An Improved Chaos-Based Image Encryption Scheme

Chong Fu[1], Zhen-chuan Zhang[1], Ying Chen[2], and Xing-wei Wang[1]

[1] School of Information Science and Engineering, Northeastern University, Shenyang 110004, China
[2] School of Economy Management, Shenyang Institute of Chemical Technology, Shenyang 110142, China
fu_chong@sohu.com

Abstract. Chaos theory provides a new approach to image encryption technology. The key stream generator is the key design issue of an image encryption system, it directly determines the security and efficiency of the system. This paper proposes an improved chaos-based key stream generator to enlarge the key space, extend the period and improve the linear complexity of the key stream under precision restricted condition so as to enhance the security of a chaos-based image encryption system. The generator is constructed by three Logistic maps and a nonlinear transform. The balance and correlation properties of the generated sequence are analyzed. The sequence is proved to be a binary Bernoulli stochastic sequence and the distribution of the differences between the amounts of 0 and 1 is analyzed. The side lobes of auto and cross correlation are proved to obey normal distribution $N(0, 1/N)$. The experimental results indicate that the scheme has advantages of long period and strong anti various attack ability over conventional chaos-based encryption system.

1 Introduction

Image is one of the most important information representation styles and above 80% information we obtained is from vision apperceiving. With the fast development of computer network technology, more and more sensitive images such as in medical, military, financial etc. fields need effective protection in open network environment and image encryption technology has become an important branch of cryptography. Conventional symmetric encryption algorithm such as DES, IDEA, AES, etc. is not suitable for image encryption due to the special storage characteristics of an image. Most of the classic image encryption algorithms are position permutation based, such as Arnold transform, magic square transform, IFS transform and scan pattern, etc. These methods have advantages of fast encryption speeds but the security completely depends on the secrecy of the algorithm that we use, which do not satisfy the requirement of a modern cryptography system [1-2]. Besides, the encrypted images are only position permutated and the grayscale of each pixel still remains its original value, which is insecure against known plaintext attack.

A chaos system has the properties of extreme initial value sensitive, nonperiodic, unpredictable and Gaussian like correlation properties, while it is deterministic, so it is very suitable to be used as key stream generator for image encryption system [3-5]. The basic idea of chaotic image encryption algorithm is producing two chaos-based

Y. Shi et al. (Eds.): ICCS 2007, Part I, LNCS 4487, pp. 575 – 582, 2007.

pseudorandom sequences, one is for position permutation and the other is for gray-scale substitution. The security of a chaos based image encryption system depends on the unpredictability of the key stream generated by the chaos system [6-9].

Unfortunately, the concrete implementation of single chaos map based encryption system is by far ideal as the abstract model with infinite and not even countable cardinality. The iteration of a chaos map will work with a finite set of rational numbers because no processor is precision unrestricted, which makes the key space limited. The maximum calculation precision of common PC processor is 16, so the key space is $10^{16} \approx 2^{53}$, which is a little smaller than DES(2^{56}) and by far smaller than AES(2^{128}). At the same time, the raw chaotic sequence will be periodic due to limited calculation precision, which will cause the quantified sequence also being periodic and making the correlation properties worse. Besides, single chaos map based key stream is easy to be attacked by using adaptive parameter chaos synchronization method [10-11]. In this paper, an improved key stream generator based on nonlinear transform of three basic Logistic maps is proposed which enlarges the key space to 2^{158}, extends the period and improves the linear complexity of the key stream under precision restricted condition, thus enhances the security of a chaos-based image encryption system.

2 The Statistical Properties of Logistic Map

Logistic map is defined as:

$$x_{i+1} = \mu x_i (1 - x_i), \tag{1}$$

μ is usually set to 4 for full map, in which $x_n \in [0, 1]$. The probability density of chaotic orbit generated by Eq.1 is [12]

$$\rho(x) = \begin{cases} \dfrac{1}{\pi\sqrt{x(1-x)}} & 0 \le x \le 1, \\ 0 & otherwise. \end{cases} \tag{2}$$

Let $\{x_i\}$ be chaotic sequence generated by Eq.1, we can get the following three properties based on Eq.2.

Property 1. The mean of $\{x_i\}$ is:

$$\bar{x} = \lim_{N\to\infty} \frac{1}{N} \sum_{i=0}^{N-1} x_i = \int_0^1 x\rho(x)dx = 0.5. \tag{3}$$

Property 2. The normalized auto correlation function of $\{x_i\}$ is:

$$AC(m) = \lim_{N\to\infty} \frac{1}{N} \sum_{i=0}^{N-1} (x_i - \bar{x})(x_{i+m} - \bar{x}) = \int_0^1 x f^m(x)\rho(x)dx - \bar{x}^2 = \begin{cases} 0.125 & m = 0, \\ 0 & m \ne 0. \end{cases} \tag{4}$$

Property 3. For any two different initial values $\{x_{i1}\}$ and $\{x_{i2}\}$, the normalized cross correlation function of the two generated sequences is:

$$\begin{aligned} CC_{12}(m) &= \lim_{N\to\infty} \frac{1}{N} \sum_{i=0}^{N-1} (x_{i1} - \bar{x})(x_{(i+m)2} - \bar{x}) \\ &= \int_0^1 \int_0^1 x_1 f^m(x_2)\rho(x_1)\rho(x_2)dx_1dx_2 - \bar{x}^2 = 0. \end{aligned} \tag{5}$$

Property 2 and 3 indicate that Logistic map is excellent to be used as key generator for image encryption system. However, above 3 properties are under ideal conditions and the sequence length is usually finite in practical use. Let $\{x_i\}$, $\{x_{i1}\}$ and $\{x_{i2}\}$ be chaotic sequences with finite length N.

The normalized auto correlation function of $\{x_i\}$ is defined as:

$$AC(m)=\begin{cases}\dfrac{1}{N-|m|}\displaystyle\sum_{i=0}^{N-1-|m|}(x_i-\bar{x})(x_{i+m}-\bar{x}) & 1-N\le m\le N-1,\\ 0 & N\le|m|.\end{cases} \tag{6}$$

The normalized cross correlation function of $\{x_{i1}\}$ and $\{x_{i2}\}$ is defined as:

$$CC_{12}(m)=\begin{cases}\dfrac{1}{N-|m|}\displaystyle\sum_{i=0}^{N-1-m}(x_{i1}-\bar{x})(x_{(i+m)2}-\bar{x}) & 1-N\le m\le N-1,\\ 0 & N\le|m|.\end{cases} \tag{7}$$

3 Key Stream Generator Construction and Its Performance Analysis

3.1 Key Stream Generator Construction

The nonlinear transform based key stream generator is shown in Fig. 1.

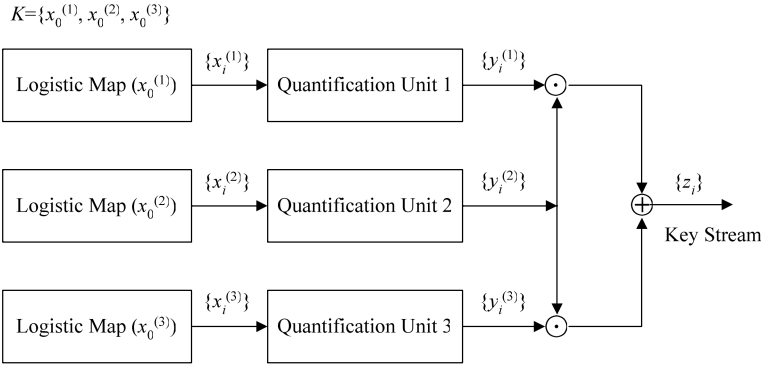


Fig. 1. Nonlinear transform based key stream generator

Three Logistic map with different initial values $x_0^{(1)}$, $x_0^{(2)}$ and $x_0^{(3)}$ produce three independent pseudorandom analog sequences, and three quantification units quantify each input analog sequence $\{x_i^{(k)}\}(k = 1,2,3)$ to binary form $\{y_i^{(k)}\}(k = 1,2,3)$ by using Eq.8.

$$y_i=\begin{cases}0 & x_i<0.5\\ 1 & x_i\ge 0.5\end{cases} \tag{8}$$

Quantification unit2 is used as control unit, when unit2 output 1, the unit2 is connected to unit1; otherwise it is connected to unit3, so the output key stream $\{z_i\}$ is

$$z_i = y_i^{(1)} y_i^{(2)} + y_i^{(3)} \overline{y_i^{(2)}} = y_i^{(1)} y_i^{(2)} + y_i^{(3)} y_i^{(2)} + y_i^{(3)}. \tag{9}$$

The key is constructed by three decimal numbers $k = \{x_0^{(1)}, x_0^{(2)}, x_0^{(3)}\}$, so the key space size is $10^{48} \approx 2^{158}$, which is larger than the acknowledged most security AES standard. Let the period of chaotic binary sequences $\{y_i^{(k)}\}(k = 1,2,3)$ under precision restricted condition be N, from the Eq.9 we can see that the period of $\{z_i\}$ is $2N^2+N$. The period of the output sequence is greatly extended and the linear complexity is improved, so the algorithm is more secure against various attacks such as adaptive parameter chaos synchronization and reverse iteration reconstruction. The balance and correlation properties are the two most important factors to evaluate the performance of a key stream, which will be analyzed in the following sections.

3.2 Balance Performance Analysis

In order to analyze the balance and correlation performance of generated key stream, lemma 1 is proposed.

Lemma 1. The generated key stream $\{z_i\}$ is a binary Bernoulli distributed pseudorandom sequence. For sequence with length N, the distribution of the differences between the amounts of 0 and 1 is shown in Table 1.

Table 1. The distribution of the differences between the amounts of 0 and 1

Differences	N	$N-2$	$N-4$	…	$-N+4$	$-N+2$	$-N$
Probability	$(\frac{1}{2})^N$	$C_N^1(\frac{1}{2})^N$	$C_N^2(\frac{1}{2})^N$	…	$C_N^{N-2}(\frac{1}{2})^N$	$C_N^{N-1}(\frac{1}{2})^N$	$(\frac{1}{2})^N$

The simulation result is shown in Fig. 2. 1000 sequences with length N=8192 are generated and the initial values are selected independently. The mean of differences is -0.9480 and the standard variance is 91.8419, while the theoretical values are 0 and 90.5097, which indicate that the binary chaotic key stream have excellent balance performance.

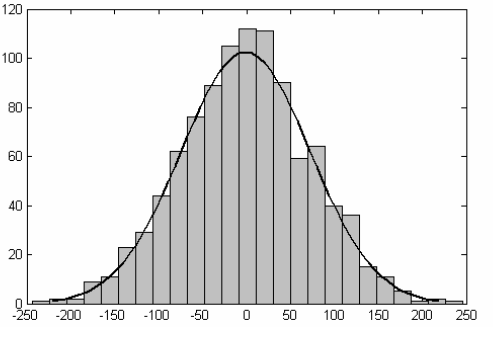


Fig. 2. Distribution of the differences between amounts of 0 and 1

3.3 Correlativity Performance Analysis

Lemma 2. For any two different key stream $\{z_{k1}\}$ and $\{z_{k2}\}$, they satisfy: When N is large enough and m is relatively small, the side lobes of auto correlation and the values of cross correlation of $\{z_{k1}\}$ and $\{z_{k2}\}$ obey normal distribution $N(0, 1/N)$.

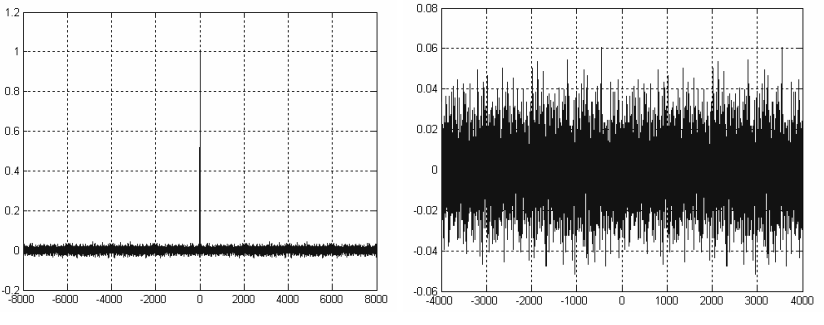
The simulation results of the auto/cross correlation functions and the distribution of auto/cross correlation side lobes are shown in Fig. 3 and 4. The sequence length is 8192 and the initial values are selected as 0.60000 and 0.60001 to identify its initial parameter sensitive property.

3.4 Security Performance Comparison

Security performance comparison of different image encryption schemes is shown in Table 2. Attack (I) represents the neural network based adaptive parameter synchronous attack. Attack (II) represents the reverse iteration based chaotic system reconstruction attack. Attack (III) represents the known plaintext attack.

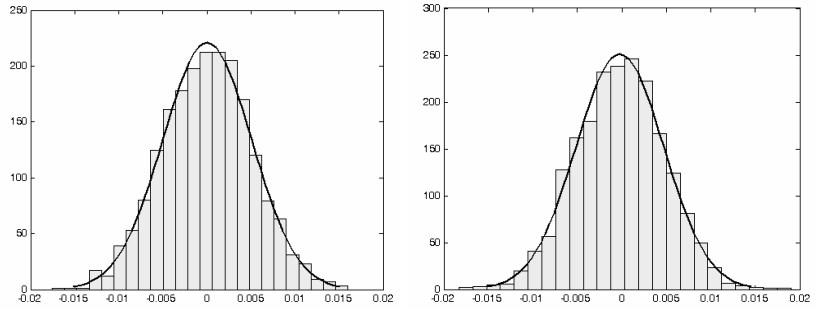
Table 2. Security comparision of different image encryption schemes

Schemes	DES	AES	Pure position permutation	Single chaos based	This paper Proposed
Type	block cipher	block cipher	—	stream cipher	stream cipher
Suitable for image	N	N	Y	Y	Y
Key space	2^{64}	2^{128}	—	2^{53}	2^{158}
Period	—	—	—	M	$2M^2 + M$
Anti attack(I)	—	—	—	N	Y
Anti attack(II)	—	—	—	N	Y
Anti attack(III)	Y	Y	N	Y	Y



(a) (b)

Fig. 3. (a) The auto correlation function, (b) The cross correlation function



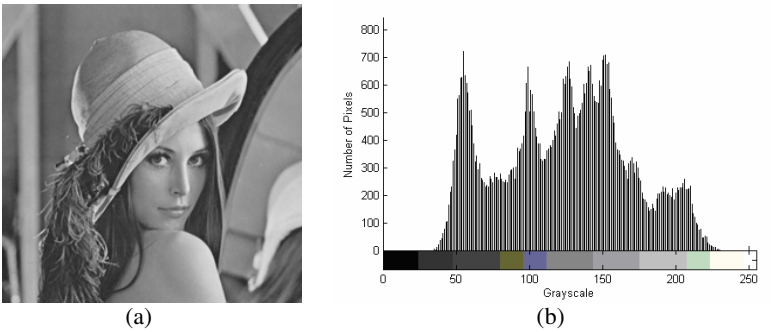
(a) (b)

Fig. 4. (a) Distribution of auto correlation side lobes, (b) Distribution of cross correlation

From Table 2 we can see, compared with the single chaos map based ones, the nonlinear transform based key stream generator proposed in this paper greatly enlarges the key space and extends the period of the key stream under precision restricted condition, which make the complete key search impossible and improves the correlation performance of the key stream. The nonlinear transform of three logistic maps also enhances the complexity of the key stream, which makes it more secure against neural network based adaptive parameter synchronous attack and reverse iteration based chaotic system reconstruction attack.

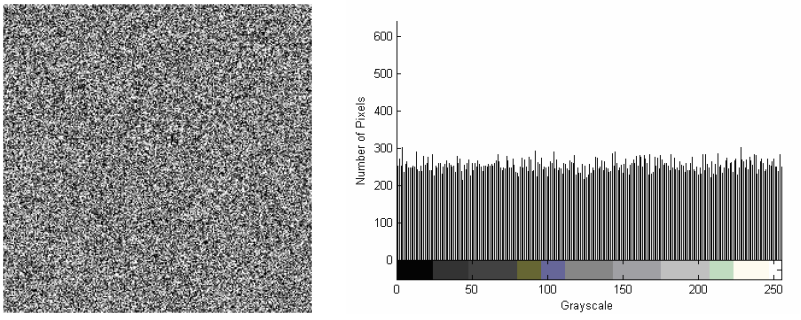
4 Experimental Results

We take 256×256 size 8 bits Lenna image as example, the two pseudorandom key streams used for position permutation and grayscale substitution are generated by scheme proposed in Section 3.1. Original image and its histogram are shown in Fig.5, and the encrypted image and its histogram is shown in Fig. 6. The initial parameters (key pair) are selected as $k = \{0.6, 0.7, 0.8\}$, note k must be far more complex in practical use. From Fig.6 we can see, the grayscale distribution of the encrypted image has good balance property, which is secure against known plaintext attack.



(a) (b)

Fig. 5. (a) Original image, (b) Grayscale histogram of original image



(a) (b)

Fig. 6. (a) Encrypted image, (b) Grayscale histogram of encrypted image

Fig. 7(a) is correct decrypted image and Fig. 7(b) is incorrect decrypted image with key k' = {0.60001, 0.7, 0.8}, from which we can see that the original image can not be restored even if with a minus difference due to the extreme initial parameter sensitive property of a chaos system.

(a) Correct decrypted image (b) Incorrect decrypted image

Fig. 7. Images decrypted with different keys

5 Conclusion

The improved chaos-based key stream generator for image encryption system proposed in this paper greatly extends the key space and improves the linear complexity of the key stream under precision restricted condition over conventional single chaos based schemes. The generator has strong anti attack ability to the commonly used chaos system attack methods such as adaptive parameter chaos synchronization and reverse iteration reconstruction, which enhances the security of a chaos-based encryption system. The nonlinear part of the generator is general and other one dimension chaotic maps such as Chebyshev, Tent, etc. can also be used as analog pseudorandom sequence source.

References

1. Alexopoulos, C. N., Bourbakis G., Ioannou N.: Image Encryption Method Using a Class of Fractals. Journal of Electronic Imaging, Vol. 4 (1995), 251–259
2. Maniccam S. S., Bourbakis N. G.: Image and Video encryption using SCAN patterns. Pattern Recognition, Vol. 37 (2004), 725–737
3. Baptista M. S.: Cryptography with Chaos. Physics Letters A, Vol. 240 (1998), 50–54
4. Alvarez E., Fernandez A.: New Approach to Chaotic Encryption. Physics Letters A, Vol. 263 (1999), 373–375
5. Masuda, N., Aihara, K.: CryptoSystems with Discretized Chaotic Maps. IEEE Transactions on Circuits and Systems, Vol. 49 (2002), 28–40
6. Fu C., Wang P. R., MA X.M.: A Fast Pseudo Stochastic Sequence Quantification Algorithm Based on Chebyshev Map and Its Application in Data Encryption. Lecture Notes in Computer Science, Vol. 3991 (2006), 826–829
7. Fridrich J.: Image Encryption Based on Chaotic Maps. IEEE International Conference on Systems, Man, and Cybernetics (1997), 1105–1110
8. Guan Z. H., Huang F. J., Guan W. J.: Chaos-based Image Encryption Algorithm. Physics Letters A, Vol. 346 (2005), 153–157
9. Zhang L. H., Liao X. F., Wang X. B.: An Image Encryption Approach Based on Chaotic Maps. Chaos, Solitons and Fractals, Vol. 24 (2005), 759–765
10. Chen G., Mao Y.: A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps. Chaos, Solitons and Fractals, Vol. 21 (2004), 749–761
11. Jakimoski G., Kocarev L.: Analysis of Some Recently Proposed Chaos-based Encryption Algorithms. Physics Letters A, Vol. 291 (2001), 381–384
12. Li S. J., Mou X. Q., Cai Y. L.: On the Security of a Chaotic Encryption Scheme: Problems with Computerized Chaos in Finite Computing Precision Computer. Physics Communications, Vol. 153 (2003), 52–58
13. Lian S. H., Sun J. S., Wang Z. Q.: Security Analysis of a Chaos-based Image Encryption Algorithm. Physica A, Vol. 351 (2005), 645–661
14. Kohda T., Tsuneda A.: Statistics of Chaotic Binary Sequences. IEEE Transactions on Information Theory, Vol. 43 (1997), 104–112