International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
www.ijset.com, Volume No.1, Issue No.4, pp : 24-27 01 Oct. 2012

A Review on Chaotic Map Based Cryptography

Shoaib Ansari, Prof. Neelesh Gupta, Prof.Sudhir Agrawal
Department of Electronics and Communication, T.I.E.I.T Bhopal (M.P.)
ershoaib.ansari@gmail.com, neelesh.9826@gmail.com,sudhiragraw@yahoo.com

Abstract: this paper presents a review of Image cryptography techniques based on chaotic maps. The chaotic cryptography is gaining more attention than others because of its lower mathematical complexity & better Security. It also avoids the data spreading hence reduces the transmission cost & delay. The digital image cryptography which is based on chaotic systems utilizes the discrete non-linear system dynamics generally called chaotic maps. Depending upon the type of system many types of chaotic maps are available. By combining them a large number of cryptographic techniques could be designed in this paper we are presenting a review of some of those techniques.

Keywords: chaotic map's, discrete non-linear system dynamics, symmetric cryptography.

1. Introduction

The cryptography term is used with the encryption of visual information. It is needed to protect the exposure of confidential or personal information especially in a system where the information is transferred through the open or insecure channel. The modern field of cryptography can be divided into several areas of study. But it can be broadly divided into two types 1) Symmetric-key cryptography and 2) Asymmetric-key cryptography. Generally the symmetric key cryptography is preferred for large data such as image and video because of its properties. The chaotic cryptography also falls in this category. Since in this paper we are only focusing on chaotic cryptography in rest of paper the considerations & designation will be specific to this method only. The chaotic cryptography techniques is generally made by combination of two operations called permutation (generally called Shuffling) & diffusion the both operations are repeatedly tautened till the sufficient encryption level is achieved. The quality of encryption is tested by its capability to defend different attacks like known plaintext attack, cipher text only attack, statistical attack, deferential attack, and brute-force attack, etc. The defending capability from each attack depends upon certain properties of the selected map and its configuration parameters. In this paper we are reviewing different techniques and configurations proposed recently.

1. Diffusion Techniques

Diffusion means spreading out the influence of a single plaintext digit over many ciphertext digits, so that the statistical structure of the plaintext becomes unclear.
Yaobin Mao and Guanrong Chen [1], an XOR plus modulo (mod) operation is inserted to each pixel in between every two adjacent rounds of the map used. In their proposal the one dimensional logistic map is used for generating the diffusion template

$$x(k+1) = 4x(k)[1 - x(k)] \quad \text{..... (1)}$$

The values generated by the map is initially floating and maintained from 0.2 to 0.5 then it is scaled and quantized for 8 bit data, which can directly used for XOR and Mod operations, the initial values of the map is taken from the key. Another approach based on W7 stream cipher is proposed by Alireza Jolfaei,Abdolrasoul Mirghadri [2]. The W7 stream cipher is a synchronous symmetric encryption designed for efficient hardware implementation at very high data rates. W7 algorithm supports key lengths of 128-bit and consists of a control and a function unit.

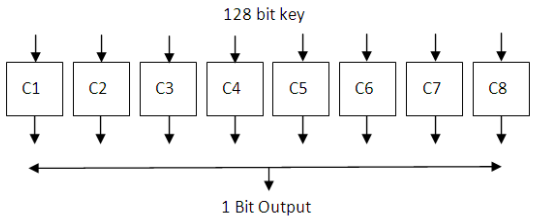

Figure 1: W7 key stream generator used with method describe in [2].

International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
www.ijset.com, Volume No.1, Issue No.4, pp : 24-27 01 Oct. 2012

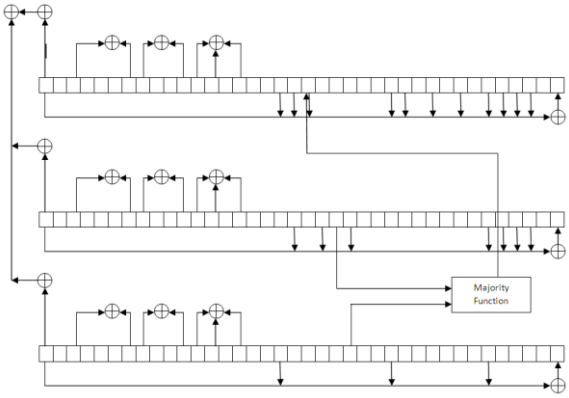

Figure 2: C2 block of W7 key stream generator used with method describe in [2].

The final diffusion is performed by

Shuffled_image ⊕ Keystream = Cipher_image

Musheer Ahmad and M. Shamsher Alam [3] used the 1D logistic map to generate the diffusion template which is similar to method proposed by [1] after generating the template XOR operation is performed for diffusion. The Xin Ma, Chong Fu, Wei-min Lei and Shuo Li [4] proposed Chebyshev map as cipher stream generator, which is described as follows:

$$x(n+1) = T_k(x_n) = \cos(k \cdot cos^{-1} x_n)$$
$$x_n \in [1, -1] \quad \ldots\ldots\ldots\ldots\ldots (2)$$

where k and x(n) are parameter and state value, respectively. If one chooses, k Є [2 ∞), the system is chaotic. The initial value x(0) and parameter k are used as the key for diffusion module. In [5] also used logistic map for diffusion template generation but they also added a coupling intensity factor which modifies the weight of generated pixels before XORing it can be represented as:

Shuffled_image⊕Keystream*f = Cipher_image.

where f is the coupling intensity factor. f Є (0 1].

2. Confusion Techniques

Confusion, on the other hand, means using transformations that complicate the dependence of the statistics of the ciphertext on the statistics of the plaintext.
Yaobin Mao and Guanrong Chen [1] used 2D to 3D conversion technique for providing the depth in confusion, in their proposal they firstly converted the 2D image in to 3D such as

$$W \times H = W_1 \times H_1 \times D_1$$
…… (3)

Where W and H are the width and height in pixels of original image and W_1, H_1 and D_1 are the new dimensions of 3D space. After this the 3D transformed image is shuffled by the 3D bakers map

$$B(x,y,z)\begin{cases} \left(2x, 2y, \frac{z}{4}\right) & 0 \le x < \frac{1}{2}, 0 \le y < \frac{1}{2} \\ \left(2x, 2y-1, \frac{z}{4}+\frac{1}{2}\right) & 0 \le x < \frac{1}{2}, \frac{1}{2} \le y < 1 \\ \left(2x-1, 2y, \frac{z}{4}+\frac{1}{4}\right) & \frac{1}{2} \le x < 1, 0 \le y < \frac{1}{2} \\ \left(2x-1, 2y-1, \frac{z}{4}+\frac{3}{4}\right) & \frac{1}{2} \le x < 1, \frac{1}{2} \le y < 1 \end{cases}$$
…… (4)

The equation (3) represents the 3D bakers map equation set.
In paper [2] the Hanon map based shuffling approach used. The Henon map is a prototypical two dimensional invertible iterated map represented by the state equations with a chaotic attractor and is a simplified model of the Poincare map for the Lorenz equation proposed by Henon in 1976. The two-dimensional Henon map is defined as follows:

$$x_{n+1} = 1 + y_n - \alpha x_n^2$$
$$y_{n+1} = \beta x_n$$
…… (5)

with initial point (x0 , y0). The pair (x, y) is the two-dimensional state of the system. When α = 1.4 and β = 0.3, the system is in chaotic state. To decrease adjacent pixels correlation the permutation map is applied in two different directions: vertical and horizontal.
Musheer Ahmad and M. Shamsher Alam [3] presented a Cat map & block based shuffling algorithm, in block based algorithm the image is firstly divided into the smaller blocks then each block is independently shuffled after that the blocks are shuffled, since the Cat map having a property of cyclic repetition they used a 2D logistic map to change the Cat maps parameters after each iteration.
The two-dimensional coupled Logistic map is described as follows:

$$x_{n+1} = \mu_1 \mu_2 (1 - x_n) + \gamma_1 y_n^2$$
$$y_{n+1} = \mu_1 y_n (1 - y_n) + \gamma_2 (x_n^2 + x_n y_n)$$
…….. (6)

Three quadratic coupling terms are introduced to strengthen the complexity of 2D Logistic map. This system is chaotic when $2.75 < \mu_1 \leq 3.4$, $2.7 < \mu_2 \leq 3.45$, $0.15 < \gamma_1 \leq 0.21$ and $0.13 < \gamma_2 \leq 0.15$ and generate chaotic sequences x, y in the interval (0, 1). Now the used Cat map is first presented by V.I. Arnold in the research of ergodic theory. Let the coordinates of positions of pixels in an image are P = {(x, y) | x, y = 1, 2, 3, . . ., N}, a 2D Cat map with two control parameters is as follows:

$$x' = (x + ay) mod(N)$$
$$y' = (bx + (ab + 1)y) mod(N)$$

…… (7)

Where, a, b are control parameters which are positive integers and (x', y') is the new position of the original pixel position (x, y) of N x N plain-image when Cat map is applied once to the original. A new approach based on pixel bits permutation is proposed in [4] where each pixel is taken as a block of eight bits and then these bits are shuffled they called it the bit level permutation although for shuffling they also really on Cat Map. To implement bit-level permutation, each bit-plane of an image is shuffled separately by using Arnold Cat map with different control parameters, and then we can get the new G(x, y) give by

$$G'(x,y) = b'(7)b'(6)b'(5) \ldots b'(0)$$

where b′(n) (n∈[0-7]) are the bits moved from other positions on the bit-plane. Thus an effective diffusion mechanism is introduced. Ruisong Ye, Wei Zhou [5] proposed the Tent Map based permutation technique. The 2D tent map $T_{a,b} : [0,1]^2 \rightarrow [0,1]^2$ is given by:

$$T_{a,b}(x)\begin{cases} \begin{pmatrix} 1/a & 0 \\ 0 & 1/b \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}, (x,y) \in [0,a] \times [0,b], \\ \begin{pmatrix} \frac{1}{a} & 0 \\ 0 & \frac{1}{1-b} \end{pmatrix}\begin{pmatrix} x \\ 1-y \end{pmatrix}, (x,y) \in [0,a] \times [b,1], \\ \begin{pmatrix} \frac{1}{1-a} & 0 \\ 0 & \frac{1}{b} \end{pmatrix}\begin{pmatrix} 1-x \\ y \end{pmatrix}, (x,y) \in [a,1] \times [0,b], \\ \begin{pmatrix} \frac{1}{1-a} & 0 \\ 0 & \frac{1}{1-b} \end{pmatrix}\begin{pmatrix} 1-x \\ 1-y \end{pmatrix}, (x,y) \in [a,1] \times [b,1], \end{cases}$$

…… (8)

where (0 1) a b, ∈ (0,1),the 2D tent map is chaotic on $[0\ 1]^2$.

3. Key-space Analysis

A good image encryption algorithm should be sensitive to the cipher key, and the keyspace should be large enough to make brute-force attacks infeasible.

Yaobin Mao and Guanrong Chen [1] method having a key length of 128 bits & it's very sensitive to key as the result shows that a single bit change in key causes 99.59% difference between decoded image. The method [2] has a 128-bit key, the key space size is 2^{128}. Furthermore, if we consider the two seed points of shuffler as part of the key, the key space size will be even larger. This means if the precision is 10^{-14}, then the key space can be 2^{128}x 10^{14} = 2^{221} = 3.6x10^{66}. Apparently, the key space is large enough to resist all kinds of brute-force attacks. The Algorithm described in [3] used eight initial conditions of chaotic map in the algorithm and the initial conditions for x_0, y_0, z_0, μ_1, μ_2, γ_1, γ_2 and λ can be used as secret keys of encryption and decryption. In this case, the precision is 10^{-14}, the key space size is $(10^{14})^8$ i.e. 10^{112}, which is extensively large enough to resist the exhaustive attack. The algorithm proposed in [4] is a 153-bits encryption scheme, while the key space of the most well-known secure encryption algorithm AES is 128-bits. So it can be seen that the proposed chaotic image encryption scheme is good at resisting brute-force attack. The result shows that the single bit change in key causes 99.63% difference between decoded images. In [5] the key space is up to $(2^{52})^7$ = 2^{364}. Such a large key space can efficiently prevent opponent's brute-force attack.

4. Conclusion

After studying lots of work on chaos based cryptography it can be concluded that the architecture of all proposed work is almost same and the difference remains in the types of chaotic maps used, the way they are configured and how many variables can be created to control the characteristics of the map which reflects the robustness of the system on the other hand to speed up the process some simplifications in the mathematical process can be adapted.

References

[1] Yaobin Mao and Guanrong Chen "A Novel Fast Image Encryption Scheme Based on 3d Chaotic Baker Maps" International Journal Of Bifurcation and Chaos, Vol. 14, No. 10 (2004) 3613–3624.

[2] Alireza Jolfaei,Abdolrasoul Mirghadri "An Image Encryption Approach Using Chaos And Stream Cipher" Journal of Theoretical And Applied Information Technology 2010.

[3] Musheer Ahmad and M. Shamsher Alam "A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping" International Journal on Computer Science and Engineering, Vol.2(1), 2009, 46-50.

[4] Xin Ma, Chong Fu, Wei-min Lei, Shuo Li "A Novel Chaos-based Image Encryption Scheme with an Improved Permutation Process" International Journal of Advancements in Computing Technology Volume 3, Number 5, June 2011.

[5] Ruisong Ye, Wei Zhou "An Image Encryption Scheme Based on 2D Tent Map and Coupled Map Lattice" International Journal of Information and Communication Technology Research Volume 1 No. 8, December 2011.

[6]Zhang, G. J., Liu, Q. "A Novel Image Encryption Method Based on Total Shuffling scheme" Optics Communications, 284, pp. 2775--2780 (2011).

[7] Feng Huang, Yong Feng And Xinghuo Yu"A Symmetric Image Encryption Scheme Based On A Simple Novel Two-Dimensional Map" International Journal of Innovative Computing, Volume 3, Number 6(B), December 2007.