fig. 4 we find that we can use $m(i, j)$, $m(x, y, z)$ to overcome this disadvantage. All of that will be proved later.

3. Description of algorithm

3.1. Cipher algorithm

Input: Any $K \times N$ image F, the common initial values of u and x_0 for logistic map.

Output: the ciphered image F'.

Step 1: Generate two chaotic sequences x_{1i} and x_{2i} by Eq. (1). x_{10}, x_{20}, u_{10}, u_{20} are the parameters as initial secret keys, where $i = 1, 2, \ldots, K \times N$.

Step 2: We use sequence x_{1i} and x_{2i} to generate $H_1(i)$ and $H_2(i)$ by Eq. (1).

$$\begin{cases} H_1\text{: floor}(\bmod(x_{1i} \times 10^{12}, N) + 1) \\ H_2\text{: floor}(\bmod(x_{2i} \times 10^{12}, K) + 1) \end{cases} \tag{3}$$

where $i = 1, 2, \ldots, K \times N$, floor$(x)$ returns the value of x to the nearest integers less than or equal to x.

Step 3: On the image F, we exchange the value of $F(i)$ and $F(H_1(i))$ by row scan. k stands for row variable, n stands for column variable. k is changed from 1 to K by adding 1 once as the outer loop and n is changed from 1 to N by adding 1 once as the inner loop, we exchange the value of $F(K \times N)$ and $F(H_1(K \times N))$ till $k = K$ and $n = N$. At last we get an image F_1.

$$F((k - 1) \times N + n) \leftrightarrow F(H_1((k - 1) \times N + n)) \tag{4}$$

Step 4: On the image F_1, we exchange the value of $F_1(i)$ and $F_1(H_1(i))$ by column scan; column scan is similar to the row scan. k is changed from 1 to K by adding 1 once as the outer loop and n is changed from 1 to N by adding 1 once as the inner loop, we exchange the value of $F_1(K \times N)$ and $F_1(H_2(K \times N))$ till $k = K$ and $n = N$. According to exchange the value of image pixel by row scan and column scan, we get the image F_2 as pixel position shuffling image.

$$F_1(k + (n - 1) \times K) \leftrightarrow F_1(H_2(k + (n - 1) \times K)) \tag{5}$$

Step 5: On the image F_2, change the value of pixel according to improved Gravity Model, G, x, y, z, $m(x, y, z)$, $m_{ij}(i, j)$ are as key. So, we can get the diffused image F_3.

$$B'_{ij} = \left[\frac{Gm(x, y, z)m_{ij}(i, j)}{(x - i)^2 + (y - j)^2 + z^2}\right] \bmod 256 \oplus B_{ij}$$

where $i = 1, 2, \ldots, K$, $j = 1, 2, \ldots N$