Badr Mesned Alshammari

University of Ha'il , Ha'il, Saudi Arabia

doi:10.15199/48.2021.01.24

Cryptanalysis of a Bilateral-Diffusion image encryption algorithm based on dynamical compound chaos

Abstract. *This paper proposes an attack on a recently proposed cryptosystem using bilateral-diffusion algorithm with dynamical compound chaos. The original image encryption scheme employed a compound chaotic function and (linear feedback shift register) LFSR. Experimental results of the studied scheme showed that it is strong enough to resist against different attacks. The method used in the cryptosystem under study, presents weakness and a chosen plaintext attack can be done to recover the plain image without any knowledge of the key value. Only one pair of (plaintext/cipher text) is needed to totally break the cryptosystem.*

Streszczenie*, W artykule zaproponowano atak na kryptosystem wykorzystujący algorytm bilateral-diffusion z dynamiczna składową chaosu. Pokazano że jest możliwe wystarczająco mocny opór przeciwko różnym atakom. Jest więc możliwe odzyskanie obrazu. (****Analiza systemu szyfrowania z algorytmem bilateral diffusion bazującej na dynamicznej składowej chaosu*** *)*

Keywords: Power systems, Cryptanalysis; Chaos; LFSR; bilateral-diffusion; Chosen-plaintext attack
Słowa kluczowe:systemy szyfowania, chaos, algorytm bilateral diffusion

Introduction

Security of multimedia data is receiving an enormous attention due to the widespread transmission over various communication networks and designing the desired image encryption schemes has become a focal research topic. In this regards, in the last recent years, many researches have been concerned with the issue of chaos-based cryptography. The main features of chaotic systems (sensitivity to initial conditions, ergodicity, mixing property, simple analytic description and high complex behaviour) make them very interesting to design new cryptosystems. Inspired by the subtle similarity between chaos and cryptography, a large number of chaos-based image encryption schemes is proposed [1-5]. However, most of the encryption systems [6-11] have proved to be very weak and have a low level security, which makes them vulnerable to classical attacks, as the chosen plaintext attack or the known plaintext attack or other types of attacks. Fridrich in [12] used a model of image encryption architecture that divided the whole encryption process into two phases -- "permutation" and "substitution". Now many encryption systems are designed to fit this principle. Permutation is utilized to move the image pixels from one place to another, while sub-situation is used to make the statistics of cipher independent on the plaintext. Recently, a bilateral-di using image encryption algorithm with dynamical compound chaos and LFSR (Linear Feedback Shift Register as shown in Figure 1) is proposed in [13]. In this cryptosystem, the author neglects the permutation phase and the scheme is based only on the diffusion phase: sub-situations of pixel values with XOR operations. The XOR substitutions are controlled by a real number sequence generated by dynamical compound chaotic maps and LFSR. This research aims at cryptanalyzing this encryption algorithm using chosen plaintext attack. Only one pair of (plaintext/cipher text) was needed to break the cryptosystem. The rest of the paper is organized as follows. The next section presents a description of the original encryption algorithm briefly. Then, some weaknesses of this system are revealed in section 3. Section 4 is dedicated to explaining how to break the cryptosystem through a chosen plaintext attack. Finally, Section 5 encloses the summary and main conclusions of the current cryptanalysis work.

Review of the cryptosystem

The original image encryption scheme employed a compound chaotic function and LFSR. The map was designed by the author and it proved to be chaotic.

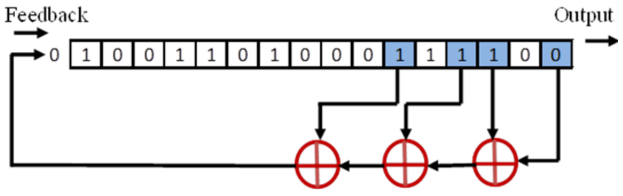

Fig. 1. Linear Feedback Shift Register

Chaos theory

Chaos theory is a distinguished theory which describes that the nonlinear dynamical systems convert from ordered state to disordered state. The dynamical systems are established based on various chaos functions such as logistic map. They are very sensitive to the initial parameters. A large number of random iterative values with the desirable properties of non-correlation, pseudo-randomness, and ergodicity is generated from the use of a chaotic map. The chaotic maps have demonstrated a great potential for information security, especially for image encryption. Chaotic cryptography is the application of the mathematical chaos theory to the practice of the cryptography. Since being first investigated by Robert Matthews in 1989,[1] the use of chaos in cryptography has attracted much interest; however, long-standing concerns about its security and implementation speed continue to limit its implementation [14-18]. In order to use chaos theory efficiently in cryptography, the chaotic maps should be implemented such that the entropy generated by the map can produce the required confusion and diffusion. Properties in chaotic systems and cryptographic primitives share unique characteristics that allow the chaotic systems to be applied to cryptography [19].The unpredictable behaviour of the chaotic maps can be used in the generation of random numbers. The concept of chaos cryptography, or in other words, chaos-based cryptography can be divided into two major groups: the asymmetric [20-24] chaos-based cryptography and the symmetric chaos-based cryptography. The majority of the symmetric chaos-based algorithms are based on the application of discrete chaotic maps in their process. Some of the earliest chaos-based random number generators tried to directly generate random numbers from the logistic map. The speed of the cryptosystem is always an important parameter in the evaluation of the efficiency of a cryptography algorithm;

therefore, the designers were initially interested in using simple chaotic maps such as the tent map, and the logistic map. However, in last years, the new image encryption algorithms based on more sophisticated chaotic maps proved that application of chaotic maps with higher dimension could improve the quality and security of the cryptosystems. Chaos and cryptography share some similar characteristics shown in Figure 2.

a) Both of the chaotic map and the encryption system are deterministic (not probable).
b) Both of the chaotic map and the encryption system are deterministic (not probable).
c) A chaotic system is sensitive to the initial condition. Hence small changes to any element can lead to changing the output fully. Cryptography depends on key-based confusion and diffusion. Therefore, modifying one bit of plain text or key could change all bits of the cipher text with 50% probability.
d) The iterative chaotic system is topological transitive and cryptography is multi round transformation.

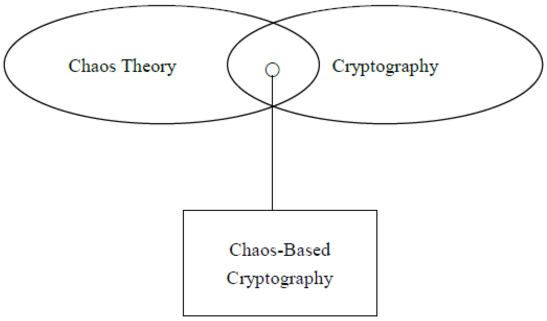

Fig. 2. Relation between chaos and cryptography

Chaos is also different from cryptography in some other features.
a) Chaotic systems are based on real/complex number spaces (bounded continuous space) whereas cryptography is defined as binary sequences (finite discrete space).
b) Chaos theory provides the idea to understand the asymptotic behaviour of iterative processes whereas cryptography defines the characteristics of first a few iterations.

The design of dynamical compound chaotic system

The compound chaotic function is generated as follows.

(1) $$\begin{cases} f_0(x_{n-1}) = 8x_{n-1}^4 - 8x_{n-1}^2 + 1 \\ f_1(x_{n-1}) = 4x_{n-1}^3 - 8x_{n-1} \end{cases}$$

(2) $$x_n = F(x_{n-1}) = \begin{cases} f_0(x_{n-1}) & IF\ x_{n-1} < 0 \\ f_1(x_{n-1}) & IF\ x_{n-1} \geq 0 \end{cases}$$

Where $x \in [-1,1]$

The system will choose one of the functions and mix it with LFSR to produce the chaotic two-value sequence dynamically. LFSR is made up of two parts: output and feedback function as shown in Figure 1. The first part consists of k1, k2,…,kn, and the second part of c1, c2,…, cn. The register shifts right one bit and outputs one bit. The feedback function inputs one bit on the left high position, which is cycle on one time after another. N level output sequences of LFSR $\{k_j\}$ are as follows.

(3) $$k_j = c_{j-1}.k_{j-1} \oplus c_{j-2}.k_{j-2} \oplus \cdots \oplus c_{j-n}.k_{j-n} (j \geq n)$$

Then plus the pseudorandom number generated by chaotic sequence to get a new numbers. Then the new result is used to mod 256, and the result is the real key stream to be used for encryption. It can be mentioned that the keystream does not depend on the plaintext.

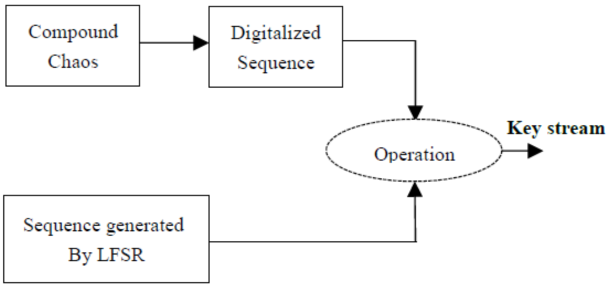

Fig. 3. The mix system of LFSR and compound chaos.

The design of bilateral-diffusion image encryption

The encryption scheme is performed in four steps. These are as follows:

Step 1: Read the plain image I with the size of (m×n).

Step 2: Choice of chaotic map (Figure 4)

where x_0 and x_1 are the initial values of chaotic maps; $f_0(x)$ and $f_1(x)$. If x ≥ 0 then, choose $f_1(x)$.

Put x_1 into $f_1(x)$ to get the first value of the chaotic sequence value1, and then make x_1 = value1, compute again, compute x =0.5 (x_0 + x_1), then judge which map to chose. The Algorithm 1, named Gen_Seq(x_0, x_1), and which was applied to generate the chaotic compound sequence Seqi, is described as follows.

Step 3: Chaotic sequence:

(4) $$S(i) = \left(d_i \times 2^{10}\right) \bmod 256,\ i = 1,\cdots,m*n$$

d_i is the real number generated by the dynamical compound chaotic maps and LFSR and S(i) is the digital chaotic sequence.

Algorithm 1 $Gen\_Seq(x_0, x_1)$

```
Input: $x_0$, $x_1$
Output: $Seq$
    $i \leftarrow 1$
    while $i \leq m*n$ do
      $x \leftarrow (x_0 + x_1)/2$
      if $x \geq 0$ then
        $x_1 \leftarrow 4x^3 - 3x$
        $Seq(i) = x_1$
      else
        $x_0 \leftarrow 8x^4 - 8x^2 + 1$
        $Seq(i) = x_0$
      end if
      $i \leftarrow i + 1$
    end while
```

Step 4: Bilateral-Di using encryption: Encrypt the plain image with Eq. (5) to get an intermediate cipher image C*.

(5)) $$C_i^* = \left[\left(S(i) + I_i\right) \bmod 256\right] \oplus C_{i-1},\ i = 1,2,\cdots,m*n$$

Reverse C*, using Eq. (6) to obtain the final ciphered image.

(6) $$C_i = C^*_{M+1-i}, i = 1, 2, \cdots, m*n$$

The method of bilateral-diffusion encryption is shown in Figure 5. In addition, the process of diffusion function is shown in Figure 6.

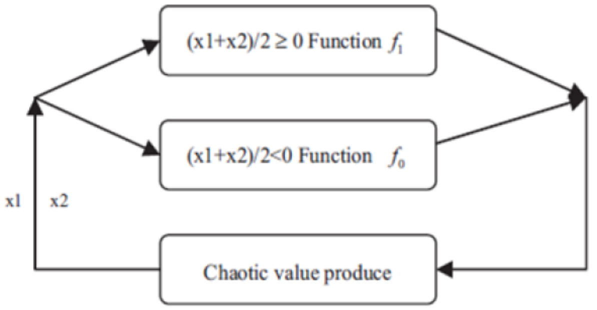

Fig. 4. Method for choosing chaotic map dynamically

Design weaknesses

In the system under study in [13], there is a serious problem with the encryption architecture, which informs about security breaches and presents a clear idea about the attack that can break the system.

Weak keys

Referring to [25], the cryptosystem under study, it is observed that some keys will cause some or even all encryption parts to fail, due to the existence of some fixed points of the chaotic maps:

$$f_0(1) = 1,\ f_0(-0.5) = -0.5,\ f_1(1) = 1,\ f_1(0) = 0,\ f_1(-1) = -1$$

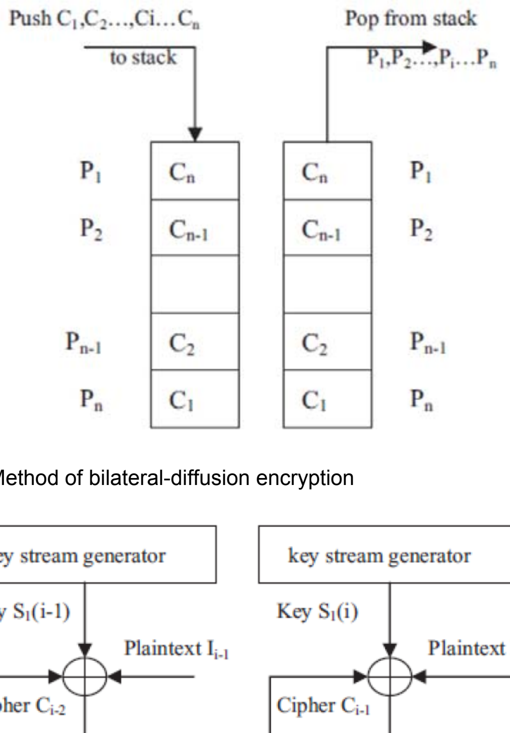

Fig. 5.Method of bilateral-diffusion encryption

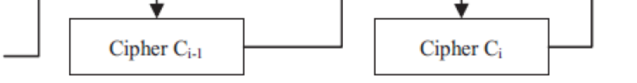

Fig. 6. Process of the diffusion

Thereby, five classes of weak keys are listed.

1. $\{1,1\} \Rightarrow$ sequence generated by the compound chaotic map $= \{1,1,1,\cdots\}$
2. $\{-1,-1\} \Rightarrow$ sequence generated by the compound chaotic map $= \{-1,0,-1,0,-1,0,-1,\cdots\}$
3. $\{0,0\} \Rightarrow$ sequence generated by the compound chaotic map $= \{0,0,0,\cdots\}$
4. $\{1,-1\} \Rightarrow$ sequence generated by the compound chaotic map $= \{-0,-1,0,-1,0,-1,\cdots\}$
5. $\{-0.5,-0.5\} \Rightarrow$ sequence generated by the compound chaotic map $= \{-0.5,-0.5,-0.5,\cdots\}$

Vulnerability against a chosen-plaintext attack

Vulnerability against a chosen-plaintext attack:

- Cipher text-only attack: the attacker only knows the result of the encryption.
- Known-plaintext attack: several pairs of plaintext and cipher text are accessible for the attacker.
- Chosen-plaintext attack: the attacker gains access to the encryption machine and performs cryptanalysis by selecting adequate plaintexts.
- Chosen-ciphertext attack: the decryption machine can be used by the cryptanalyst.

Through analysing step 3, it is found that the keystream remains unchanged for different image encryption schemes. Thus, the chaotic keystream S will be revealed instead of the two secret keys (x_0, x_1). In fact, the cryptosystem proposed is Inadequate secured and can be broken with the Chosen-plaintext attack.

Sensitivity to the change of plain-image

From Equations (5-6) one can easily see that changing one bit of I_i influences the same bit of Ci only. Note that this low sensitivity is actually a common problem with all XOR-based encryption systems. On the other hand, it becomes trivial if the key is not repeatedly used. In this case, it is rare that two slightly different plaintexts are encrypted by the same keystream.

Proposed attack

The goal of the attack described in the following section is to recover the plain image from its ciphered image C without knowing the cryptosystem keys x_0 and x_1 (the initial values of chaotic map).

Chosen-plaintext attack

Suppose that the attacker has temporary access to the encryption machinery. This enables him to choose special images and generate their corresponding ciphered images.

Suppose the attacker chooses a zero-image, Ii, as an input to the encryption machinery and generates the corresponding ciphered image Ci to recover the key stream Si. It is found that the keystream S_i does not depend on the plaintext. Therefore, it will be the same for all other images. According to Equation (6), the ciphered image, Figure 7(a), is reversed to obtain the intermediate ciphered image C^*_i Figure 7(b), Having, C^*_i Equation (5) becomes:

(7) $$C^*_i = S(i) \oplus C^*_{i-1}$$

The keystream S(i) is obtained through:

(8) $$S(i) = C^*_i \oplus C^*_{i-1}$$

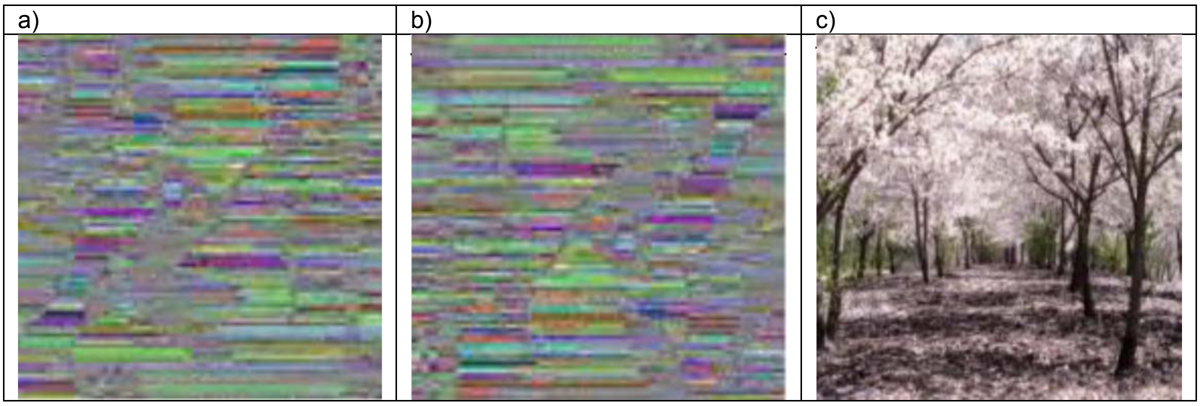

Fig. 7. The proposed attack.
a) encrypted image, b) intermediate encrypted image , c) recovered image

Conclusion

In this paper, the problems and weaknesses in a recent image encryption scheme with dynamical compound chaos are presented. The work in this paper has shown that it can be successfully cryptanalyzed through one couple of (plaintext / ciphertext). This paper has demonstrated that the scheme has some weak keys, and isn't sufficiently sensitive to the changes of plain-images.

Author: *Dr. Badr Mesned Alshammari (corresponding), Electrical Engineering Department, University of Hail, KSA. e-mail: bms.alshammari@uoh.edu.sa;*

REFERENCES

[1] J.-C. Yen, J.-I. Guo, A new chaotic key-based design for image encryption and decryp-tion, Proc. IEEE Int. Conf. Circuits and Systems, vol. 4, (2000) 49-52.

[2] A. Kanso, M. Ghebleh, A novel image encryption algorithm based on a 3D chaotic map, Commun Nonlinear Sci Numer Simulat (2012);17:2943-59.

[3] N. Pareek, V. Patidar, K. Sud, Image encryption using chaotic logistic map, Image and Vision Computing 24 (9) (2006) 926-934.

[4] Y. Tang, Z. Wang, J. Fang, Image encryption using chaotic coupled map lattices with time-varying delays. Commun Nonlinear Sci Numer Simulat (2010);15:2456-68.

[5] K. Wong, B. Kwok, W. Law, A fast image encryption scheme based on chaotic standard map. Phys Lett A (2008);372:2645-52.

[6] Arroyo D, Rhouma R, Alvarez G, Li S, Fernandez V. On the security of a new image encryption scheme based on chaotic map lattices. Chaos Interdiscip J Nonlinear Sci (2008);18. Art No. 033112.

[7] Solak E, okal C. Comment on encryption and decryption of images with chaotic map lattices. Chaos Interdiscip J Nonlinear Sci 2008;18(3). Art No. 03810.

[8] E.Solak,C.Cokal, O.T.Yildiz,T.Biyikoglu, Cryptanalysis of Fridrichs chaotic image encryption,International Journal of Bifurcation and Chaos 20(5)(2010)1405-1413.

[9] E.Solak,C.Cokal, Algebraic break of image ciphers based on discretized chaotic map lattices,Information Sciences 181 (1) (2011) 227-233.

[10] C. Li, D. Arroyo, K.-T. Lo, Breaking a chaotic cryptographic scheme based on compo-sition maps, International Journal of Bifurcation and Chaos 20 (8) (2010) 2561{2568.

[11] D.Arroyo,G.Alvarez,J.M.Amigo, S.Li,Cryptanalysis of a family of self-synchronizing chaotic stream ciphers,Communications in Nonlinear Science and Numerical Simulation 16 (2) (2011) 805-813.

[12] J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps, International journal of Bifurcation and Chaos 8 (1998) 1259{1284.

[13] X.J. Tong, The novel bilateral{Di usion image encryption algorithm with dynamical compound chaos, The Journal of Systems and Software 85 (2012) 850-858.

[14] D.D. Wheeler, R.A.J. Matthews, Supercomputer investigations of a chaotic encryption algorithm, Cryptologia, Vol. 15, No. 2,pp. 140-152, 1991.

[15] C. Yong, X. Liao, Cryptanalysis on a modified Baptista-type cryptosystem with chaotic masking algorithm, Physics letters A, Vol. 342, No. 5-6,pp. 389-396, 2005.

[16] X.E. Yong, On the cryptanalysis of Fridrich's chaotic image encryption scheme, Signal processing, Vol. 132, pp. 150-154, 2017.

[17] A. Akhavan, A. Samsudin, A. Akhshani, Cryptanalysis of an improvement over an image encryption method based on total shuffling, Optics Communications, Vol. 350,pp. 77-82, 2015.

[18] A. Akhavan,A. Samsudin, A. Akhshani,Cryptanalysis of an image encryption algorithm based on DNA encoding, Optics & Laser Technology, Vol. 95, pp. 94–99, 2017.

[19] M.S. Baptista, Cryptography with chaos, Physics letters A, Vol. 240, No. 1-2 , pp. 50-54, 1998.

[20] K. Ljupco, Public-key encryption with chaos, Chaos: An Interdisciplinary Journal of Nonlinear Science, Vol. 14, No. 4, pp. 1078-1082, 2004.

[21] L. Kocarev, J. Makraduli, P. Amato, Public-key encryption based on Chebyshev polynomials, Circuits, Systems and Signal Processing, Vol. 24, No. 5, pp. 497-517, 2005.

[22] A. Amir, A. Samsudin, A. Akhshani, A symmetric image encryption scheme based on combination of nonlinear chaotic maps, Journal of the Franklin Institute, Vol. 348, No. 8, 1797-1813, 2011.

[23] M.Yaobin, G. Chen, Chaos-based image encryption, Handbook of geometric computing, Springer, Berlin, Heidelberg, pp. 231-265, 2005.

[24] B. Sohrab, A novel algorithm for image encryption based on mixture of chaotic maps, Chaos, Solitons & Fractals, Vol. 35, No. 2, pp. 408-419, 2008.

[25] C. Li, S. Li, G. Chen, W.A. Halang, Cryptanalysis of an image encryption scheme based on a compound chaotic sequenceImage and Vision Computing 27 (2009) 1035-1039

[26] D. Stinson, Cryptography: Theory and Practice, CRC Press, 1995.