A Composite Image Encryption Scheme Using AES and Chaotic Series

Xiao Huijuan
South China U. of Technology
Dongguan U. of Technology
xiaohj126com@126.com

Qiu Shuisheng
South China U. of Technology
eessqiu@scut.edu.cn

Deng Chengliang
Dongguan U. of Technology
dengcl@dgut.edu.cn

Abstract

This paper presents a composite scheme for image encryption. In the temporal domain, chaotic series acts as a key for the AES (Advanced Encryption Standards) encryption. It is used to generate and administer AES key while preserving its other nice features. In the spatial domain, we present a new method of deriving a space transform matrix with chaotic series. In both domains, the chaos series is generated by the logistic equation, whose parameter is modulated by another logistic equation with a different initial value. Therefore, short period effect is avoided in the solution sequence of the chaotic system. Finally our experimental results confirm the effectiveness of the proposed method. Also, there is no damage caused to the decrypted image.

1. Introduction

To fulfill security and privacy needs, encryption of images is an effective technique to frustrate malicious attacks from unauthorized parties.

Chaotic signals possess many desirable features, such as pseudo-randomness, ergodicity and sensitivity to the initial value. All these features enable chaos-based encryption to achieve better confusion and diffusion. Chaotic maps, nonlinear equations, equation parameters and the initial value can all play the role of encryption key.Because chaos signals are very sensitive to parameters and the initial value, in principle, using them as encryption key would produce a huge key space. Besides, pseudo-randomness, ergodicity and wideband property make it difficult for attackers to find patterns of encrypted data in temporal domain or frequency domain.

On the other hand, chaotic encryption has a few weaknesses[1-3]. First, chaotic signals exhibit the periodic or non-periodic recurrence effect. In general it is hard to theoretically determine the period, which is usually measured through experiments. Hence the security of chaotic encryption may be compromised. Second, in practice chaotic sequences generated by chaotic map are iterated with finite precision. Therefore, the real chaotic sequences may differ a lot from theoretical ones, due to the sensitivity to the initial value. Finally, in the cryptosystem of piecewise linear map, neighboring states may be projected on to the same line segment. In this case, the key can be recovered if a little plaintext-ciphertext block is known.

2. Related work

Conventional cryptography, such as RSA(Rivest-Shamir-Adleman), DES(Data Encryption Standard) and AES(Advanced Encryption Standards), are rather mature[4]. Their key spaces are definite and their security performances are easy to evaluate. Hence conventional cryptography is more popular than chaos-based cryptography [5]. Intuitively, combining chaotic encryption with convention encryption would strengthen the security of the cryptosystems.

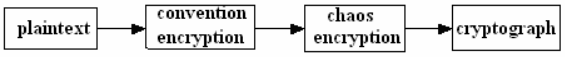


Figure 1. Chaotic encryption in series with conventional encryption

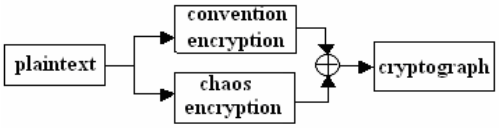


Figure 2. Chaotic encryption in parallel with conventional encryption

In general, there are two ways of combination, as illustrated in Fig. 1 and 2 respectively. 1) Chaotic encryption is used as a separate part, preprocessing or postprocessing, in the combination. 2) Modify conventional encryption algorithms with chaotic signals. We could build new stream ciphers and new

0-7695-3016-8/07 $25.00 © 2007 IEEE
DOI 10.1109/ISDPE.2007.28

symmetric block ciphers by breaking inner structure of conventional encryption. For example, we could use chaotic sequences as the initial key, round key or S-boxes (substitution boxes) for the symmetric block cipher.

3. Image encryption using AES and chaotic series

In our proposed scheme, the image undergoes two encryption stages, which is shown in Fig. 3. In the first stage, we modify the pixel values with chaotic AES substitution. In the second stage, we permute the positions of pixels with a chaotic matrix.

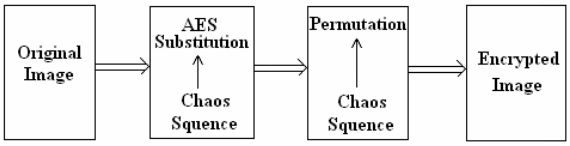


Figure 3. The system architecture

3.1. Chaotic AES substitution

In the first stage, we employ the AES encryption algorithm. In AES, data block is of 128b(bit).The key length may be set to 128b, 192b or 256b. In our system, we choose 128b for the key length and yield a key space of size 2^{128}.

If one key is adopted at a time, the plaintext size would be the same as the key text size. Obviously such a strategy is not scalable, since it is quite challenging to generate and manage so many keys. If we use static key, the same plaintext would produce the same ciphertext. The resulting recurrent pattern easily invites attack.

In our system, we use logistic chaotic sequence $X_{n+1}= rX_n(1-X_n)$ as AES initial keys. It generates keys with good randomness while at little additional cost. Besides, it can save the space of key storage and simplify the subsequent management.

To avoid similar values appearing first in the chaotic sequences, which is usually caused by similar initial values, we discard the first part of the sequence. To avoid short period, we set parameter r in the sequence $\{X_n\}$ according to another chaotic logistic sequence with a different initial value. That is, $r=f(Y_n)$, $Y_{n+1}= uY_n(1-Y_n)$. So the key space of the first stage is composed by [X(0),Y(0)], the initial values of two logistic maps.

3.2. Chaotic Permutation

In the second stage, we employ chaotic sequences again to generate permutation matrices, which are used to permute all pixels.

First, the chaotic sequence is produced the same way as in the first stage, but with different initial values. The key space of the second stage is composed by [Z(0),W(0)]. That is, the chaotic map W controls the parameter r of the chaotic map Z, $Z_{n+1}= rZ_n(1-Z_n)$.

Next, we generate the permutation matrix as follows: Since the value of logistic sequence Z is between 0 and 1, we use Z'= int(256Z) to generate a new integer sequence Z' with range [0,255]. If $j>i$ and Z'[j]=Z'[i], we discard repeated element Z'[j]. Then we arrange the resulting new sequence Z'' into an m by n image matrix, which is used as the permutation matrix.

As the following example shows, given the permutation array B(i), we can apply it to the original image array A(i) to produce the encrypted image array C(i) as C(i)=A(B(i)). Given the inverse permutation array B'(i), we can also obtain the decrypted image array D(i) as D(i)=C(B'(i)). For example: C(0)=A(B(0))=A(4)=a_4, D(0)= C(B'(0))= C(2)= A (0)=a_0.

$$A=\begin{bmatrix} a_0 & a_1 & a_2 \\ a_3 & a_4 & a_5 \\ a_6 & a_7 & a_8 \end{bmatrix} \quad B=\begin{bmatrix} 4 & 1 & 0 \\ 8 & 6 & 2 \\ 3 & 5 & 7 \end{bmatrix} \quad C=\begin{bmatrix} a_4 & a_1 & a_0 \\ a_8 & a_6 & a_2 \\ a_3 & a_5 & a_7 \end{bmatrix}$$

$$B'=\begin{bmatrix} 2 & 1 & 5 \\ 6 & 0 & 7 \\ 4 & 8 & 3 \end{bmatrix} \quad D=\begin{bmatrix} a_0 & a_1 & a_2 \\ a_3 & a_4 & a_5 \\ a_6 & a_7 & a_8 \end{bmatrix}=A$$

4. Experimental evaluation

First we evaluate the proposed chaotic permutation. We use Z'''=Z''/256 to generate a new permutation sequence Z''' with range [0,1]. The autocorrelation of the new permutation sequence is shown in Fig. 4. The waveform of auto-correlation property is rather acute.

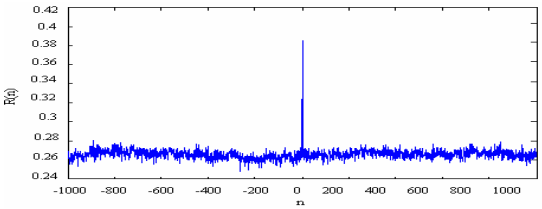
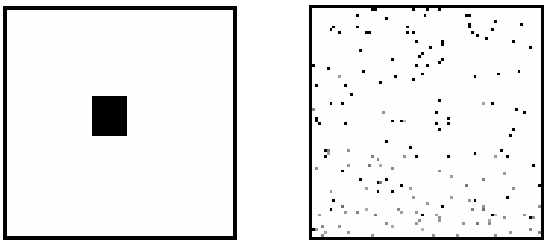


Figure 4. Auto-correlation property of the permutation sequence

The effect of image diffusion is better by permutation, as shown in Fig. 5. Therefore, due to the

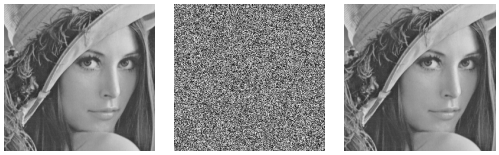
randomness of the permutation sequence, it is very suitable for image encryption.



original image encrypted image after permuting

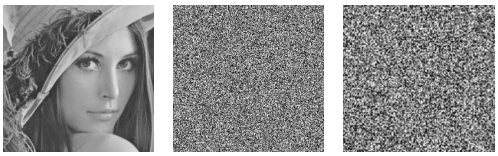
Figure 5. The effect of image diffusion

We tested the proposed cryptosystem on quite a few images. Due to lack of space, we only illustrate the results of "Lena", a 256 by 256 gray image of 8 bits. The original, encrypted and decrypted images are shown in Fig.6, respectively. One can see that the encrypted image is rather irregular and it is hard to find any pattern. However, there is no damage caused to the decrypted image. If one of four initial values [X(0),Y(0), Z(0),W(0)] is modified a bit, e.g., setting X(0)=0.4 for encryption, but setting X(0)=0.4+10^{-15} for decryption, the decrypted image becomes totally unrecognizable, as shown in Fig. 7.



original image encrypted image decrypted image

Figure 6. The effect of image encryption and decryption



original image encrypted image decrypted image

Figure 7. The decrypted image while decryption key is a little different from encryption key

5. Concluding Remarks

The initial values [X(0),Y(0), Z(0),W(0)] constitute the key space of the cryptosystem. During experiments, we employed double float format with precision up to 15-16 digits. Hence the key space size of the chaotic sequence is 10^{15}. The key space of the cryptosystem is up to 10^{60}-10^{64}, which is far greater than 2^{128} of AES with 128b key. Chaotic sequences were employed as AES initial keys. They preserved the strengths of AES as a conventional cryptography and also solved the problem of key generation and management. As for the pixel permutation, we proposed a new way of converting chaotic sequences into permutation matrices. Our experiments showed that it is both simple and effective.

The proposed composite scheme scrambled the image in both temporal domain and spatial domain, which enhanced the security by making decryption more difficult. For further security, we can enlarge the key space by generating the chaotic sequence with a multi-dimensional chaotic map. In practice, initial keys can be also encrypted by the RSA algorithm for key delivery security. The chaotic sequence used in our system was generated by a chaotic map. It is pseudo-chaotic[6], due to computation precision. The real chaotic sequence can be obtained by using an analog chaos oscillator and an A/D converter. We plan to study the above problems for future work.

6. References

[1] S. T. Fryska and M. A.Zohdy, "Computer dynamics and shadowing of chaotic orbits", Physics Letter A,166(5-6):340-346, 1992.

[2] S.J. Li, X.Q. Mou, B. L.Yang,Z. Ji,and J.H. Zhang, "Problems With A Probabilistic Encryption Scheme Based On Chaotic Systems", Int. J. Bifurcation and Chaos,13(10): 3063-3077, 2003.

[3] N. Masuda and K. Aihara, "Dynamical characterstics of discretized chaotic permutations", Int. J. Bifurcation and Chaos,12(10): 2087-2103, 2002.

[4] S. Gee, Basic Methods of Cryptography, Cambridge University Press, Cambridge, 1998.

[5] L. Kocarev, "Chaos-Based Cryptography: A Brief Overview". IEEE Circuit and System Magazine, 1(3):7-21, 2001.

[6] L. Kocarev and G. Jakimoski, "Pseudorandom bits generates by chaotic maps". IEEE Trans.Circuits and Systems-I,50(1):123-126, 2003.