Journal of mathematics and computer Science 9 (2014) 451 - 457

Contents list available at JMCS

Journal of Mathematics and Computer Science

Journal Homepage: www.tjmcs.com

The Confusion-Diffusion Image Encryption Algorithm with Dynamical Compound Chaos

J. Vahidi

Department of Applied Mathematics, Iran University of Science and Technology, Behshahr, Iran,

jvahidi@iust.ac.ir

M. Gorji

Department Of Computer Engineering Software, Science and Research Branch, Islamic Azad University, Mazandaran, Iran,

A_gorji55@yahoo.com

Article history:
Received December 2013
Accepted February 2014
Available online February 2014

Abstract

Chaos may be degenerated due to finit precision effects, Therefore, in this study, a new compound two-dimensional chaotic function consists of two one-dimensional chaotic functions which are randomly created. A new chaotic sequences generator is designed by LFSR and the compound chaotic functions, which can generate very large key space. Image encryption algorithm is proposed based on diffusion and confusion by mapping 3D baker and dynamic combination chaos functions.

Keywords: Image encryption, Dynamical Compound chaos, Diffusion, confusion, 3D baker, LFSR

1. Introduction

Chaos seemingly random and chaotic behavior that occurs in many real-world phenomena. In 1963, American meteorologist Lorenz found random behavior in definite system and proposed "butterfly" theory.

Since the 1990s, chaotic dynamic systems are used in the design for data encryption extensively. Chaotic system has many good features such as pseudorandom, orbit inscrutability, sensitivity of initial and control parameters, which are in line with the cryptography requirements. So it has been widely used in the field of cryptography since 1990. In the late 80th, British mathematician Matthews firstly used chaos to encrypt (Matthews, 1989; Xiang and Qiu, 2008), who officially proposed a new algorithm producing key stream based on Logistic map in issue “Cryptologia”, and the information is encrypted in the method of stream cipher. Later, Habutsu and others proposed the first chaotic block cipher algorithm in the 1991s European cryptology meeting, which had signed the birth of chaotic block cipher. In 1998, Friedrich was suggested that an image encryption scheme should be repeated two steps: diffusion and confusion. The

confusion step is transferring the image pixels with using of the two-dimensional or three-dimensional chaotic maps to the new location. In diffusion stage, the pixel values change to stream form, Changes made to a particular pixel is dependent on the all pixels previous. Chen and colleagues (2004) at substitution step used of a ACM three-dimensional and 3D Baker mapping. Lian and colleagues (2005) was used of the standard two-dimensional mapping in confusion phase and a logistic map in the diffusion phase. The parameters and initial values of these chaotic maps determine by key sequences in each round. The rest of this paper is organized as follows. The first explain the proposed algorithm components, and then is presented proposed image encryption algorithm. This is symmetric algorithm. The encryption architecture consists of two parts: permutation and diffusion an image pixel.

2. Components of the encryption algorithm

2.1. The design of dynamical compound chaotic system

Since the Lorentz published his observations in the context of chaos, it has attracted much attention in the scientific community. Nonlinear mechanics and chaos theory is developed to model the behavior of complex systems and caused describe many of the systems behavior with the mathematical model.
The compound chaotic referred in this paper is generated as follows (Tong and Cui, 2008):

$$\begin{cases} f_0(x_{n-1}) = 8x_{n-1}^4 - 8x_{n-1}^2 + 1 \\ f_1(x_{n-1}) = 4x_{n-1}^3 - 3x_{n-1} \qquad x \in I = [-1,1] \\ x_n = F(x_{n-1}) = \begin{cases} f_0(x_{n-1}) & x_{n-1} < 0 \\ f_1(x_{n-1}) & x_{n-1} \geq 0 \end{cases} \end{cases} \tag{1}$$

The system will choose one of the functions to produce the chaotic two-value sequence dynamically. With the method of trajectory transition, the system acquired more properties of randomness. If we get a value smaller than 0 after n-1 iterations we will put the last value into function $f_0(x)$, else if the value is not smaller than 0 we put the last value into function $f_1(x)$.

User inputs two double precision parameters χ_1, χ_2 as the initial values of chaotic map $f_0(x)$ and $f_1(x)$. Using $x = (\chi_1 + \chi_2)/2$ to judge which map should be chosen. If $x \geq 0$, then choose $f_1(x)$. Put χ_1 into $f_1(x)$ to get the first value of the chaotic sequence value1, and then make χ_1=value1, compute $x = (\chi_1 + \chi_2)/2$ again, then judge which map to be chosen. This dynamic method of choosing chaotic maps is more random then traditional single chaotic map, and makes key space bigger, which increases the difficulty of attack.

2.2 Design key stream

Linear Feedback Shift Registers (LFSR) because of the pseudo-noise sequences with very long periods and their behavior is analyzed well-algebraic methods, used widely in the key sequence generator, the Cryptography system. The register is generate a sequence of binary bits. LFSR is made up by two parts seen in Fig. 1 shift register and feedback function. 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.

Here we given one LFSR with the primitive polynomial $x^{20}+x^{3}+1$ is seen in Fig 1. Using LFSR of 20 bits to generate 8 bits binary number every time, and 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. Here $s_1(i)=\left(p_i \times 2^{10}\right) \bmod 256, \quad i=1,2,\ldots$, p_i is the real number generated by the dynamical compound chaotic maps and LFSR. $s_1(i)$ is the digital chaotic sequence.

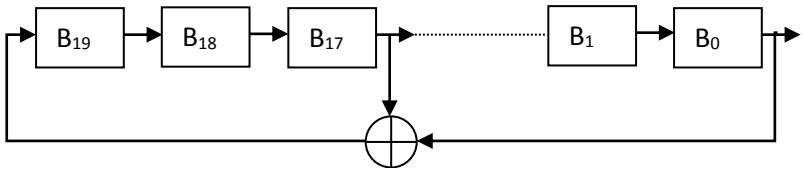


Fig. 1 LFSR of 20 bit [Tong 2012]

3. The proposed encryption algorithm

In order to produce diffusion and confusion effect, a round times is applied in the processes of encryption and decryption.

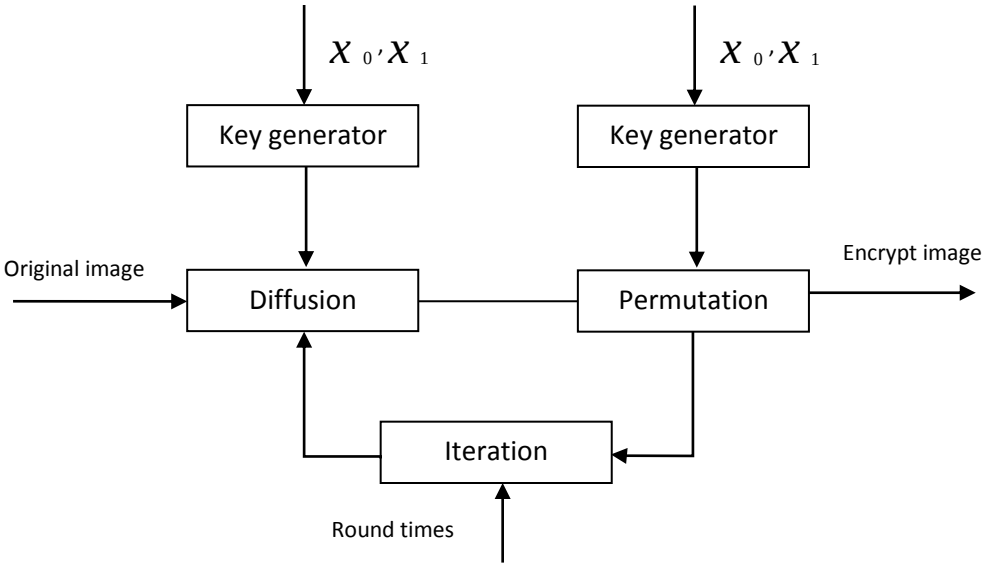


Fig.2. the model of encryption

3.1 Permutation of the pixels matrix based on 3D baker

The image data should be convert into a 3D array, which is described as a unit cube. The unit cube is first divided into several small cubes. The unit cube is divided into k*t blocks, there are two sets as follows:

$$\begin{aligned}&\{n_i \mid i = 1,2,3,...,k, n_1 + n_2 + ... + n_k = w\}\\&\{m_i \mid i = 1,2,3,...,k, m_1 + m_2 + ... + m_t = L\}\end{aligned} \quad (2)$$

Where W is the width of unit cube and L is the length of unit cube. Then length, width and height of the unit cube should be defined as follows:

$$W \times L \times H = M \times N$$

$$\begin{cases} W = \dfrac{M}{4}, L = \dfrac{N}{3}, H = 32 & if \quad N \mod 8 = 0, \\ W = \dfrac{M}{4}, L = \dfrac{N}{4}, H = 16 & if \quad N \mod 8 \neq 0 \quad and \quad N \mod 4 = 0, \\ W = \dfrac{M}{4}, L = \dfrac{N}{2}, H = 8 & if \quad N \mod 4 \neq 0 \quad and \quad N \mod 2 = 0, \\ W = \dfrac{M}{4}, L = N, H = 4 & if \quad N \mod 2 \neq 0, \end{cases} \quad (3)$$

Second, the blocks number of the unit cube should be defined. The user needs to initialize block number k and t. Through Eq. (1) to produce the compound chaotic sequence, a lot of different float numbers in [-1, 1] are obtained and the array X and Y are initialized with these numbers, where the length of the array X is k and the length of the array Y is t. The value of the array X and Y can be converted into integer according to the two formulas:

$$\begin{aligned}X_i &= \left\lfloor \left[x_i - (-1) \right] \times W/2 \right\rfloor \\ Y_i &= \left\lfloor \left[y_i - (-1) \right] \times L/2 \right\rfloor\end{aligned} \quad (4)$$

The length m_j and the width n_i of every block can be acquired according to the distance between every two points on the x-axis and y-axis according to the two formulas:

$$\begin{aligned}n_i &= X_i - X_{i-1}, \qquad X_0 = 0 \\ m_j &= Y_j - Y_{j-1}, \qquad Y_0 = 0\end{aligned} \quad (5)$$

The 3D baker map is as follows:

$$
\begin{aligned}
&B3(x, y, z) = (x', y', z'),\\
&x' = \mathrm{mod}\left(\mathrm{mod}(num, WL), W\right)\\
&y' = \left\lfloor \mathrm{mod}(num, WL) / W \right\rfloor\\
&z' = \left\lfloor num / WL \right\rfloor\\
&num = (WG_j + m_j F_i) H + z m_j n_i + (y - G_j) n_i + x - F_i,\\
&F_i = \sum_{k=1}^{i-1} n_k \quad , F_1 = 0 \quad , G_j = \sum_{k=1}^{j-1} m_k \quad G_1 = 0,
\end{aligned}
\tag{6}
$$

The cryptosystem's security is relation with its iteration times k,t and round times n of the confusion.

3.2 Diffusion function

The encryption method can be expressed as $C_i = \left[\left(S_1(i) + I_i\right) \bmod N\right] \oplus C_{i-1}$, shown in Fig. 3. where C_i means the value of ith cipher byte, $S_1(i)$ means the key sequence, I_i means the value of ith byte plaintext, N is 256. $S_1(i)$ is generated in section 2.2, which is from 0 to 255.

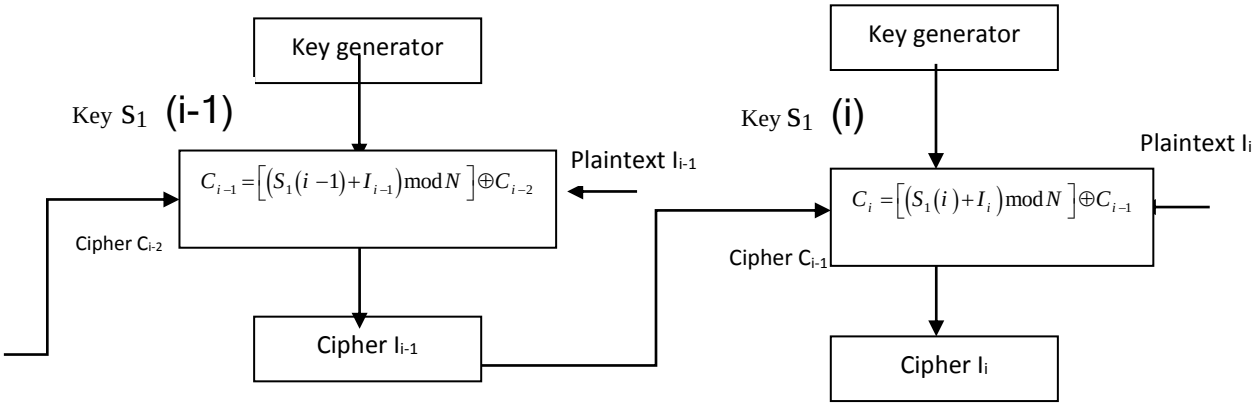


Fig. 3. The mode of diffusion

4. Security analysis for the compound chaotic function

4.1. Space of the key

The compound chaotic map $F(x)$ needs two initial two values, so the key space of the chaotic system is larger than that of the chaotic system based on the logistic map. One dimensional key space of chaotic function is 2×10^{28}, but the key space of two-dimensional compound chaotic function is 4×10^{28}, which has larger key space than one-dimensional chaotic function. Balance, avalanche effect and other properties are better than one-dimensional chaos functions. It is the motivation for using the compound two-dimensional chaotic function.

4.2 Histograms of encrypted image

From Fig. 4 we can see that the histograms of the encrypted image are fairly uniform and significantly different from the histograms of the original image and hence it does not provide any clue to employ and statistical analysis attack on the encryption image.

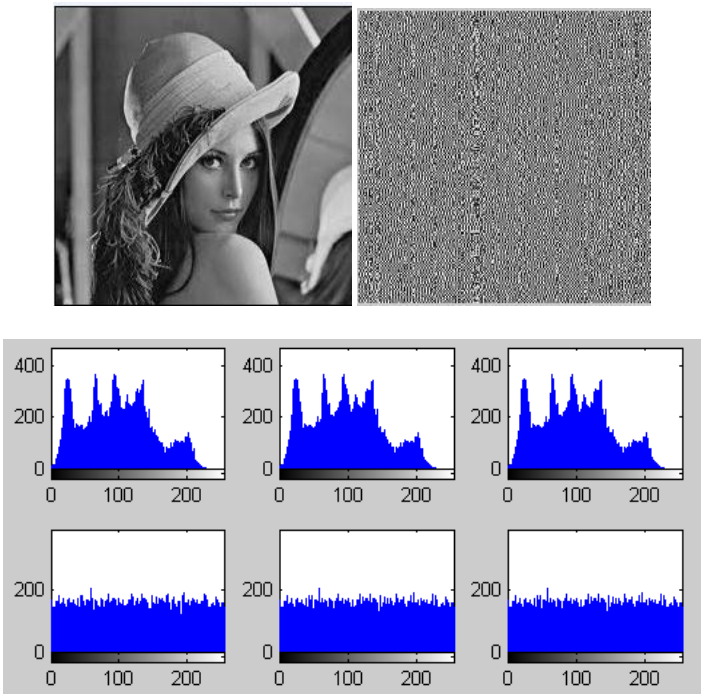
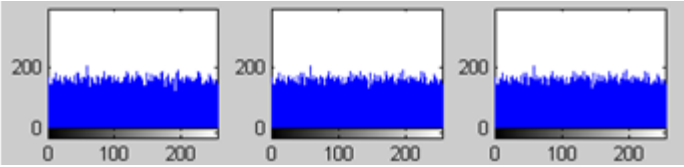


Fig.4. Histogram of Lena

4.3 Sensitivity analysis

Sensivity analysis for the cipher to key: First Lena image is encrypted by using a pair of keys. Then the least significant bit of key is changed, which is used to encrypt the same image. Finally, the above two cipher images, encrypted by the two slightly different keys, are compared.



5. Conclusions

In this paper we propose the scheme, a compound chaotic function with two one-dimensional dynamically chaotic functions. We also design a Diffusion-Confusion image encryption with LFSR and dynamical compound chaos and dynamical dividing #d baker model. The experimental results show that our design has the wide key space, cipher is sensitive to the key and plaintext, also show that the key space is large enough to resist exhaustive key attacks and difference analysis.

References

[1] F. Xiang, S. Qiu, Analysis on stability of binary chaotic pseudorandom. IEEE Communications Letters 12 (5): (2008) 337–339.
[2] G. Chen, Y. Mao, C. Chui, A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solutions & Fractals 12: (2004) 749-761.
[3] M.A. Fadhil Al-Husainy, A novel encryption method for image security. International Journal of Security and Its Applications Vol. 6, No. 1, (2012).
[4] J. Fridrich, Symmetric ciphers based on two dimensional chaotic maps. International Journal of Bifurcate Chaos, 8(6): 1259-1284, (1998).
[5] K. Lu, J.H. Sun, R.B. Ouyang, et al. Chaotic Dynamics. Shanghai Translation Press. Shanghai, pp. 17–51, (1990).
[6] Y. Mao, G. Chen, S. Lian, A novel fast image encryption scheme based on 3d chaotic baker maps. International Journal of Bifurcation and Chaos, Vol. 14, No. 10 : 3613-3624, (2004).
[7] Y. Mao, G. Chen, Chaos-based image encryption. Handbook of Computational Geometry for Pattern Recognition, Computer Vision, Neurocomputing and Robotics. New York: Springer-Verlag; in press (2003).
[8] G. Makris, I. Antoniou, Cryptography with Chaos. Chaotic Modeling and Simulation (CMSIM) 1: 169-178, (2013).
[9] N.K. Pareek, V. Patidar, K.K. Sud, Image encryption using chaotic logistic map. Image and Vision Computing (24): 926–934, (2006).
[10] L. Pecora, T. Caroll, Synchronization in chaotic system, Physical Review Letters 64 (8) 821-824, (1990).
[11] R. Matthews, on the derivation of a chaotic encryption algorithm. Cryptology 8 (1): 29–41, (1989).
[12] S.G. Lian, J. Sun, Z. Wang, A block cipher based on a suitable use of chaotic standard map. Chaos, Solitons and Fractals. 26(1):117-129 (2005).
[13] Xiao-jun Tong, M.G. Cui, Image encryption with compound chaotic sequence ciphershifting. Image and Vision Computing 26 (6): 843–850, (2008).
[14] X.J. Tong, M. Cui, Image encryption scheme based on 3D baker with dynamical compound chaotic sequence cipher generator. Signal Processing 89: 480–491, (2009).
[15] X.J. Tong, The novel bilateral – Diffusion image encryption algorithm with dynamical compound chaos. The Journal of Systems and Software 85: 850– 858, (2012).
[16] K.W. Wong, B.S. Kwok, W.S. Law, A fast image encryption scheme based on chaotic standard map. Physics Letters A (372): 2645–2652, (2008).
[17] M.A.B. Younes, Image encryption using Block-Based transformation algorithm. Thesis of Doctor of philsophy, (2009).
[18] H.S. Kwok, W.K.S. Tang, A fast image encryption system based on chaotic maps with Finite precision representation. Chaos, Solitons and Fractals, 32: 1518-1529, (2007).
[19] Z. Guan, F. Huang, W. Guan, A chaos-based image encryption algorithm. Phys. Lett. A. 346: 153-157, (2005).