Cryptanalysis of Bigdeli Algorithm using Çokal and Solak Attack

Fatih Özkaynak*‡, A. Bedri Özer**, Sırma Yavuz***

* Department of Software Engineering, Faculty of Technology, Fırat University, 23119 Elazığ/Turkey

** Department of Computer Engineering, Faculty of Engineering, Fırat University, 23119 Elazığ/Turkey

*** Department of Computer Engineering, Faculty of Electric Electronic Engineering, 34220 İstanbul/Turkey

‡ Corresponding Author; Address: Tel: +90 424 237 0000, Fax: +90 424 236 7064, e-mail: ozkaynak@firat.edu.tr

Abstract- Since 1990s, chaos has been widely investigated to construct multimedia encryption scheme for its characteristics, such as the ergodicity, mixing and the sensitivity to initial conditions. This study is concerned with the cryptanalyses of recently proposed chaos based image encryption schemes [N. Bigdeli, Y. Farid, K. Afshar, A robust hybrid method for image encryption based on Hopfield neural network, Computers and Electrical Engineering 38 (2012) 356–369]. The security of the schemes against Çokal and Solak attack is investigated in detail with theoretical analyses and experimental results. We show that all the secret parameters can be revealed.

Keywords- Chaos based cryptography; cryptanalysis; chosen-plaintext attack.

1. Introduction

With the rapid development of multimedia and network technologies, the security of digital image data becomes more and more important, since digital image data are transmitted over open networks more and more frequently. Typically, reliable security in storage and transmission of digital image is needed in many applications.

Due to the tight relationship between chaos theory and cryptography, a great number of image encryption schemes use chaos as a mechanism to realize secret permutations of digital images, or as a source to generate pseudo-random bits to control secret encryption operations [1-5]. Meanwhile, some cryptanalysis work has also been published and a number of image encryption schemes have been found to be insecure from the cryptographic point of view [1, 2].

In [6], a new image encryption algorithm is proposed by Z.-H. Guan et al. (called Guan algorithm). In Guan algorithm, the plain image is first permutated with Arnold's cat map; then the shuffled image is encrypted by a keystream *B* generated from a Chen's chaotic system. In [7], Çokal and Solak pointed out that the secret key of Guan algorithm was independent of plain or ciphered image, then Authors proposed two attacks on the algorithm — chosen-plaintext attack and known-plaintext attack.

Similarly, Bidgeli et al. [8] proposed chaos based image encryption algorithm. The algorithm uses Arnold's cat map to shuffle the image pixels and hyper chaotic Hopfield neural network to change the gray levels of the shuffled image pixels. In this Letter, we give a complete break of proposed image encryption algorithm using Çokal and Solak attack.

The outline of the paper is as follows. In the next section we describe the encryption algorithm in detail. In Section 3, we summarize Çokal and Solak attack; then we illustrate the success of attack. Finally, we give concluding remarks.

2. Description of The Encryption Algorithm

In this section, we describe the encryption algorithm in detail. The encryption process consists of two parts. In the first part, the algorithm takes an image P and shuffles its pixels using Arnold cat map. The second part of the algorithm changes the gray levels of the pixels using hyper chaotic Hopfield neural network. The secret keys of the algorithm are $(m_{l1},m_{l2},X_{l1}(0),X_{l2}(0),M,R)$. The parameters $m_{l1},m_{l2},X_{l1}(0),X_{l2}(0)$ are initial values and control parameters of two logistic map. Logistic maps are used to generate chaotic control parameter for the permutation and diffusion stages. M is iteration number for two logistic map and R is round number for encryption scheme. The encryption steps are as follows:

- First logistic map is used to generate initial condition and control parameter of Arnold cat map. Shuffle the image P using Arnold cat map and obtain the shuffled image S. Assume that we have a $N\times N$ image P with the pixel coordinates $l=\{(x,y)|x,y=0,1,2,\ldots,N-1\}$. In [8], Arnold's Cat Map is given as Eq. (1). In Eq. (1) p,q are positive integers and x',y' are the coordinate values of the shuffled pixel. Using Arnold cat map with iterations, images are shuffled chaotically.

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} \bmod N \tag{1}$$

- Rearrange the image pixels as the sequence $S=\{s_1,s_2,\ldots,s_{(N\times N)}\}$ by scanning the image S using the usual row-scan method.
- Second logistic map is used to generate initial condition and control parameter of hyper chaotic Hopfield neural network; then Iterate chaotic system $N_0=(N\times N)/4$ times and obtain the real values x_i,y_i,z_i,t_i where $1\le i\le N_0$.
- Obtain the key sequence $B=\{B_1,B_2,\ldots,B_{(N\times N)}\}$ as:

$$\begin{aligned} B_{4(i-1)} &= \bmod(round((abs(x_i) - floor(abs(x_i)))\times 10^{14} + S_{4(i-1)}),256) \\ B_{4(i-1)+1} &= \bmod(round((abs(x_i) - floor(abs(x_i)))\times 10^{14} + S_{4(i-1)}),256) \\ B_{4(i-1)+2} &= \bmod(round((abs(x_i) - floor(abs(x_i)))\times 10^{14} + S_{4(i-1)}),256) \\ B_{4(i-1)+3} &= \bmod(round((abs(x_i) - floor(abs(x_i)))\times 10^{14} + S_{4(i-1)}),256) \end{aligned} \tag{2}$$

- Obtain the encrypted sequence $C=\{c_1,c_2,\ldots,c_{(N\times N)}\}$ as:

$$c_i = s_i \oplus b_i \tag{3}$$

- By reshaping the sequence C into an $N\times N$ image, obtain the ciphered image.

3. Cryptanalysis of Encryption Scheme

In this section, we describe how the secret parameters of the proposed encryption algorithm can be extracted using Çokal and Solak attack. In the chosen-plaintext attack, the attacker chooses a plain image and somehow obtains the corresponding ciphered image. By analysing the plain/ciphered image pair, he tries to reveal the secret parameters.

In [1], Solak says: "A particular class of attacks against chaos based ciphers aims at bypassing the chaotic part of the cryptosystem. In this class, the encryption algorithm is expressed in an equivalent form in which the chaotic subsystems are replaced by a set of secret maps or parameters". The security of the proposed image encryption scheme relies on the secrecy of the initial conditions and system parameters of two logistic maps. If an attacker knows the A of Arnold cat map and B generated with hyper chaotic Hopfield neural network, he can decrypt the ciphered image. Thus, the parameters A and B are the equivalent keys of the cryptosystem. If an attacker knows B, by using Eq. (3), he can obtain the shuffled image S. If he also knows A, he uses Eq. (1) and obtains the original image P.

For ease of understanding, assume that a small image with dimensions of 5×5 would be encrypted. For encryption algorithm, the same parameters selected in [8] were used. First, the attacker chooses the two images as plain images. Note that the first image P_1 consists of zero valued pixels and the second image P_2 has only two non-zero and distinct pixel. Then the attacker obtains the corresponding ciphered images, C_1,C_2.

$$P_1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}, P_2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{4}$$

The shuffling process using Arnold cat map for P_1 does not change the image because P_1 is identically 0. Hence, the shuffled image S_1 is equal to the image P_1. The attacker uses this fact with Eq. (3), and obtains that the ciphered image C_1 is exactly equal to the key K as:

$$C_1 = S_1 \oplus B = P_1 \oplus B = 0 \oplus B = B \tag{5}$$

The attacker already knows B. By using Eq. (3), the attacker obtains the corresponding shuffled image S_2 from C_2 as:

$$C_2 = S_2 \oplus B \tag{6}$$

Now, the attacker has the image P_2 and the corresponding shuffled image S_2. By searching for two non-zero and distinct pixel values in S_2, the attacker determines the shuffled coordinates (x_1', y_1') and (x_2', y_2'). Using Eq. (1), the attacker obtains the following sets of equations:

$$\begin{bmatrix} x_1' \\ y_1' \end{bmatrix} = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \bmod N$$
$$\begin{bmatrix} x_2' \\ y_2' \end{bmatrix} = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \bmod N \tag{7}$$

4. Conclusion

In this study, we gave a complete break of a chaos-based image encryption algorithm. We demonstrated that the secret keys can be revealed using Çokal and Solak attack. The computational complexity of the chosen-plaintext attack is only O(n), where n=2 is the number of chosen plain/ciphered image pairs used.

Design of cryptosystem by using the properties of chaotic systems has attracted the attention of many researchers. However, since most of the researchers have focused on the rich dynamics presented by chaotic systems, they did not pay attention to the fundamental criterions which must be considered while designing a cryptosystem. Therefore, that several algorithms are not cryptographically secure was shown by known, simple attacks. Eventually, chaos-based cryptology stays distant to mainstream cryptology literature only as an application field in cryptology subject of chaotic systems. Chaos based cryptography needs to incorporate rigorous tools and methods developed in mainstream cryptography. The designers should be well aware of the existing attacks and use strong and well-known structures in their designs.

References

[1] E. Solak, "Cryptanalysis of Chaotic Ciphers, in: L. Kocarev, S. Lian (Eds.), Chaos Based Cryptography Theory Algorithms and Applications", Springer-Verlag, pp.227-256, 2011.

[2] G. Alvarez, J. M. Amigo, D. Arroyo, S. Li, "Lessons Learnt from the Cryptanalysis of Chaos-Based Ciphers, in: L. Kocarev, S. Lian (Eds.), Chaos Based Cryptography Theory Algorithms and Applications", Springer-Verlag, pp. 257-295, 2011.

[3] J. M. Amigo, L. Kocarev, J. Szczapanski, "Theory and practice of chaotic cryptography", Physics Letters A 366, pp.211-216, 2007.

[4] G. Jakimoski, L. Kocarev. "Chaos and cryptography: block encryption ciphers". IEEE Trans Circ Syst—I 48/2, pp.163–169, 2001.

[5] G. Alvarez, S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems". International Journal of Bifurcation Chaos 16/8, pp.2129–2151, 2006.

[6] Z.-H. Guan, F. Huang, W. Guan, "Chaos-based image encryption algorithm", Physics Letters A 346, pp.153–157, 2005.

[7] C. Çokal, E. Solak, "Cryptanalysis of a chaos-based image encryption algorithm", Physics Letters A 373, pp.1357–1360, 2009.

[8] N. Bigdeli, Y. Farid, K. Afshar, "A robust hybrid method for image encryption based on Hopfield neural network", Computers and Electrical Engineering 38, pp.356–369, 2012.