Image Encryption of Multiple Keys Method Based on Chaotic Maps

Yan Cheng
College of Software, Shenyang Normal University
Shenyang, China
yu.yan123@163.com

Shu Yang
College of Software, Shenyang Normal University, Shenyang, China
Shuyang024@163.com

Shi-feng Li
School of Electronic and Information Engineering, Dalian University of Technology, Dalian, China
lishifeng2007@gmail.com

Abstract

Abstract— **This paper presents a multiple keys method of image encryption on chaotic maps. Different from other existing methods, two chaotic maps and multiple keys are used to encrypt the image. Firstly, the Arnold map permutes the image as preprocessing using the 1st key, and then the permuted image is divided into non-overlap n*n blocks which are permuted by random sequences whose random seed is created by logistic map whose initial value and parameters are the 3rd keys, and the size of block can be considered as 2nd key. At last the obtained results XOR with the binary result created by logistic map the initial value of which is the 4th keys. The experiments prove that the scheme is robust to the signal processing procedure such as noise, compression and have a super security.**

Keywords—image encryption; logistic map; arnold map; multiple keys

I. INTRODUCTION

With the development of multimedia technology, the research on multimedia encryption, such as image, audio and video, becomes a hot topic. A lot of techniques are employed by researchers, e.g. [1] proposed a new steganography based on genetic algorithm which is robust to RS analysis. Ryouichi Nishimura et al. [2] developed a technique to enhance the security of vocal communication. Hsiang-Cheh Huang et al. [3] introduced a new watermarking using the optimization technique - bacterial foraging. Besides, chaos has been utilized in encryption.

The idea of using chaos for data encryption is certainly not new and can be traced back to the classical Shannon's paper [4]. Probably, the most obvious application of chaotic maps is to use one or more than one dimensional maps as pseudo random number generators to produce a binary stream, then the binary stream is XOR-ed with the plain-text to produce the cipher-text. Some new algorithms are only based on confusion or substitution. They are simple and efficient, while these schemes have been shown that they can only produce weak ciphers. Recently some researchers such as [5], they used two chaotic maps to encrypt the image to enhance the security. Similarly, Ashtiyani *et al.* [6] also employed chaotic maps and other method to encrypt the images. However, these methods can't resist common signal processing. The method presented by [7] has a super security while it is hard to recover when a little error happens hence it is not appropriate for communication. A method which can resist compression was proposed by [8], which performed well under high compression, however, it is not clear whether or not the method can resist other signal attacks. Ahmad [9] introduced a new method using two logistic chaotic maps and a large enough external secret keys for image encryption. This method exhibits a high security, but they did not proof this method is robust or not to common signal processing attacks.

The scheme proposed in this paper is based on two chaotic maps which can overcome the periodicity of Arnold map and is more security; besides, it is robust to the common signal attacks.

The rest of this paper is organized as follows. Section 2 describes the technique of chaotic, and the image encryption algorithm. And the properties of security, computational complexity are analyzed in Section 3. The experimental results are given in Section 4. Finally, in Section 5, some conclusions are drawn.

II. IMAGE ENCRYPTION

The proposed chaotic image encryption method based on multiple secret keys is shown in figure 1.

A. Chaotic Maps

A one-dimensional chaotic map is used to generate 1-D sequences of real numbers:

$$x_{n+1} = f(x_n, \lambda) \tag{1}$$

978-0-7695-4180-8/10 $26.00 © 2010 IEEE
DOI 10.1109/PCSPA.2010.220

Where $n = 1, 2, \cdots$ is the map iteration index and λ is the system parameter. Two chaotic maps are employed in our image encryption. One is the Arnold map which is also called cat mapping [10].

$$\begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_i \\ y_i \end{pmatrix} (\mathrm{mod}\, N) \qquad (2)$$

where $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $a, b, c, d \in Z^+$ is the initial position coordinate, and $|A| = ad - bc = 1$. In order to apply to the image processing, we change (2) into the follow expression:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod} \quad N) \qquad (3)$$

The initial position coordinate A and the N can be considered as the first group keys.

The other chaotic sequence is logistic map [11]:

$$x_{i+1} = \mu x_i (1 - x_i) \qquad (4)$$

where $0 \le \mu \le 4$ is called bifurcation parameter, when $3.5699456\cdots < \mu \le 4$, the logistic map goes into the chaotic state and it will produce a sequence $\{x_i \mid i = 0, 1, 2\cdots\}$ which is non-convergent, and sensitive to the initial value. Therefore we can use the parameter μ and the initial value as the second group keys [12,13].

B. Encryption Method

The image encryption method employs two chaotic maps and multiple keys to encrypt the image; the figure 1 depicts the process of the image encryption.

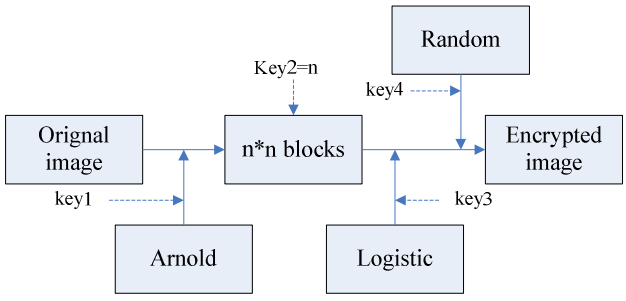

Figure 1. Image encryption

We can depict the encryption process as $I = f(k_1, k_2, k_3, k_4)$, where k_1 is the secret keys of Arnold map, k_2 is the size of the block, k_3 is the third group keys of logistic which includes μ and the initial value producing the random permute seeds, k_4 is another group key of logistic which is used to XOR the every block.

The details of encryption are as follows, here we suppose the image size is $w \times h$, where the width of image is w, and the height is h.

Step 1 the original image is permuted by the Arnold map using the first key.

Step2 the permuted image is divided into non-overlapping $n * n$ blocks and the n is as the second key where $10 \le n \le \min(w, h)/3$ which is obtain by experiments. Let us suppose the number of the blocks is n.

Step3 using the logistic map produces a sequence x_n the length of which is n, where the initial values can be considered as the third key. Then we map the sequence x_n to $X_n \in [1, 255]$ using the following equation (5).

$$X_n = \lfloor 255 \times x_n \rfloor + 1 \qquad (5)$$

Step4 the derived integer sequence X_n is used as a random seed to permute the every block, obtaining new sequence $x_n^{'}$. And then the achieved sequence $x_n^{'}$ XOR with the binary sequence created by logistic map whose initial value is used as the fourth key to obtain the last sequence x_{new}.

Step5 Finally the sequence x_{new} is transformed to form the whole image.

III. QUALITY ANALYSIS

Many experiments have been done by adopting the new algorithm presented in the paper. The new method is sensitive to the initial value, since we use the logistic map to XOR the every block sequence while the logistic map is sensitive to initial value. So if the secret key has a little different from the original secret one, it is difficult for us to decipher the encrypted image. Furthermore, if we want to enhance the security, we can XOR with the sequence twice with two different keys, which can completely destroy the self-similarity and correlation.

In our method, the third step is to permute the every block using initial keys. The keys are produced not by a fixed seed but irregular seed, and the seed is sensitive to the initial value. Therefore the keys are greatly expanded, and the key space is large enough to resist to the brute-force process attacks.

The purpose of the second step in our algorithm is to handle the failure of encryption caused by the self-similarity and correlation. In addition, in order to destroy the correlation of the image and enhance the security further, when the step 4 is finished, we can permute the blocks using another key by Arnold map.

IV. ENCRYPTION RESULTS

In order to test our algorithm, including the super security and the ability of resisting kinds of attacks, a lot of experiments are evaluated by us, which is discussed in the following.

A. Encryption Experiments

Firstly, we use the gray image Lena (size is 256*256) and the binary image (size is 128*128), the key of encryption is (40, 16, (0.87123, 0.5), (0.87123, 0.49)).

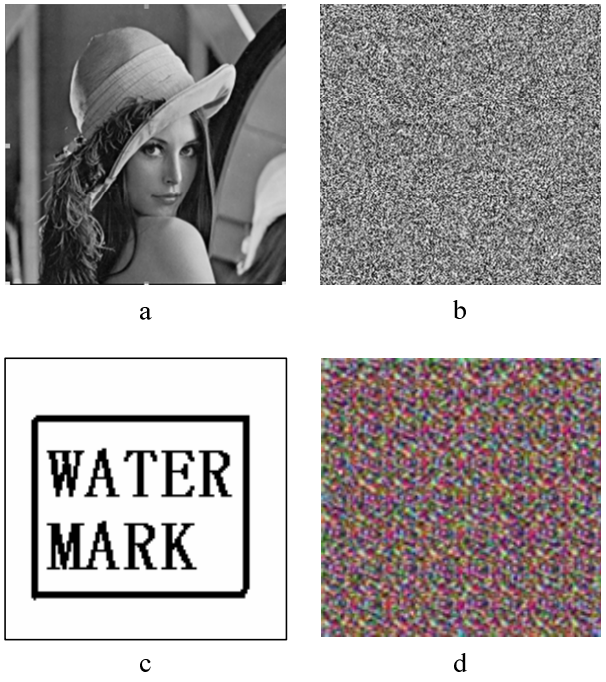

Figure 2. Encryption (a) Original gray Image (b) Encrypted gray image (c) Original binary Image (d) Encrypted binary image

As we observed in figure 2, in order to test our algorithm, gray image and binary image are employed. (b) is the encrypted image from the gray image, whose pixels are permuted irregularly. And (d) is the encrypted result of binary image, it is clear that from (b) we can obtain nothing.

B. Attacks Experiments

The encrypted images can be decrypted correctly although they have been directly attacked by several signal processing. Here we use the same image Lena to test the attacks. The secret is the same as in the section 4.1. As illustrated in figure 3, (a) is the decrypted image under cropping of 1/4, (b) is the decrypted image under JPEG compression by 50%, (c) is the recovered image under 5*5 Gaussian attacking, and (d) is the recovered image from resizing. Experiments show that our method can be resist to the common signal processing and it is appropriate for communication.

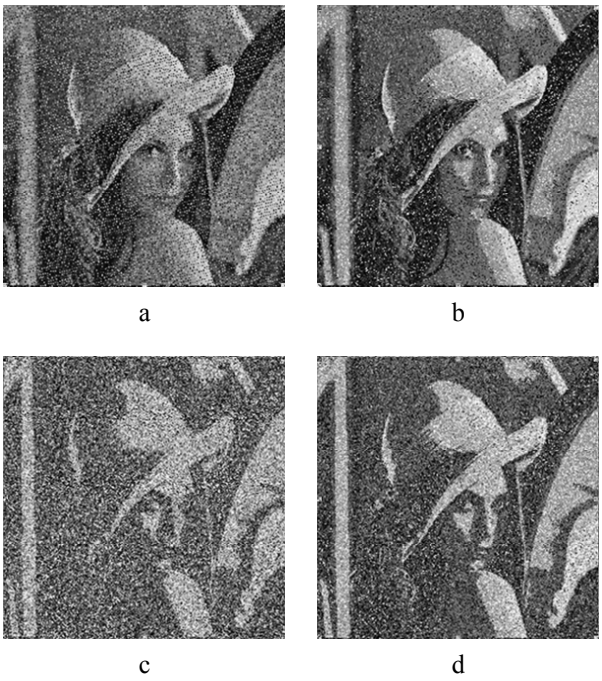

Figure 3. Experiments of attacking (a) Decrypted Images under cropping 1/4 (b) Decrypted Images under JPEG 50% compression (c) Decrypted Images under 5*5 Gaussian filtering (d) Decrypted Images under resizing

C. Security Experiments

Our scheme is more security than only using one chaotic sequence, which has been demonstrated by many literatures [5, 6]. It is obvious that our method has a large secret key space due to the multiple keys strategy. Therefore, it is difficult to decipher the secret keys by brute-force process attacks. Furthermore our method is sensitive to the initial key values. In order to evaluate the sensitivity of the initial key value, here we also use the image of figure 2 (a) for the experiment. The secret keys are the same as section 4.1 simply. We use the secret (40, 16, (0.87123, 0.5), (0.87123, 0.49999)) to decipher the encrypted image. Figure 4 shows the result of the experiment.

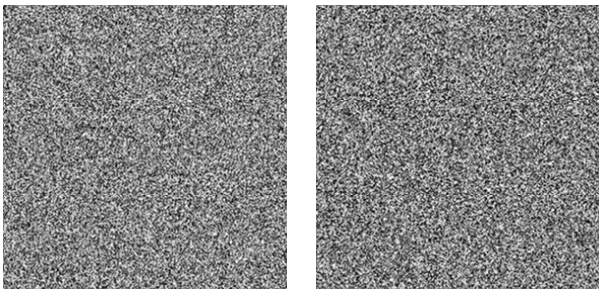

Figure 4. Security experiment (a) Encryption with the secret (40, 16, (0.87123, 0.5), (0.87123, 0.49999)) (b) Decipher with the secret (40, 16, (0.87123, 0.5), (0.87123, 0.49999))

V. CONCLUSION

In this paper, we propose a new method of image encryption which is based on Arnold and Logistic maps. On one hand, we permute the pixels using Arnold map, on the other hand, we also permute the blocks by random numbers whose seeds are provided by the logistic map. Both schemes make our scheme more security. For the block size n , from the experiments, we see that if you select the n more bigger, which can speed up the compute， but at the same time it will reduce the security of the encryption and if n is selected smaller, it will cost more computation time. Experiments suggest it is better to select the size n as the value mentioned in section 2.2. Furthermore, our method employs four group keys, some of which is sensitive to the initial value, which makes our scheme more security. What is more, our method has the ability to resist the common signal attacks, making it is more appropriate for communication.

References

[1] S. Wang, B. Yang and X. M. Niu, "A Secure Steganography Method Based on Genetic Algorithm," Journal of Information Hiding and Multimedia Signal Processing, vol. 1(1), 2010, pp. 28-35.

[2] R. Nishimura, S. I. Abe, N. Fujita and Y. Suzuki, "Reinforecement of VoIP Security with Multipath Routing and Secret Sharing Scheme," Journal of Information Hiding and Multimedia Signal Processing, vol. 1(3), 2010, pp. 204-219.

[3] H. C. Huang, Y. H. Chen and A. Abraham. "Optimized Watermarking Using Swarm-Based Bacterial Foraging," Journal of Information Hiding and Multimedia Signal Processing, vol. 1(1), 2010, pp. 51-58.

[4] C. Shannon, "Communication Theory of Secrecy Systems," Bell System Technical, New York, vol. 28(4), 1948, pp. 656-715.

[5] C. M. Li and L. X. Hong, "A New Image Encryption Scheme based on Hyperchaotic Sequences," Anti-counterfeiting, Security, Identification, 2007 IEEE International Workshop, Xiamen, Fujian, April 2007, pp. 237-240, doi:10.1109/IWASID.2007.373734.

[6] M. Ashtiyani, P. M. Birgani and H. M. Hosseini, "Chaos-Based Medical Image Encryption Using Symmetric Cryptography," Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference, Damascus, April 2008, pp. 1-5. doi:10.1109/ICTTA.2008.4530291.

[7] Y. D. Zhang, F. Zuo and Z. J. Zhai, "A New Image Encryption Algorithm Based on Multiple Chaos System," Electronic Commerce and Security, 2008 International Symposium, Guang Zhou, Aug 2008, pp. 347-350,doi:10.1109/ISECS.2008.142.

[8] S. Lian, J. Sun, and Z. Wang, "A Novel Image Encryption Scheme Based-on JPEG Encoding," in *Proceedings of the 8th* International Conference on Information Visualization, London, vol. 8, July 2004, pp. 217–220.

[9] M. Ahmad, C. Gupta and A. Varshney, "Digital Image Encryption Based on Chaotic Map for Secure Transmission," Multimedia Signal Processing and Communication Technologies, 2009. IMPACT '09. International, Aligarh, March 2009, pp.292-295, doi:10.1109/MSPCT.2009.5164233.

[10] Q. D. Xu, "Fractal and Its Application," Science Press, Beijing, 1994. pp. 143-145.

[11] T. Kohda and A. Tsuneda, "Statistics of Chaotic Binary Sequences," IEEE Trans Information Theory, Kyushu, vol.43(1), Jan 1997, pp. 104-112, doi:10.1109/18.567654.

[12] J. C. Zou, C. Z. Xiong, D. X. Qi and R. W. Ward, "the Application of Chaotic Maps in Image Encryption," IEEE-NEWCAS Conference, Guangzhou, June 2005, pp. 331- 334, doi:10.1109/NEWCAS.2005.1496703.

[13] M. Asim and V. Jeoti, "on Image Encryption: Comparison between AES and A Novel Chaotic Encryption Scheme," Signal Processing, Communications and Networking, ICSCN'07. International Conference, 2007, pp. 65-69.