Analysis and Improvement of Image Encryption Algorithm Based Translation Chaotic System

Yue LIU*

College of Electrical and Electronic Engineering, Changchun University of Technology, Changchun 130012, China

*Corresponding author

Keywords: Translation chaotic system, Image encryption and decryption, Cryptographic system.

Abstract. In this paper, we propose and improvement the translation chaotic system is applied to the field of image encryption and decryption, which is analyzed for Lena image. For the cryptographic system studied, firstly, the row and column of the image are used to map the correlation between pixels by Logistic mapping. Secondly, we use the translation chaotic system to mix the structure and pixel of the image to generate the key stream. Finally, the simulation results show that the encryption part proposed in this paper can be completed without knowing anything about the image key. In the decryption section, we only need to know the initial value set in the encryption system to completely crack the encryption system.

Introduction

In recent years, the security of digital images has attracted much attention in computer communication and network engineering [1,2]. Since Mathews, a British scholar, first proposed the "chaotic cipher" in 1989, many scholars had studied the close relationship between chaos and cryptography, such as Logistic [3], Arnold cat [4,5], Chebyshev and Henon mapping, and others algorithms, which based on some mathematical transformations[6-11]. Jessica Fridrich, the first person, whom applied chaos theory to image encryption, in 1997 [3]. In 2005, Z Guan and fellows proposed a new encryption algorithm based on Arnold cat mapping [4,5]. In 2009, Xiao D and fellows analysis and improvement it[5]. In the same year, Cahit Cokal and et al analyzed the security of this algorithm [4]. In 2008, R Rhouma and B Safya first applied Logistic mapping to hyperchaotic systems [2,3]. In 2009, K Wong pointed out that an existing image encryption system based on chaos includes two stages: substitution and diffusion. The multi-dimensional chaotic mapping usually uses the image pixel arrangement in the alternative phase, and the one-dimensional (1D) chaotic mapping is used for the purpose of diffusion, and an efficient chaotic image encryption and diffusion method is proposed [6]. In 2010, Narendra Singh and Aloka Sinha proposed Chaos based multiple image encryptions using multiple canonical transforms [7]. In the same year, Lang J and others proposed image encryption based on the multiple-parameter discrete fractional Fourier transform and chaos function [8], and so on. The results on chaos have also obtained. That is, the translation-type chaotic systems were proposed [12,13] by Liu in 2016.

Inspired by previous works and used the unique properties of this chaotic system, which can be related to the cryptography that has the character of "chaos" and "diffusion". Therefore, it is a natural idea to enrich the design of new cryptographic schemes based chaos. And so far, many applications have been put forward in the field of chaotic ciphers, especially the direction of image encryption. Undoubtedly these results will improve this chaotic system application value in the image encryption and cryptographic system.

We now outline the remainder of this paper. The encryption algorithmic based on the translation chaotic system is described in Section II. In Section III, the result of simulation and analysis are also given to illustrate. Finally, concluding remarks are given in Section IV.
Image Encryption Algorithmic

This encryption scheme consists of two parts: (1) the encryption based on the overall reset of the image pixel matrix; (2) using the translation chaotic system to form a key stream, which can be embedded in the pixel image.

Firstly, consider the image with a size of $N \times M$, which is represented by $P_{i,j} (i = 0, \ldots, M-1, j = 0, \ldots, N-1)$. By Logistic mapping, the initial condition is $x_0$

$$x_{n+1} = 4x_n(1 - x_n) \quad (1)$$

Then, after a series of $n$ iterations, the final state $x_n$ is obtained. Further, set $x_n$ to the new $x_0$ and $h_i$ as follows

$$h_i = \text{mod}(x_0 \times 10^{14}, M) \quad (2)$$

That is the iterative process of Logistic maps. Until the group $M$ different data ($0 \sim M-1$) were obtained, namely $h_i, i = 0, \ldots, M-1$, where $h_i$ indicates $ith$ after disturbance, as $P^h$. Then, each column of the $P^h$ is rearranged in the same way to get a comprehensive reset of the pixel matrix of the image, which is called mixed images, as $P^{hl}$. The following equation is used to calculate the pixel location of each row of the mixed column.

$$l_{i,j} = \text{mod}(x_0 \times 10^{14}, N) \quad (3)$$

where, each column is $i = 1, \ldots, M$, each row is $j = 1, \ldots, N$, $l_{i,j} \epsilon [0,N-1]$.

Secondly, the translation chaotic system is described as follows

$$\begin{cases}
    x_1 = -x_1 + x_3 \\
    x_2 = 2x_3 - [\text{sgn}(x_1 + x_2 + x_3 + 1) + \text{sgn}(x_1 + x_2 + x_3 - 1)] \\
    x_3 = -2x_2 + 0.1x_3 + 1.9 \times 1/2 [\text{sgn}(x_1 + x_2 + x_3 + 1) + \text{sgn}(x_1 + x_2 + x_3 - 1)]
\end{cases} \quad (4)$$

The encryption scheme is based on the combination of the state variables of the image pixels and this chaotic system. The steps are as follows:

1. The system (4) is iterated $N_0th$ time.
2. Generated three variables from the chaotic system and transformed them into integers.
3. $x_i = \text{mod}( |x_0| - \text{Floor}(|x_0|) \times 10^{14}, 256 ) \quad (5)$

3. $x_1$ are generated as follows

$$x_1 = \text{mod}(x_1, 3) \quad (6)$$

Based on the value of $x_1$, according (5), three variables ($B_1, B_2, B_3$) are selected from three variables ($X_1, X_2, X_3$) to perform the encryption operation. Then, three key streams are defined, namely $B_K, k = 1, 2, 3$, as follows:

$$\begin{align*}
    C_{3i(\sim 1)} &= P_{3i(\sim 1)} \oplus B_1 \\
    C_{3i(\sim 1)} &= P_{3i(\sim 1)} \oplus B_2 \\
    C_{3i(\sim 1)} &= P_{3i(\sim 1)} \oplus B_3
\end{align*} \quad (7)$$
where $P_i$ and $C_i$, $i = 1, 2, \ldots, N\times M$, representing the reset image $P^{hl}$ and the encrypted image, respectively.

(4) Continued iterate the chaotic system and repeat steps (2) until the whole image is completely encrypted. The process of decryption is to decrypt the encrypted image of the chaotic system by using the same parameters and initial values. And then the image is generated by anti-shuffling, and the decrypted image can be obtained.

Simulation

In this section, the proposed image encryption algorithm is applied to the Lena image. The original image as shown in Fig.1(a), the size is 256 ×256, which is processed in the following order: Image gray-scale processing as shown in Fig.1(b); Image approximation of the original image as shown in Fig.1(c) and then, the low frequency, the low frequency vertical and the high frequency of the original image are extracted as shown in Fig.1(d–f); Finally, The histogram as shown in Fig.1(g).

![Figure 1. Original image and its processing: (a) Original image; (b) Gray-scale processing; (c) Image approximation; (d) Low Frequency; (e) Low frequency Vertical; (f) High Frequency; (g) Histogram.](image1)

The encrypted image is shown in Fig.2 (a). The histogram as shown in Fig.2 (b). And then, the encrypted image is reconstructed by wavelet, and the reconstructed image is shown in Fig.2 (c).

![Figure 2. The encrypted image and its processing: (a) Histogram; (b) Encrypted image is reconstructed by wavelet; (c) Reconstructed image.](image2)
When the encrypted image is decrypted, the same parameters and initial values are selected. First, the decrypted wavelet reconstruction is performed on the encrypted image, as shown in Fig.3 (a); the histogram as shown in Fig.3 (b); then, the anti-shuffle produces decryption images, as shown in Fig.3 (c); if the decryption method is incorrect, the decryption is not successful, as shown in Fig.3 (d).

As we can see from Fig.3, if the same parameters and initial values are selected, decryption image could be obtained. However, even if the same algorithm, if the different value are chosen, the decryption image could not be obtained.

![Figure 3. The decrypted image and its processing](image)

(a) (b) (c) (d)

Figure 3. The decrypted image and its processing: (a) Gray-scale processing; (b) Histogram; (c) Anti-shuffle produces; (d) Different parameters and initial values are selected.

Summary

In this paper, image encryption algorithm are analyzed and improvement based the translation chaotic system. Firstly, four steps of this algorithm introduced in detail. Then, this algorithm is applied to Lena image, which information are extracted. Finally, the simulation results shown that the encryption can be completed decryption without anything about image key. And then, the decryption process, the same parameters and initial values must be selected as the key stream, otherwise failed.

References


