IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 10, Issue 5 (Mar. - Apr. 2013), PP 61-64
www.iosrjournals.org

Image encryption using chaotic sequence and its cryptanalysis

Sagade A.G.[1], Prof. Pratap Singh[2]
[1]*Dept. of Computer Engineering, Institute Of Knowledge College Of Engineering, Pune, India*
[2] *Dept. of Computer Engineering, Institute Of Knowledge College Of Engineering, Pune, India*

Abstract : *MultiMedia is growing application in various areas ,security is an important issue in communication and storage of images and Encryption is a very common technique to uphold image security. Many encryption systems have been introduced among them; image encryption using chaotic sequence has many proposals. In this paper we analyze the security weakness of the proposal. We use chosen plain-text attack and known plain-text attack to reveal the secret parameters of the algorithm. That is to say, this method is not at all secure from the point of cryptography.*

Keywords - *Image encryption, Cryptography, Chaotic system, Encryption, Decryption.*

I. INTRODUCTION

Multimedia and visual information play an important role in people's life due to the wide application of computer and its relative technology. Image as necessary tool to transmit information has shown its great attention, it can be seen everywhere, The security of an image is very different from that of a text file. Because of its intrinsic characteristics, the encryption speed and algorithm simplicity are usually considered more important than the "absolute security" even if that were possible. The combination of chaotic theory and cryptography forms an important field of information security. Inspired by the subtle similarity between chaos and cryptography, a large number of chaos-based image encryption schemes have been proposed [1–3]. Chaotic systems have many important properties, such as the sensitive dependence on initial conditions and system parameters, pseudorandom property, no periodicity and topological transitivity, etc. Most properties meet some requirements such as diffusion and mixing in the sense of cryptography [4].Unfortunately, many of these schemes have been found insecure, especially against known and/or chosen-plaintext attacks [5]. In this paper, we study a complete break of the image encryption algorithm proposed in [6]. Where chosen-plaintext and known-plaintext attacks and observe that the algorithm can be completely broken using only a couple of known or chosen images. The method discussed is similar in spirit to the one proposed in [7]. However, in this approach uses the particular structure of the permutation to yield an exact break.

This paper is organized as follows. In the next section the image encryption scheme under study is briefly introduced. Then, in Section 3, chosen plain-text attack is briefly described. A known plain-image attack is introduced in Section 4. Some experimental results reported in section 5. Finally, some conclusions are given in Section 6.

II. DESCRIPTION OF ALGORITHM

The plaintext is an image of size $h \times w$, where each pixel is represented as a byte. The scheme uses three chaotic systems to generate the pseudo-random variables used in the three steps. The key of the overall system is two real parameters $x_0, y_0 \in (-1, 1)$. T he first chaotic system is a 2D discrete-time system given as,

$$\begin{bmatrix} x_0 \\ y_0 \end{bmatrix} = F\left(\begin{bmatrix} x_{n-1} \\ y_{n-1} \end{bmatrix}\right)$$

$$= \begin{cases} \begin{bmatrix} f_0(x_{n-1}) \\ y_n \end{bmatrix} & if\ x_{n-1} + y_{n-1} < 0 \\ \begin{bmatrix} x_{n-1} \\ f_1(y_{n-1}) \end{bmatrix} & if\ x_{n-1} + y_{n-1} \geq 0 \end{cases} \quad (1)$$

Where $f_0(u) = 8u^4 - 8u^2 + 1$ and $f_1(u) = 4u^3 - 3u$ at each step x_n, y_n one of the state variable is chosen as

$$z_n = \begin{cases} x_n & if\ x_{n-1} + y_{n-1} < 0 \\ y_n & if\ x_{n-1} + y_{n-1} \geq 0 \end{cases}$$

Finally, we obtain z_n from an integer k_n in the set {0, 1 …255} as

$k_n = [128(z_n + 1)]$

The chaotic system (1) is iterated *hw* times and the sequence $\{k_1, k_2, \ldots\ldots, k_{hw}\}$ is reshaped into an image using row scan. Let K denote this noise-like image. After finding the values of x_n, y_n we find out the integer sequence of $\boldsymbol{\rho}_n$ and $\boldsymbol{\sigma}_n$.

The second chaotic system is given by,

$x_n = \boldsymbol{f_0}(\boldsymbol{x}_{n-1})$ (2)

The third chaotic system is given by,

$y_n = \boldsymbol{f_1}(\boldsymbol{y}_{n-1})$ (3)

1.1 Encryption scheme :

These sequences are used in encryption operations - mixing, row rotation and column rotation [6]. Let P denote the plaintext image. In the mixing step, the plaintext is XORed with *K* to obtain the intermediate value *M*. In the row rotation step, each row of *M* is circularly rotated right with rotation amounts given in the sequence to obtained second intermediate variable *N*. Finally, the columns of *N* are circularly rotated down with rotation amounts taken from the sequence$\boldsymbol{\rho}_n$. So we get the cipher image *C*. Figure 1 shows the block diagram representation of the Encryption algorithm.

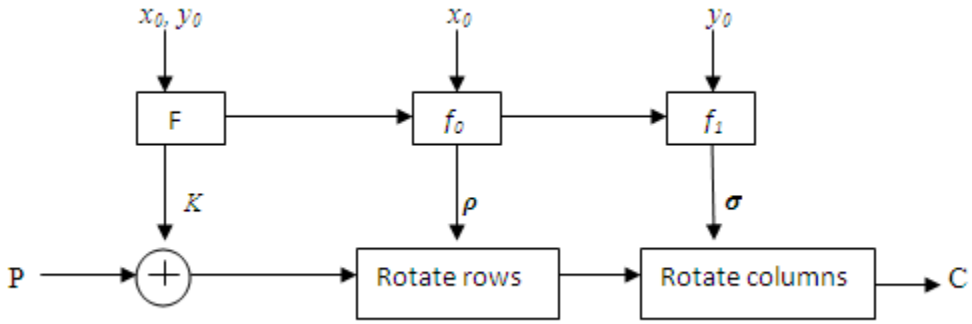

Fig.1. Encryption algorithm

1.2 Decryption scheme :

The decryption is straightforward. Using the secret parameters, x_0, y_0, we use (1), (2) and (3) to produce *K* and $\boldsymbol{\rho}$. We go from *C* to *M* using row rotation and column rotation steps respectively. We recover *P* with

$P = M \; XOR \; K$ (4)

III. Chosen Plain-Text Attack

In this section, we describe how the secret parameters of the proposed encryption algorithm can be extracted using a chosen plaintext attack. The paper [8] tells us that chaotic sequence K XOR with plain image *P*, is a breakthrough for chosen plaintext. If an attacker knows the parameters x_0 and y_0, he can reverse the two steps of the encryption and decrypt a cipher text image but there is no necessity to know secrete keys. If he succeed to reveal K, $\boldsymbol{\rho}$ and $\boldsymbol{\sigma}$ then, he can obtain the original image *P*. In this and the next section, we study attacks that try to recover K, $\boldsymbol{\rho}$ and $\boldsymbol{\sigma}$. Let attacker has pair of encrypted and decrypted image as (*P,C).* He chooses another plain image P_1 of size $h \times w$, Namely, P_1 differs from *P* only in the first row, and the Difference in every pixel is just 1. The attacker observes the cipher text C_1. Using,

$M = P \; XOR \; K$ (5)

We get M_1 image with zeros everywhere except on the first row, where we have 1s. Now using this with row rotation step, we have N_1 image such that $N_1 = M_1$. As M_1 remains the same under row rotation. When we

apply the column rotation to *N1*, the row of 1s is distributed according to σ in, $\Delta C = C \oplus C_1$

Since each column of has only one nonzero pixel, the attacker can thus determine σ . Now that the attacker knowsσ, he chooses another plaintext P_2 and obtains the cipher text C_2. This time, P_2 differs from P only in the first column Difference is again just 1 in every pixel. Since the attacker knows ΔC he uses row rotation to obtain the value of ΔN. He also knows ΔM. Note that, by the particular choice of P_2, the first column of ΔM is 1s and it is zero everywhere else. Once the attacker has revealed the rotation amounts σ and ρ, finding K is straightforward. He starts with C and uses row rotation then column rotation to obtain *M1*. Then, he reveals K using $K = P1 \oplus M1$.The chosen-plaintext attack requires one known and two chosen plaintext images. The attack requires very little amount of computation.

IV. Known Plain-Text Attack

Every time it is difficult to the attacker to chose a plain text and apply chosen plain text attack. In this section we describe a known-plaintext attack that requires about two known plaintext-cipher text pairs of images. Assume the plaintext-cipher text pairs *(P1, C1)* and *(P2, C2)* are known by the attacker. Attacker know $\Delta M = \Delta P$. Also, he calculates ΔC. Going from ΔM to ΔC we have first the rows and then the columns rotated. There are no modifications to the pixel values of ΔM. After observing the pixels position attacker shifts the pixels to certain positions and get the sequences *A*. Now, repeating the same procedure for all the pixels on the same row in ΔM. Attacker uses following intersection set to find out rotation sequence,

$$P_i \in \bigcap_{j=1}^{w} A_j \qquad (6)$$

Once the attacker has the sequence σ , he uses a similar set intersection method to reveal ρ. Again, the attacker repeats the set intersection, with additional known plaintexts if necessary, until the intersection is a single point. He repeats the whole procedure for all the columns. Once the attacker has σ and ρ, he uses column rotation then row rotation on a cipher text image *C1* to obtain *M1*. He then recovers the key *as* $K = M_1 \oplus P_1$.The attack requires only a few known plaintext-cipher text pairs for moderate image sizes.

As we know, the known-plaintext and chosen-plaintext attacks will be very meaningful if a same key is used to encrypt more than one plaintexts, especially in the case that a larger number of plaintexts are all encrypted with a same key [9]. For a "good" cipher, the capability to resist known-plaintext attack is very important and generally needed. It is because of the following fact: the key management will be very complex, inconvenient and inefficient in many applications, if any key must not be used to encrypt more than one plaintexts.

V. Simulations

To show some experimental results are shown. Fig.2 (a) shows original image which is encrypted using chaos compound sequence as shown in Fig.2 (b). The algorithm can be broken using chosen and known plain-text attack and correct image can be decrypted as in Fig.2 (c).

(a) (b) (c)

Fig.2. (a)Original image (b) Encrypted image (c) Correct decrypted image

The attack takes less than a minute on MATLAB running on Mac OS X 10.5.4 with Intel Core 2 Duo 2.16 GHz processor and 2 GB RAM[4] to give complete break to the image encryption algorithm.

VI. Conclusion

The security of a recently published image encryption scheme based on a compound chaotic sequence has been studied. It is found that the scheme can be broken with only three chosen plain-images. In addition, it is found that the scheme has some weak keys and equivalent keys, and that the scheme is not sufficiently sensitive to the changes of plain-images. Furthermore, the pseudo-random number sequence generated by iterating the compound chaotic function is found not to be sufficiently random for secure encryption. In summary, the scheme under study is not secure enough. Therefore, it is not be recommended for applications requiring a high level of security.

References

[1] J.C.Yen, J.I.Guo, A new chaotic key-based design for image encryption and decryption in *Proc. IEEE Int. Conf. Circuits and Systems, vol. 4*, 2000, pp. 49–52.

[2] H.-C. Chen, J.-C. Yen, A new cryptography system and its VLSI realization, *Journal of Systems and Architecture 49* (2003) 355–367.

[3] H.-C. Chen, J.-I. Guo, L.-C. Huang, J.-C. Yen, Design and realization of a new signal security system for multimedia data transmission, *EURASIP Journal on Applied Signal Processing 2003 (13)* (2003) 1291–1305.

[4] Zhang LH, Liao XF, Wang XB. An image encryption approach based on chaotic maps. *Chaos, Solitons & Fractals2005;24*: 759–65.

[5] Ercan Solak, Cryptanalysis of image encryption with compound chaotic sequence, 2009 6th International Multi-Conference on Systems, Signals and Devices, 978-1-4244-4346-8/09/ 2009 IEEE

[6] X. Tong, M. Cui, Image encryption with compound chaotic sequence cipher shifting dynamically, *Image and Vision Computing 26 (2008) 843–850*.

[7] S. Li, C. Li, G. Chen, N. G. Bourbakis, K. -T. Lo, A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks, *Signal Processing: Image Communication, 23 (2008) 212–223*.

[8] Fangjun Huang, Information Security Research Based on Discrete Chaotic Theory [D], Huazhong University of Science and Technology,Wuhan, 2005.

[9] Bruce Schneier, *Applied Cryptography – Protocols, algorithms,and souce code in C*, John Wiley & Sons, Inc., New York, second edition, 1996.