International Journal of Signal Processing, Image Processing and Pattern Recognition
Vol.7, No.3 (2014), pp.1-8
http://dx.doi.org/10.14257/ijsip.2014.7.3.01

Image Encryption using CAT Mapping and Chaos Approach

Weihua Zhu

Department of Computer Science, Xinyu College, Xinyu, Jiangxi, China
Erinshen2010@163.com

Abstract

Image encryption algorithm usually features high iteration and low confidentiality since the key space of low-dimensional discrete chaotic encryption is small. In order to address these challenges when carrying out image encryption, this paper proposes an innovative method which uses Cat mapping to realize the image discretization. The proposed approach uses the periodic changes to achieve the encryption of images. Images with different sizes may use different cycles to encrypt. The experiments show that the encryption approach is able to fulfill the image encryption effectively through drawing the best parameters to achieve the best image encryption effect. The sensitivity analysis implies that, this method is capable of performing well on the image pixel scrambling and replacement. For encrypted security, this proposed method has strong sensitivity to the plaintext which may attribute to handle the plaintext attack under difference situations.

Keywords: *Image Processing, Encryption, Cat Mapping, Chaos, Plaintext, Cycle, Discreteness*

1. Introduction

Security mechanisms define the conditions of the control system behavior and the relationship of the entity (*e.g.*, user, file, network interface, *etc*.,) [1]. These conditions are usually set with a set of rules (or set of constraints) to express these rules set security policy mechanism. Security policy model requires the ability to give the status of the embedded security operating system migration model, the relationship between the needs of security services and access control [2]. System security policy requires flexibility, good to handle multi-strategy integration and dynamic configuration issues, supporting policy description language and configuration tools, support for dynamic upgrade, update and management strategy. One of the most important security mechanisms is image encryption that is common in our daily life.

Most chaotic encryption is simply chaotic system based on low-dimensional discrete chaotic iterative image scrambling [3]. This approach has a simple form, and encryption time is short. It is easy to realize according to its advantages too. But it has the small key space confidentiality with poor performance. Studies have shown that the use of low-dimensional chaotic system encryption confidentiality is not enough [4].

Currently, the common image encryption methods are categorized into two dimensions: replacement of the image pixel values and the scrambled image [5]. Replacement encryption method of the image pixel values is achieved by changing the gradation value of the original image pixel image for the purpose [6]. This method has been widely used for image encryption [7-8]. The scrambled location of image pixel refers to change the position of pixels from original image so that an attacker is difficult to identify the original image so as to achieve the purpose of image encryption [3, 9]. Chaotic system, due to its sensitive

ISSN: 2005-4254 IJSIP

dependence on initial conditions, is very suitable for image encryption. If there are small differences in the initial conditions for a chaotic system, a completely chaotic sequence will be generated. Thus, the chaotic system has better security image encryption characteristic comparing with traditional methods.

The innovative approach proposed in this paper uses a two-dimensional chaotic cat map image pixel scrambling and a new hybrid chaotic system image replacement to overcome the above challenges. The system mixes two discrete chaotic systems together by a certain percentage. After that, it is injected into a continuous chaotic system. Such behaviors are able to get an extremely complex chaotic sequence. Finally chaotic sequence is used for computing image data so as to fulfill the encryption purpose.

The confidential performances from this approach do not depend on the complexity of chaotic sequences and computation algorithm. It depends on the complexity of the chaotic sequence generated by the method. The method and the requirements of modern cryptography is the same so that the confidentiality of the system does not rely on the confidentiality of the encryption, decryption algorithm and system confidentiality. It merely relies on the secrecy of the key. This is the most important feature of the proposed method. Experiments show that this method has several advantages such as large key space, simple-to-use, easy to implement, confidentiality, and convenient decryption.

The rest of this paper is organized as follows. Section 2 introduces the Cat mapping approach briefly, which is a typical chaos system. The discreteness and cyclicity of Cat mapping are highlighted. Section 3 illustrates the experiments and results in terms of histogram analysis, different sensitivity analysis to plaintext, and findings. Section 4 concludes this paper by giving the future work.

2. Cat Mapping Approach

In this proposed encryption algorithm, a two-dimensional chaotic Cat mapping method is used for scrambling the image. There are several reasons to use this mapping approach: (1) the mapping is one-to-one mapping, therefore, there is a one-to-one relationship between the plaintext images and ciphertext image to avoid the coordinate position of conflict; (2) two-dimensional chaotic map has large key space, and the stable structure; (3) using the mapping, the image scrambling is fast; (4) this approach is with simple structure, it can be achieved through matrix operations.

Cat mapping was first discovered by Arnold from Soviet Union, who is a famous mathematician [10]. Since an image of a cat is often used for illustration, as shown in Figure 1, it is named as Cat mapping. An image of Cat is under mapping as follows: the linear stretch is carried out firstly, and then modulo operation is done and folded. The operations will be repeated so on and eventually reach the encryption of the image.

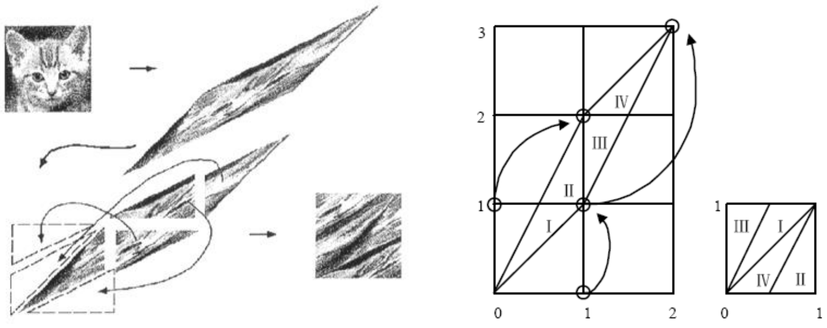


Figure 1. Mechanism of Cat Mapping

Chaos Cat mapping could be expressed as:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = A \begin{pmatrix} x_n \\ y_n \end{pmatrix} (\mathrm{mod}\, 1),\ A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

Since detA＝1, Cat mapping is unique. The Lyapunov index of the Cat mapping is:

$$\lambda_1 = \ln(\frac{3+\sqrt{5}}{2}) > 0\ ,\quad \lambda_2 = \ln(\frac{3-\sqrt{5}}{2}) < 0$$

2.1. Discreteness of Cat Mapping

Using Cat mapping for image encryption, it is necessary to carry out the pre-processing first. The processing procedures are as follows.

First of all, parameters are initialized. The initialization could be carried out through modifying the elements in matrix A. Considering a general Cat mapping as follows:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = A_d \begin{pmatrix} x_n \\ y_n \end{pmatrix} (\mathrm{mod}\, 1),\ A_d = \begin{pmatrix} ab+1 & a \\ b & 1 \end{pmatrix}, a, b \in N$$

The Cat mapping is a unique function, which has the no-minus Lyapunov coefficient. Secondly, the Cat mapping is extended to N×N and then carry out the discretization operation. Thus, the following formula could be obtained:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = A_d \begin{pmatrix} x_n \\ y_n \end{pmatrix} (\mathrm{mod}\, N),\ x_0, y_0 \in \{0, 1, \cdots, N-1\}$$

The extended function is still a one-to-one mapping. It is easy to proof that the parameter a， b have the cycle N. Thus, it could be expressed as:

$$\begin{pmatrix} (a+k_1N)(b+k_2N)+1 & a+k_1N \\ b+k_2N & 1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} (\mathrm{mod}\, N) = \begin{pmatrix} ab+1 & a \\ b & 1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix}$$

Where， k_1, k_2 are non-minus integer and a, b are non-minus integer which less than N.

2.2. Cyclicity of Cat Mapping

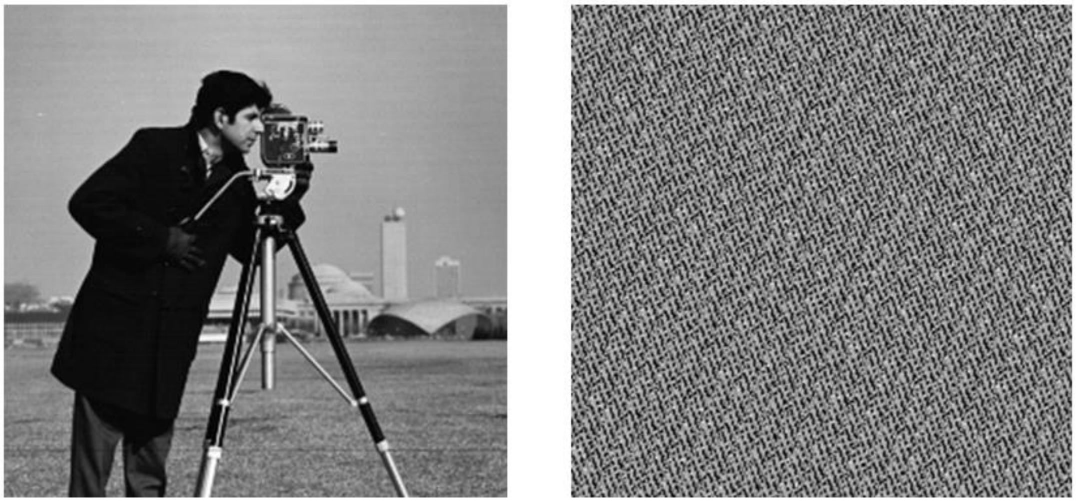
Since an image is a set of limited points, the results of iteration could have cyclicity. For example, in the beginning, the image will be chaos when the positions of different pixels changing. The chaos could last for a certain time when the iteration carries on. However, due to the characteristics of the iteration system, the pixels are able to move back to their original positions. That means, after a certain time, the image could be recovered after a change. This is the cyclicity of Cat mapping. It could be observed that if

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

taking an image with the size of 128×128 for example, the iteration cycle is 96. If the image size is 240×240, the iteration cycle is 60. If the image size is 256×256, the iteration cycle is 192.

3. Experiments and Discussions

The experiments are carried out by using the parameters as follows: a＝40， b＝30. The iteration time is 5. The environments of the experiments are Pentium IV 2 GHz CPU, 2 GB Memory; the operation system is Windows XP Professional SP2. Matlab 2008 is used for the experiments. The experimental results are as shown in the following figures.



(a) Original Image

(a) Encrypted Image

Figure 2. Experimental Results

From the Figure 2, (a) shows the original image with 256×256 pixels. After changing the positions of the pixels, (b) shows the encrypted image. It is observed that the encrypted image from (a) is hardly to figure out the direct information. Figure (b) only changes the position of the figure. The pixel values are the same. The unchanged pixel values could be proofed from the image histogram.

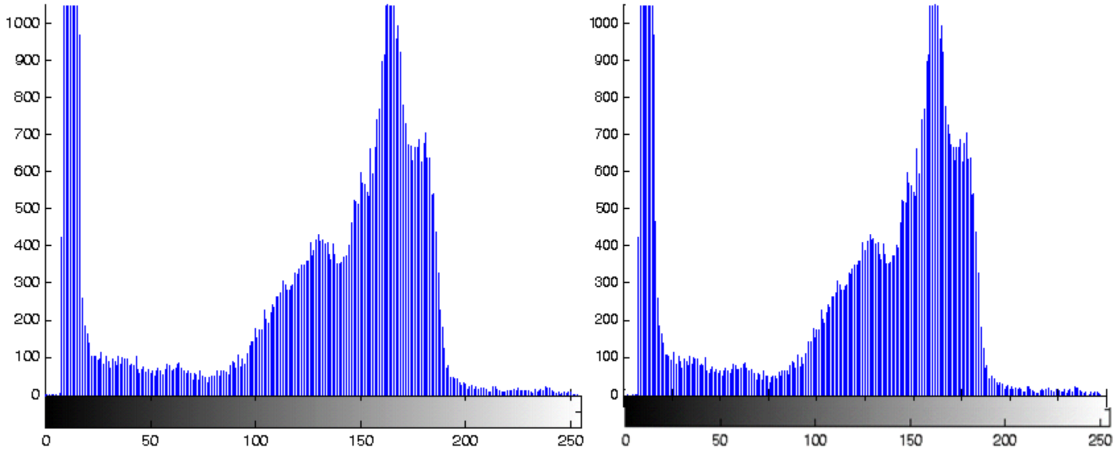
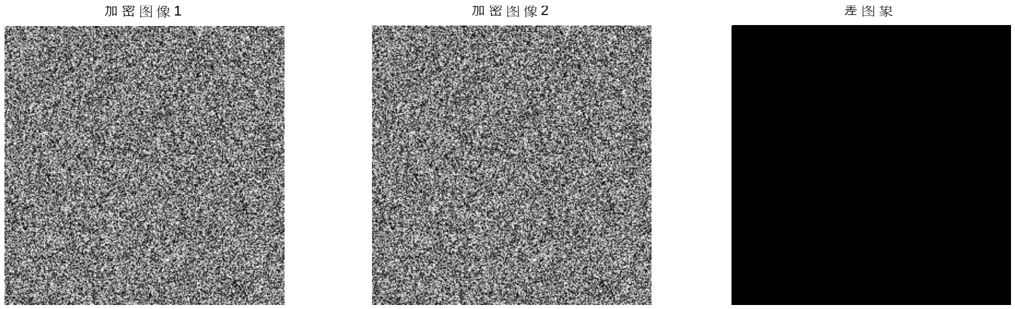


Figure 3. Histogram of the Experiments

The algorithm can be performed well on the image pixel scrambling and replacement from the above figures. For encrypted security, however, a very important aspect - sensitivity to the plaintext cannot be well positioned to meet the plaintext attack. Chosen plaintext attack means that an attacker can use encryption system to encrypt and chosen plaintext through comparative analysis of changes between the plaintext and ciphertext so as to get the encryption key, crack secret text, and so on [11]. For instance, an attacker can choose different plaintexts of two images which is only one pixel contrast. Ciphertext can be found from comparing this pixel location converting repeatedly. The comparisons can find the relationship of all the pixels corresponding to the plaintext and the ciphertext [12]. Although this method is, compared with other attack methods, more difficult to achieve, it is less likely to be happened. However, if the attacker is able to implement this attack, the threat of the encryption system is the largest [13-14]. Given a lot of chaos-based encryption system, many of them cannot resist this attack [15-16], the risk exists in our approach as well.



(a) (b) (c)

Figure 4. Sensitivity to Plaintext-1

Figure 4 shows the sensitivity experiments based on the approaches in this paper. (a) and (b) are the encryption results from two original images which have only different of one pixel value. The fixed point of these two images is close to 1. From (c), a difference image from (a) and (b), it can be seen that the pixel values of the two images is substantially the same. So the above algorithm cannot resist the plaintext attack.

However, if the changes of each pixel value in ciphertext are able to influence all or most of the gray values in the plaintext, the plaintext attack could be avoided. Thus, the following improvements are implemented so as to enhance the ability for resisting plaintext attack in the above algorithm:

The mapping described above uses different mixing ratio of different factors as a key, which will affect the output results. However, the system is very sensitive for these factors. Therefore, if the plaintext changes can affect the factors, the encrypted image will be sensitive to the plaintext. Thus, the most important improvement is the change of the factors. They could be modified as follows: First, all the plaintext pixel values are carried out by bitwise XOR operations. Secondly, the resultant values are done modulo operation and set to [0, 1]. Finally, in accordance with the correspondence relationship, a pixel value changes may greatly influence the encrypted image.

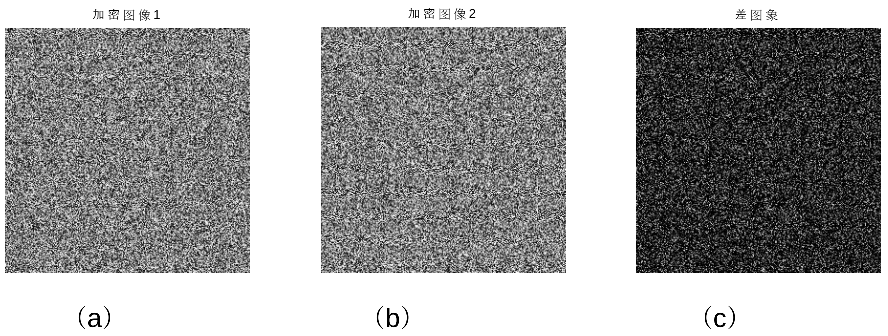


Figure 5. Sensitivity to Plaintext-2

Figure 5 (a) is an encrypted image of Figure 2 (a). If there is an arbitrarily change the pixel values of the diagram, an encrypted image obtained in (b). The fixed point ratio from these two figures is 0.4%. That essentially implies that all most of the pixels are different. (C) shows their difference image. From (c), the figure (a) and (b) is totally different. The improved algorithm for the encryption is very sensitive to the plaintext, even if only a few changes of a pixel can result the ciphertext completely. So the improved algorithm can be very effective against selective plaintext attack.

4. Conclusions

Based on scrambling pixel displacement and diffusion of ideological from Cat mapping, this paper designs a fast and secure image encryption algorithm. Firstly by using Cat mapping, the pixel values from images are scrambled. Secondly, the pixel value is replaced by a new hybrid chaotic system. Thirdly, this paper proposes a new method to enhance the ability of the algorithm to resist select plaintext attack. In this paper, the effect of various tests and detailed analysis are carried out. The experiments results prove that this new image encryption algorithm has good advantages such as real-time feature, high security, and ease of implementation. It is ideal for image encryption under the situations of a large amount of data and real-time requirements.

Future research directions could be carried out from several dimensions. First of all, the Cat mapping could be extended with advanced chaos functions like deterministic chaos, or simply chaos with dynamic behavior initials. Thus, the encryption parameters could be more complex. However, the decryption procedures are much more sophisticated. Secondly, the evaluation of the Cat Mapping and Chaos approach could be carried out via more dimensions. This paper only analyzes the histogram and sensitivity to plaintext. Thus, the availability and practicality of using this approach in real-life case should be examined. Finally, the method proposed in this paper could be used in real applications like Internet for transferring the images which should be confidential like online chatting system. This approach is easy to implement due to the high cost efficient.

References

[1] O. Mirzaei, M. Yaghoobi and H. Irani, "A new image encryption method: parallel sub-image encryption with hyper chaos". Nonlinear Dynamics, vol. 67, no. 1, **(2012)**, pp.557-566.

[2] R. Y. Zhong, Q. Y. Dai, T. Qu, G. J. Hu and G. Q. Huang, "RFID-enabled Real-time Manufacturing Execution System for Mass-customization Production", Robotics and Computer-Integrated Manufacturing, vol. 29, no. 2, **(2013),** pp. 283-292.

[3] D. James and M. Philip, “A Novel Security Architecture for Biometric Templates Using Visual Cryptography and Chaotic Image Encryption Eco-friendly Computing and Communication Systems” **(2012)**. pp. 239-246 Springer.

[4] S. Ravi, A. Raghunathan, P. Kocher and S. Hattangady, “Security in embedded systems: Design challenges”, ACM Transactions on Embedded Computing Systems (TECS), vol. 3, no. 3, **(2004),** pp. 461-491.

[5] Q. Y. Dai, R. Y. Zhong, G. Q. Huang, T. Qu, T. Zhang and T. Y. Luo, “Radio frequency identification-enabled real-time manufacturing execution system: a case study in an automotive part manufacturer”, International Journal of Computer Integrated Manufacturing vol. 25, no. 1, **(2012),** pp.51-65.

[6] T. Kasper, D. Carluccio and C. Paar, “An embedded system for practical security analysis of contactless smartcards. Information Security Theory and Practices”, Smart Cards, Mobile and Ubiquitous Computing Systems, **(2007),** pp.150-160.

[7] R. Y. Zhong, Q. Y. Dai, K. Zhou and X. B. Dai, “Design and Implementation of DMES Based on RFID”, Paper presented at the 2nd International Conference on Anti-counterfeiting, Security and Identification, Guiyang, **(2008)** August 20-23 pp. 475-477.

[8] S. Bhatti, J. Carlson, H. Dai, J. Deng, J. Rose, A. Sheth, R. Han, “MANTIS OS: An embedded multithreaded operating system for wireless micro sensor platforms”, Mobile Networks and Applications, vol. 10, no. 4, **(2005),** pp. 563-579.

[9] R. Y. Zhong, G. Q. Huang, Q. Y. Dai and T. Zhang, “Estimation of Lead Time in the RFID-enabled Real-time Shopfloor Production with a Data Mining Model”, Proceeding of The 19th International Conference on Industrial Engineering and Engineering Management, **(2012)** October 27-29, ChangSha,P.R China.

[10] M. S. Seyedzadeh and S. Mirzakuchaki, “A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map”, Signal processing, vol. 92, no. 5, **(2012),** pp. 1202-1215.

[11] J. Lifton, D. Seetharam, M. Broxton and J. Paradiso, “Pushpin computing system overview: A platform for distributed, embedded, ubiquitous sensor networks”, Pervasive Computing, **(2002),** pp. 605-614.

[12] M. L. Wang, Q. Y. Dai, R. Y. Zhong and G. Q. Huang, “RFID-enabled Real-time Mechanical Workshop Training Center”, International Journal of Engineering Education, vol. 28, no. 5, 1**(2012),** pp. 199-1212.

[13] L. Y. Zhang, C. Li, K.-W. Wong, S. Shu and G. Chen, “Cryptanalyzing a chaos-based image encryption algorithm using alternate structure”, Journal of Systems and Software, vol. 85, no. 9, **(2012),** pp. 2077-2085.

[14] C. Li, L. Y. Zhang, R. Ou, K.-W. Wong and S. Shu, “Breaking a novel colour image encryption algorithm based on chaos”, Nonlinear Dynamics, vol. 70, no. 4, **(2012),** pp. 2383-2388.

[15] I. Hussain, T. Shah, M. A. Gondal and H. Mahmood, “A novel image encryption algorithm based on chaotic maps and GF (28) exponent transformation”, Nonlinear Dynamics, **(2013),** pp. 1-8.

[16] R. Y. Zhong, Z. Li, A. L. Y. Pang, Y. Pan, T. Qu and G. Q. Huang, “RFID-enabled Real-time Advanced Planning and Scheduling Shell for Production Decision-making”, International Journal of Computer Integrated Manufacturing, vol. 26, no. 7, **(2013),** pp. 649-662.

Author

Weihua Zhu, a senior lecture from department of Computer Science got the master degree of communication and information system from Nan Chang University. He has been published a large number of articles in international journals and conferences. His main research areas are algorithm design and embedded system.