Advanced Engineering Forum
ISSN: 2234-991X, Vol. 1, pp 183-187
doi:10.4028/www.scientific.net/AEF.1.183
© 2011 The Author(s). Published by Trans Tech Publications Ltd, Switzerland.
Online: 2011-09-09

A New Algorithm of Image Encryption Based on 3D Arnold Cat

Pan Tian-gong [a], Li Ta-yong [b]

College of Measurement-Control Tech & Communications Engineering, Harbin University of Science and Technology, Harbin, 150080, China

[a] ptg99@163.com, [b] dyli@hrbust.edu.cn

Keywords: image encryption, Arnold cat map, chaotic theory, logistic map

Abstract. 3D Arnold cat map can be applied in image encryption, and it has more security and better effect. However, its period is fixed. The original image will be returned to itself if iterating some times. On the basis of 3D Arnold cat map, it presented an algorithm of image encryption which separates the original image to many same blocks and no period. Simulation analysis shows that the encryption algorithm has characters of strong keys, better effect and fast.

Introduction

Image encryption is very important method in many fields such as military, medical system and communication [1]. The classic algorithms of image encryption [2,3,4], including Arnold cat transform, baker's transformation, Hilbert transformation and Zigzag transformation and so on, in which the Arnold cat transformation is most widely used, scrambling effect is relatively best, but the key of Arnold cat is smaller, and visual effects is also less than ideal [5]. At the same time, these image encryption algorithms applying mathematics transformation are carried out from position scrambling, the image pixel values have not changed, that is, no change the gray histogram, so the attacker can analyze through statistical means.

From the substance of image scrambling, this paper proposes an algorithm of image encryption based on 3D Arnold cat map, combined with logistic chaotic map to image encrypt. The encryption system can be applied in medical image processing and transformation. The experiments show that the feasibility and effectiveness of the algorithm.

The 3D Arnold Cat Map and Logistic Map

Arnold Cat Map. Arnold cat transformation is a classical encryption algorithm. 3D Arnold cat map is shown as Eq.1.

$$\begin{bmatrix} F'_x \\ F'_y \\ F'_z \end{bmatrix} = (\begin{bmatrix} 1 & \mathrm{a} & \mathrm{b} \\ \mathrm{c} & \mathrm{ac}+1 & \mathrm{bc} \\ \mathrm{d} & \mathrm{abcd} & \mathrm{bd}+1 \end{bmatrix} \begin{bmatrix} F_x \\ F_y \\ F_z \end{bmatrix}) \bmod(N) \tag{1}$$

Where a, b, c, d and e are positive integers, F_x and F_y is the original pixel positions while F'_x and F'_y is scrambled pixel positions. F_z is a temp parameter and F'_z is scrambled pixel value.

Chaotic Map. The technology of image encryption that based on chaos is a code encryption technology that having developed in recent years. It looks upon the original image as the binary data stream that according to some encoded mode, then encrypts the image by using chaotic signal. The reason that Chaos is fit to image encryption is closely related to some of its dynamics characteristics. The chaotic signal has natural concealment, high sensibility to initial condition and to tiny perturbation motion, all those make the chaotic signal has an ability of long time unforeseeable. The security of this encryption system depends on the degree of approximation between signal and random numbers that produced by secret key stream generator (be chaotic). The secret key stream is getting higher security as it approaching random numbers, whereas it is easily to be broken through. Logistic map is an example among nonlinear equation which can be applied on the experiment mathematic studies triumphantly. Although it is simple, it can embody all the nature of nonlinearity phenomenon. Its function is shown as Eq.2.

$$X_{n+1} = f(\mu, X_n) = \mu X_n (1 - X_n) \tag{2}$$

Where $\mu \in (3.57, 4]$, $X_\text{n} \in (0, 1)$. If μ =4 then the system is in chaotic state, and the sequence that the system produces now has the characteristics of randomness, erotic, and the sensibility sensibility to original value. And the range of it is (0,1). All these characteristics can provide a very good maintenance for the image encrypt operation.

Image Encryption Algorithm based on 3D Arnold Cat

On the basis of 3D Arnold cat map, an improved algorithm is defined as Eq.3.

$$\begin{cases} \begin{bmatrix} F'_x \\ F'_y \\ F_z \end{bmatrix} = (B \times \left\{ \begin{bmatrix} 1 & \text{a} & \text{b} \\ \text{c} & \text{ac}+1 & \text{bc} \\ \text{d} & \text{abcd} & \text{bd}+1 \end{bmatrix} \begin{bmatrix} F_x - 1 \\ F_y - 1 \\ e \end{bmatrix}) \,\text{mod}(\frac{N}{B}) \right\}^K + \begin{bmatrix} K_1 \\ K_2 \\ K_3 \end{bmatrix} \\ F'_z = F_z \oplus \varphi(X_i) \oplus A_i \qquad (\text{i} = [1, \text{n}]) \end{cases} \tag{3}$$

Where a, b, c, d and e are positive integers, F_x and F_y is the original pixel positions while F'_x and F'_y is scrambled pixel positions. F_z is a temp parameter and F'_z is scrambled pixel value. B is the number of blocks in original image. K is the iteration times. (k_1, k_2, k_3) is the positions of original blocks. A_i is the original pixel value and $\varphi(X_i)$ is a function about logistic map.

The details of image encryption are as follows.

(1) Initial value of logistic x_0, product a sequence $\{x_0, x_1, \cdots, x_n\}$.

(2) Enlarge the sequence 1000 times, and then get the part of integer.

(3) Using mod (256) to get the final sequence $\{k_0, k_1, \cdots, k_n\}$ ($k \in [0, 255]$).

(4) Initial value of a, b, c, d, e and K to iterate K times to get position scrambled image.

(5) $\varphi(X_i) = \{k_0, k_1, \cdots, k_n\}$.

(6) Calculate $F_z \oplus \varphi(X_i) \oplus A_i$ to get pixel value scrambled image.

The details of image decryption are as follows.

(1) Initial value of logistic x_0, product a sequence $\{x_0, x_1, \cdots, x_n\}$.

(2) Enlarge the sequence 1000 times, and then get the part of integer.

(3) Using mod (256) to get the final sequence $\{k_0, k_1, \cdots, k_n\}$ ($k \in [0, 255]$).

(4) Calculate the period T of 3D Arnold cat map of N×N.

(5) Initial value of a, b, c, d, e.

(6) Iterate (T-K) times to get original image.

(7) $\varphi(X_i) = \{k_0, k_1, \cdots, k_n\}$.

(8) Calculate $F_z \oplus \varphi(X_i) \oplus A_i$ to get original pixel value image.

Simulation Experiment and Analysis

The original gray image of 256×256 is shown as Fig.1 (a). When the parameters of B=16, K=1, x_0=0.1368, a=2, b=4, c=6, d=5and e=2, the scrambled image is shown as Fig.1 (b). When B=16, K=100, x_0=0.9876, a=2, b=4, c=3, d=23 and e=201 is shown as Fig.1 (c). When K=200, B=32, x_0=0.9456, a=11, b=14, c=23, d=3 and e=101 is shown as Fig.1 (C).
It can get better effect no matter the parameters.

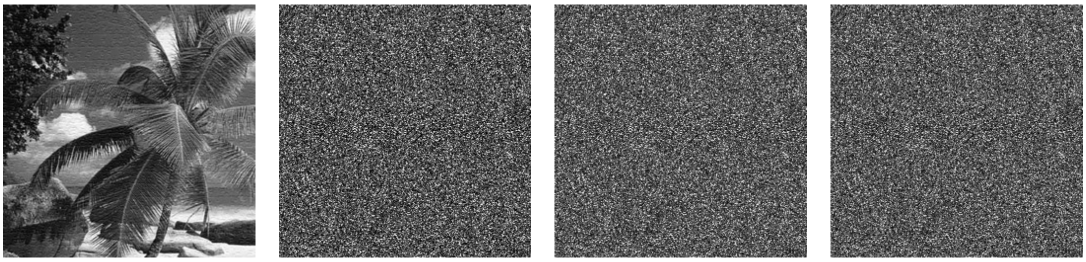

(a) (b) (c) (d)

Fig.1 Original image and scrambled image

Analysis of Security Key's Space. The security key space of the presented 3D Cat Map based image encryption algorithm consists of the type of edge detectors, threshold values, parameters and iteration times of the 3D Cat Map. Each of them has a sufficiently large number of possible variations. Therefore, the key space of the presented encryption algorithm is unlimited. It is impossible for unauthorized users to decode the encrypted image by means of an exhaustive searching for the possible choices in the security key space. As a result, the image is protected by a high level of security. In cryptanalysis, the chosen-plaintext attack is an attack model in which the attacker can choose a number of plaintexts and then get their corresponding cipher texts. In this manner, the attacker can choose any useful information as plaintext in order to deduce the security keys of encryption algorithms, or to reconstruct the original plaintexts from the unknown cipher texts. If the image pixel values are not changed by the encryption process, the chosen-plaintext attack can break the encrypted image without knowing the encryption algorithm or its security keys.

The presented 3D Cat Map based image encryption algorithm changes image pixel values while changing the locations of all image pixels. This ensures that the encrypted image data is not useful in the case of a chosen-plaintext attack. As a result, the presented algorithm is able to withstand chosen-plaintext attacks.

Ability of resisting statistic attack. Studies have indicated that there exists inverse ratio between the stand or fall of an image scrambling effect and the correlative degree of adjacent pixel points, the more correlativity the worse displacement effect ,on the contrary the correlativity is getting less then the scrambling effect is better. Testing the correlativity of horizon (vertical) adjacent pixel points in the scrambling image, the method is as follows:

Take the image pixel with its horizon (vertical) direction next pixel form an adjacent pixel couple, and randomly sampling 100 couples like this, then making use of Eq.4, Eq5 and Eq.6 to calculate the related coefficients of horizon (vertical) adjacent pixel points separately.

$$D(x) = 1/k\sum_{i=1}^{k}[x_i - E(x)]^2 \tag{4}$$

Among the formula: X is the grey value of pixel point; K is the number of pixel point; E(x) is mathematic expectation of x; D(x) is variance of x.

$$\operatorname{cov}(x, y) = 1/k\sum_{i=1}^{k}[x_i - E(x)][y_i - E(y)] \tag{5}$$

Among the formula: X is grey value of the former pixel point; Y is grey value of the latter pixel point; cov (x , y) is the covariance of x, y.

$$r_{xy} = \mathrm{cov}(x, y)/(\sqrt{D(x)}\sqrt{D(y)}) \tag{6}$$

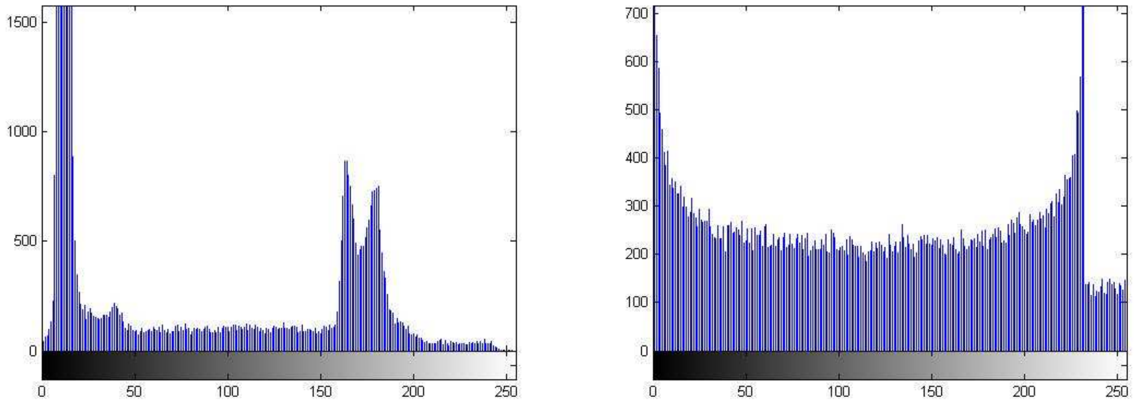
Among the formula: r_{xy} is the related coefficients. Carrying out the experiment analysis on the adjacent pixel points of the primitive image Fig.1 (a) and the encrypted image Fig.1 (b), the final outcome is expressed as Table 1.

Table 1. Correlation comparatively of adjoining pixels

	Vertical related coefficients	Horizon related coefficients
Original image	0.9353	0.9547
Encrypted image	0.0489	0.0821

From the table we can see that comparing the encrypted image with the primitive image along horizontal and vertical direction, its related coefficients are all much smaller, this has achieved the purpose of scrambling, at the same time it has also proved that the scrambling degree of this algorithm is high.

Analysis of Histogram. Carry out analysis through the gray histogram of the image before and after encryption. From the Fig.2 it can be seen that the distribution of primitive image pixel gray values is concentrated on some values, while the pixel gray values after the encryption are scattering in the entire pixel value space. Accordingly it indicates that this encryption method has very good characteristics of gray evenly distribution. Thereby, it can fight against certain degree of statistic analysis attack.



(a) original histogram (b) Encrypted histogram

Fig.2. Gray histogram analysis

Summary

On the basis of 3D Arnold cat map, it presented an algorithm of image encryption which separates the original image to many same blocks and no period. Simulation analysis shows that the encryption algorithm has characters of strong keys, better effect and fast.

References

[1] H.S. Kwok and Wallace K.S. Tang, A fast image encryption system based on chaotic maps with finite precision representation [J]. *Chaos, Solitons & Fractals*(2007), 32(4),pp.1518-1529.

[2] FanYanjun, Sun Xiehua, YanXiaodong, An image displacement encryption algorithm baseson mix chaotic sequence, *Chinese image and graph transaction*(2006), 11(3), pp.387-393.

[3] ZhangHan,Wang Wiufeng,LiZhaohui,LuDahai,An fast image encryption algorithm bases on chaotic system and Henon mapping, *Computer Research and Development* (2005),42(12), pp.2137-2142

[4] Goce Jakimoski, Ljupco Kocarev, Analysis of some rencently propose chaos—baced encryption algorithms. *physics Letter A*(2001),29(6),pp.381-384.

[5] Li TaiYong, JiaHuadiang, WuJiang, An method of digital image encryption bases on three-dimensional chaotic sequence, *Computer application*(2006),26(7),pp.1652-1654.