International Journal of Security and Its Applications
Vol.7, No.5 (2013), pp.377-386
http://dx.doi.org/10.14257/ijsia.2013.7.5.34

A Novel Image Encryption Using Arnold Cat

Pan Tian-gong and Li Da-yong

College of Measurement-Control Tech & Communications Engineering, Harbin University of Science and Technology, Harbin, 150080, China
ptg99@163.com, dyl@hrbust.edu.cn

Abstract

Hyper-chaos has more than one positive Lyapunov exponents and it has more complex dynamical characteristics than chaos. Hence it becomes a better choice for secure image encryption schemes. In this paper, 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. Theoretical and experimental analyses both confirm the security and the validity of the proposed algorithm.

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

1. Introduction

With the rapid development of Internet technology and digital signal processing technology, the secure transmission of image data is becoming a most important problem [1]. Due to some intrinsic features of images, such as bulk data capacity and high redundancy, we must consider image compression except for image encryption [2-4]. On one hand, for the purpose of reducing the image size for easy storage and fast transmission, the study on image compression has been carried out for along time. From research papers, we see that the compression performances are good [5]. However, the current methods are not confidential because they do not have the encryption effect. On the other hand, chaotic systems demonstrate excellent permutation and diffusion properties for effective ciphers. It is thus clear that based on all kinds of visible field, a variety of methods has been put forward. According to the characteristics of digital image information people has put forward a lot of digital image encryption algorithm based on chaotic system encryption technology since it has good effect and speed of encryption got an extensive use of research [6, 7]. In the chaotic encryption technology, one-dimensional Logistic mapping, two-dimensional Smale and Henon mapping and three-dimensional Lorenz of digital image mapping encryption usually were used [8]. In the chaos system, Vinod Patidar has put forward a robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption [9]. David Arroyo has used the characters of chaotic system to comment on image encryption with chaotically coupled chaotic maps [10]. Even though the results of this study realized for image encryption algorithm, but there are still some disadvantages that algorithm thought is complex and operation time is long [11-13].

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

ISSN: 1738-9976 IJSIA

transformation. The experiments show that the feasibility and effectiveness of the algorithm.

2. 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.

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

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 $\mu \in (3.57, 4]$, $X_n \in (0, 1)$. 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.

3. Image Encryption Algorithm based on 3D Arnold Cat

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

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

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. (k1, k2, k3) 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 x0, 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 x0, 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.

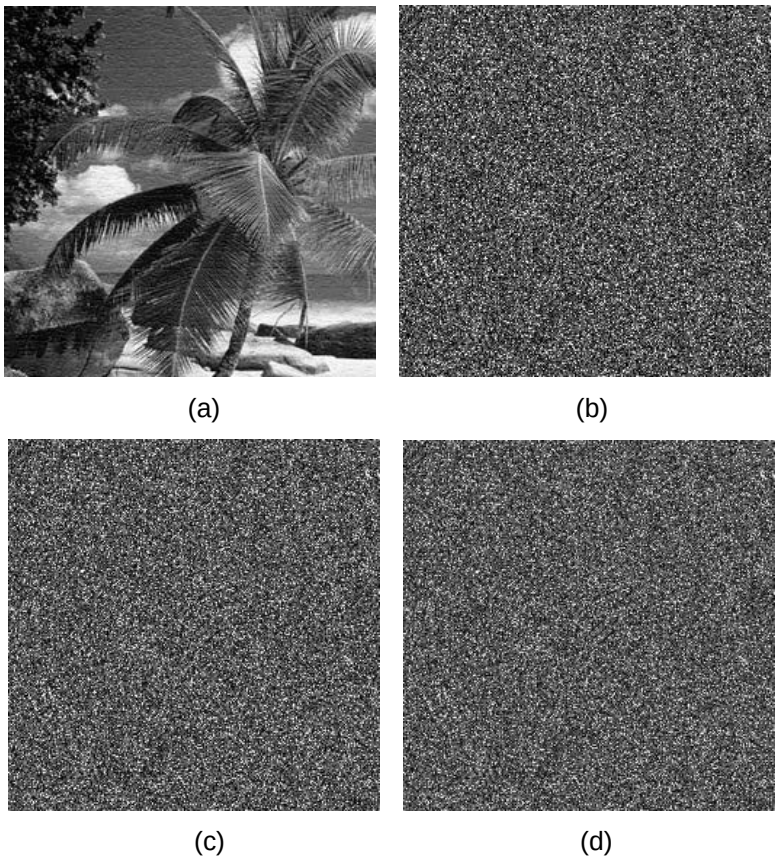
(7) $\varphi(X_i) = \{k_0, k_1, \cdots, k_n\}$.

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

4. Simulation Experiment and Analysis

The original gray im age of 256×256 is shown as Figure 1 (a). When the parameters of B=16, K=1, x0=0.1368, a=2, b=4, c=6, d=5and e=2, the scrambled image is shown as Figure 1 (b). When B=16, K=100, x0=0.9876, a=2, b=4, c=3, d=23 and e=201 is shown as Figure 1 (c). When K=200, B=32, x0=0.9456, a=11, b=14, c=23, d=3 and e=101 is shown as Figure 1 (d).

It can get better effect no matter the parameters.



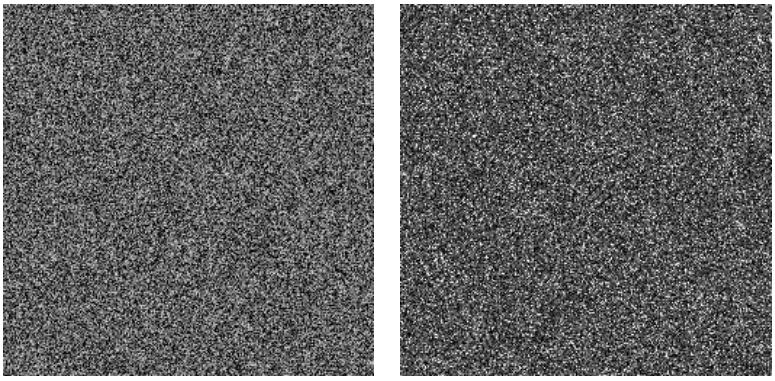
(a) (b)

(c) (d)

Figure 1. Original Image and Scrambled Image

When changing the original image as Figure 2 (a), the parameters of B=16, K=1, x0=0.1368, a=2, b=4, c=6, d=5and e=2, the scrambled image is shown as Figure 2 (b). When B=16, K=100, x0=0.9876, a=2, b=4, c=3, d=23 and e=201 is shown as Figure 2 (c). When K=200, B=32, x0=0.9456, a=11, b=14, c=23, d=3 and e=101 is shown as Figure 2 (d).

(a) (b)



(c) (d)

Figure 2. Original Image and Scrambled Image

4.1. 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.

4.2. 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.

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

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.

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

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

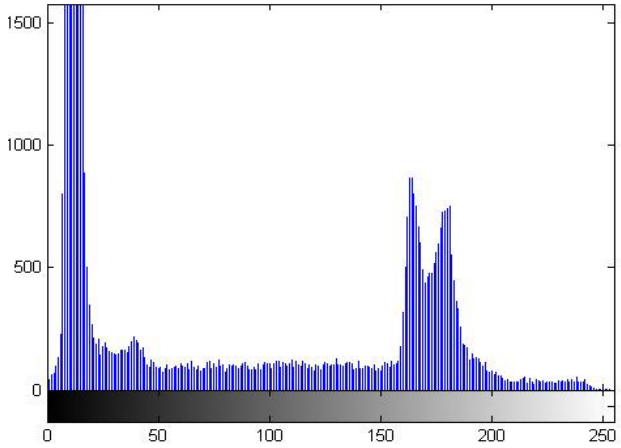
Table 1. Correlation Comparatively of Adjoining Pixels

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

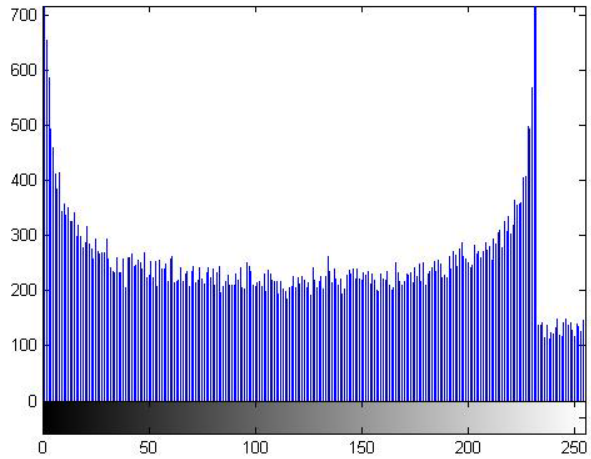
From the table we can see that comparing the encrypted image with the primitive image along horizontal and vertical direction, its related coefficients are all much smaller, this has achieved the purpose of scrambling, at the same time it has also proved that the scrambling degree of this algorithm is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

4.3. Analysis of Histogram

Carry out analysis through the gray histogram of the image before and after encryption. From the Figure 3 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

Figure 3. Gray Histogram Analysis

To quantify the performance of the proposed algorithm, we computed the signal-to-noise ratio (SNR) index for each original image. We computed SNR for the original images in the decrypted images for two experiments, respectively. For comparison, we also computed SNR for the original images in the encrypted images.

We can see that each original image is well masked by the key images in the encrypted images but recovered by BSS with very high SNR. Owing to the characteristic of human perception, the differences of the decrypted images and the original images are hard to identify.

4.4. Noise Analysis

There are many different types of noise existing in public multimedia channels such as internet and wireless communication networks. And the noise belongs to a kind of attack which has no intention. They would lead to the descending of image quality. The common noise is Salt and pepper noise, Gaussian noise, low pass filter attack and so on, and they are different kinds of image noise. The experimental results in Figure 4 show the performance of the algorithm after it has been subjected to many attacks. The bottom row shows the images reconstructed by the method above. Even though being affected by noise, these reconstructed images contain most of the original images' visual information. These experimental results demonstrate that the algorithm demonstrates a good performance against attacks as well. The original images can be completely reconstructed even though they are subject to a noisy environment.

(a)Salt Pepper (b)Gaussian

Figure 4. The Results of Many Attacks

4.5. Speed Analysis

The execution time can demonstrate how efficiently the encryption algorithms encrypt image. This feature is designed to show whether the encryption algorithm can meet the requirements of low computation and high processing speed in real-time applications. Table 2 gives the execution time. The result was measured on a computer running the Windows 7 operating system with 2GB memory and with a CPU using Intel(R) core(TM)2 Duo CPU T6600. The time of encryption process was measured when the Logistic sequence was applied individually to image. The results has shown that there is a familiar relation with the size of images and the running time of this method is short, encryption and decryption time can meet the requirements of the normal operation.

Table 2. Execution Time Statistics

Process execution time(s)	Lenna (256×256)	image(512×512)	RGB (256×256)
Encryption	0.007	0.098	0.122
Decryption	0.012	0.099	0.097

5. Conclusion

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 W. K. S. Tang, "A fast image encryption system based on chaotic maps with finite precision representation", Chaos, Solitons & Fractals, vol. 32, no. 4, **(2007)**, pp. 1518-1529.
[2] F. Yanjun, S. Xiehua and Y. Xiaodong, "An image displacement encryption algorithm baseson mix chaotic sequence", Chinese image and graph transaction, vol. 11, no. 3, **(2006)**, pp. 387-393.
[3] Z. Han, W. Wiufeng, L. Zhaohui and L. Dahai, "An fast image encryption algorithm bases on chaotic system and Henon mapping", Computer Research and Development, vol. 42, no. 12, **(2005)**, pp. 2137-2142.
[4] G. Jakimoski and L. Kocarev, "Analysis of some rencently propose chaos-baced encryption algorithms", Physics Letter A, vol. 29, no. 6, **(2001)**, pp. 381-384.
[5] L. Taiyong, J. Huadiang and W. Jiang, "An method of digital image encryption bases on three-dimensional chaotic sequence", Computer application, vol. 26, no. 7, **(2006)**, pp. 1652-1654.
[6] E. Solak, "Cryptanalysis of a chaos-based image encryption algorithm", Physics Letters A, vol. 373, no. 15, **(2009)**, pp. 1357-1360.
[7] N. Singh, "Gyrator transform-based optical image encryption", Chaos, Optics and Lasers in Engineering, vol. 47, no. 5, **(2009)**, pp. 539-546.
[8] B. Boash Ash, "Time Frequency Signal Analysis and Processing", Elsevier Science Ltd., vol. 5, no. 12, **(2003)**, pp. 743-747.
[9] V. Patidar, "A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption", Optics Communications, vol. 284, no. 19, **(2011)**, pp. 4331-4339.
[10] D. Arroyo, "Comment on Image encryption with chaotically coupled chaotic maps", Physica, vol. 239, no. 12, **(2010)**, pp. 1002-1006.
[11] J. Fredy Barrera, "Experimental opto-digital synthesis of encrypted sub-samples of an image to improve its decoded quality", Optics Communications, vol. 51, no. 11, **(2011)**, pp. 1822-1827.
[12] J. Li, "Double-image encryption on joint transform correlator using two-step-only quadrature phase-shifting digital holography", Optics Communications, vol. 285, no. 16, **(2012)**, pp. 1704-1709.
[13] J. Li, "Image encryption with two-step-only quadrature phase-shifting digital holography", Optik-International Journal for Light and Electron Optics, vol. 123, no. 18, **(2012)**, pp. 1605-1608.