GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

A REVIEW ON IMAGE ENCRYPTION USING CHAOS

Prachi S. Mankar[*1] **and Prof.S.K.Nanda**[2]
[*1]Department of Electronics and Telecommunication Amravati university
[2]HOD, Department of Electronics and Telecommunication Amravati university

ABSTRACT

These paper presents the novel idea about the various image ecryption processes available specifically the encryption of the image by using chaos theory .In the recent age of communication allows us to transfer any of the information over the longer distance.but it also involves the factors of security. This paper is the overview of the chaos theories and the encryption processes available for the transmission of image over a secured media.

Keywords- *Chaotic maps, Image Encryption, Pixel Shuffling, Chaotic theory*

I. INTRODUCTION

A large amount of digital data is being stored on different media and exchanged on the networks. This data contains private and the confidential information. For this the techniques are required to provide the confidentiality, authenticity, integrity. Recently the technologies based on the chaos are preferred over the other technologies for the transmission of the images or data over the distances for preventing its confidentiality and integrity.. The chaos is the word derived from Greek which means the unpredictability and is also defined as the study of complicated dynamic system. Its behavior changes with the change n the initial condition or change in the initial values of the parameters (i.e . key in case of encryption techniques. In last few years the digital information sharing over the internet is the fastest development. The people keeps exchanching the secured and confidential data over the internet on the open network. So while sending the images the question arises that is of the security, where the sent information follows the cryptographic principle or not. Whether it follows integrity,confidentiality or authenticity. Some times there may be the possibility of brute force attack or the possibility of intruder to introduce any data and thus loss the integrity. This will not cause much problem in the day to day life. But this will surely affect in case of military applications. To avoid the attacks and to maintain the confidentiality of the transmitted data it is necessary to send A large amount of digital data is being stored on different media and exchanged on the networks. This data contains private and the confidential information. For this the techniques are required to provide the confidentiality, authenticity, integrity. Recently the technologies based on the chaos are preferred over the other technologies for the transmission of the images or data over the distances for preventing its confidentiality and integrity.. The chaos is the word derived from Greek which means the unpredictability and is also defined as the study of complicated dynamic system. Its behavior changes with the change n the initial condition or change in the initial values of the parameters (i.e . key in case of encryption techniques. In last few years the digital information sharing over the internet is the fastest development. The people keeps exchanching the secured and confidential data over the internet on the open network. So while sending the images the question arises that is of the security, where the sent information follows the cryptographic principle or not. Whether it follows integrity, confidentiality or authenticity. Sometimes there may be the possibility of brute force attack or the possibility of intruder to introduce any data and thus loss the integrity. This will not cause much problem in the day to day life. But this will surely affect in case of military applications. To avoid the attacks and to maintain the confidentiality of the transmitted data it is necessary to send into the coded form called as encrypted form and the process is called as encryption. In the corresponding paper we are encrypting the image into the complete form of noise .for converting the image into the form of noise we are using the chaotic map and chaotic theories. This paper is the review of different encryption process and the chaotic maps

There are different encryption schemes such as Advanced encryption standards (AES) and Data encryption standards (DES) which are the best suited approach for the text encryption. But to encrypt the image this are not suitable. Because the image is the combination of pixels and consist of bulk amount of data. So different encryption techniques need to be used.

II. LITERATURE REVIEW

To protect the image from unauthorized access different types of algorithms were proposed. They are described in the following section.

1)Image Encryption Using Block-Based Transformation Algorithm, 2008

The method of block based image transformation has been invented and proposed by Mohammad Ali Bani Younes and Aman. In these method the most popular algorithm i.e. Blowfish is used for the process of encryption and decryption. The Blowfish algorithm is used with the image transformation algorithm. The plain image or the original image is divided into the blocks. These blocks are then rearranged and rearranged blocks are transformed by using the transformation algorithm.the image is called as transformed image that transformed is encrypted by using the Blowfish algorithm. From all these the Mohammad and Aman showed that there is very less correlation between the pain and cipher image.

2)An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption, 2008

The new permutation technique based on the combination of image permutation and well known encryption algorithm called RijnDael has introduced by Mohammad Ali Bani Younes and Aman Jantan . The original image was divided into 4 pixels × 4pixels blocks which were rearranged into a permuted image using a permutation process, and then the generated image was encrypted using the RijnDael algorithm.

3)Digital image encryption algorithm based on chaos and improved DES, 2009

The chaotic encryption has reasearched by Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan and Dai Wei-di , They also performed DES encryption and a combination of image encryption algorithm. In this technique firstly, new encryption scheme uses the logistic chaos sequencer to make the pseudorandom sequence, carries on the RGB with this sequence to the image chaotically, then makes double time encryptions with improvement DES. Their result show high starting value sensitivity, and high security and the encryption speed.

4)A Digital Digital Image Encryption Algorithm Based Composition of Two Chaotic Logistic Maps, 2010

The efficient Chaos- based stream cipher, Composing two chaotic logistic maps and a large enough external secret key for image encryption has been introduced by Ismail Amar Ismail, Mohammed Amin, and Hossam Diab. In this image encryption scheme two chaotic logistic maps developed for the confusion between the cipher image and the plain image and then the secrete key of 104 bits is used. Again to increase the security and robusting the attack, After encrypting the each pixel of plain image the secrete key is modified.

5)Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on it, 2011

Singh and Kaur has compared the logistic ,Ikeda,Henon ,Cross chaotic maps. After that the effect of noise is observed on the image. They used the encryption algorithm to convert the plain image into the cipher image. Then they apply the noise on the encrypted image and then the Image(with noise) is decrypted by using the decryption algorithm to obtain the original image. So it shows the best result by using the cross chaotic map.

III. METHODS

As image is the combination of pixels so the advanced encryption standard (AES) or data encryption standard(DES) can not be use for the encryption of the image. As image consists of pixels hence it has the large data compared to text. Fig.1 shows the image before and after the encryption .

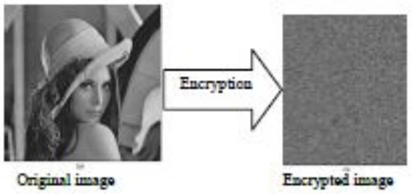

Fig 1. Image Encryption

A.Chaotic Maps

The non linear behavior of the dynamic system can be explained by using chaos theory based on the sensitivity of the initial condition. The most important properties of the chaotic systems are mixing property and the sensitivity to the initial condition. The 1D chaotic map is created to produce the chaotic sequence and used to control the encryption process. the chaotic system can be investigated and generated by using the different chaotic maps. There are very different kinds of chaotic maps.

b.Logistic Map

This is the second form the chaotic map.The most simplest and well studied example of a 1D map that exhibits the complicated behavior from interval [0,1]bin to [0,1] can be explained by logistic map. The logistic map can be parameterized by μ. And given by the following equation.

$g_{\mu}(x) = \mu * (x)$-------(1)

The state evolution is as follows.

$x(n+1)=\mu*x(n)*(1-x(n))$-------- (2)

Where $0 \leq \mu \leq 4$. This map constitutes a discrete-time dynamical system in the sense that the map g_{μ} :[0,1] ® [0,1] generates a semi-group through the operation of composition of functions. In the this map, μ is varied from 0 to 4, a period-doubling bifurcation occurs.

C. Tent Map

This the third form of the chaotic map.Tent map is the iterated function in the mathematics and that is into the form of the shape of the tent and forms the dynamic system which is discrete time in nature. The point Xn on the real line and maps it into the another point.

$$x_{n+1} = \begin{cases} \mu x_n & \text{for } x_n < \frac{1}{2} \\ \mu(1 - x_n) & \text{for } \frac{1}{2} \leq x_n. \end{cases} \text{------(3)}$$

Where μ is a positive real constant.

The tent map explains the range of the dynamical behavior of the system depending on the value of μ.

D. Quadratic Map

This is the fourth form of chaotic map. The most complicated form of the chaotic map is Quadratic map. The analysis of the map is given by the following equation.

$X_{n+1}=f_c(x_n)=x_n^{2}+c$ ------------------(4)

For an analytic map the point f '(xc) = 0 is called critical points. X c= 0 is the only critical point of the quadratic map. Quadratic map has theb only critical point Xc = 0.So a fixed point is stable (attracting), super stable, repelling, indifferent (neutral)according as its multiplier satisfies |m| < 1, |m| = 0, |m| > 1 or |m| = 1. The second fixed point is always repelling. For |x| > x2 iterations go to infinity. For |x| < x2 they go to the attracting fixed point x1. This interval is the basis of attraction of the point.

E. Bernoulli Map

This is the fifth form of the chaotic map. It is also called as the 2x mod 1 map. And is defined as

$$f(x) = \begin{Bmatrix} 2x, & 0 \leq x < 0.5 \\ 2x\text{-}1, & 0.5 \leq x < 1 \end{Bmatrix} \text{------(5)}$$

The Bernoulli process can be defined as the discrete time stochastic process which consists of a finite and infinite sequence of random variables the random variables are particularly independent random variables X1,X2,X3,….. such that for Xi the value of the i is either 0 or 1 for each i.p is the probability that Xi=1, for all the value of i. the future trials from the any given time can also be the Bernoulli process which is independent on the past trials.

F. Henon Map

The henon map is the two dimensional map which is invertible and iterated map. The state equation is use for the representation of henon map. The state equation in combination with the chaotic attractor is used. The method of generating the pseudo- random sequences can be used to propose the Henon map. The Henon map can be defined as follows:

$$X_{n+1}=1+Y_{n}- \alpha X_{n}{}^{2}\text{------}(6)$$
$$Y_{n+1}=\beta X_{n}\text{-------------}(7)$$

($x0$, $y0$) is the initial point. The pair (x, y) is called as two

dimensional state of the system. The chaotic state of the system is defined for the values of α =1.4 and β = 0.3. henon showed that if the initial point is in the area S defined by the points (-1.33, 0.42), (1.32,0.133), (1.245, -0.14) and (-1.06, -0.5), then all the points (xi, yi) for $i \geq 1$ also lies in the area S. The Henon map contains a chaotic attractor which is also called as the strange attractor due its property of converging all the points in area S attracted towards the attractor and remains there for the subsequent iterations.

G. Stream Cipher

The stream ciphers are used along with the chaotic map for encrypting the image. And hence to increase the security of the data or image or text. The stream cipher is the symmetric type of encryption algorithm. This encryption process takes the binary digits of plain image sequentially (one by one)and encrypts them by using an encryption transformation which varies with time. In case of stream cipher mainly the XOR operation is used. The plain image bits are XORed with the key stream and the cipher text is obtained. This is the symmetric process..W7 stream cipher is the type of stream ciphers. Fig. 2 shows W7 key stream generator and Fig. 3 shows the detailed design of the block C2.

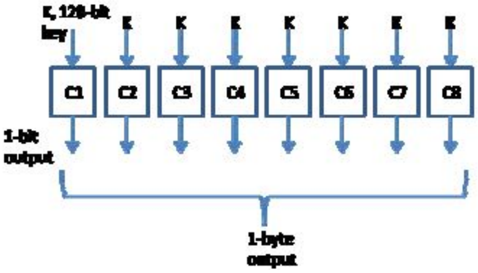

Fig 2. W7 key stream generator

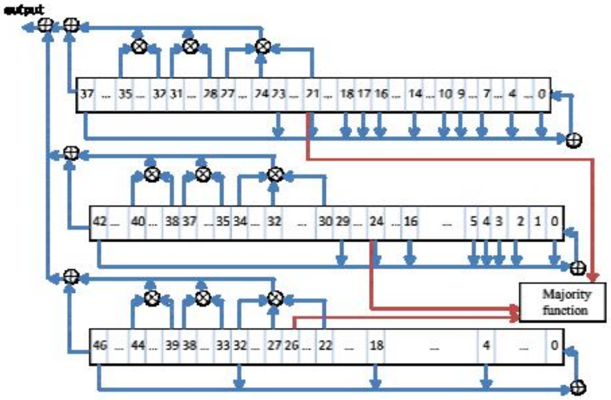

Fig 3. Diagram of C2 Block in W7 stream cipher

IV. CONCLUSION

Compared with the other chaotic schemes and maps the Henon map gives the best suited result for the secured transmission and for the encryption process. The performed security analysis shows that the method can resistmany forms of cryptanalysis.The Henon map converts the simple plaintext image into the ciphertext which is the complete noise.the ciphertext image has the complete random like structure. There is no correlation between the ciphertext

ISSN 2348 – 8034
Impact Factor- 3.155

and plaintext so its become difficult to analyse the plaintext from ciphertext and vice versa. The best suited result is obtained by using the henon map and DES encryption algorithm.

REFERENCES

1. *G.A.Sathishkumar, Dr.K.Bhoopathy bagan,Dr.N.Sriraam," "Image Encryption based on Diffusion and Multiple Chaotic Maps" International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, March 2011.*

2. *Minal Govind Avasare, Vishakha Vivek Kelkar, "Image Encryption using Chaos Theory", International Conference on Communication, Information & Computing Technology (ICCICT), Jan. 16-17, Mumbai, India,2015.*

3. *Danial Roohbakhsh, Mahdi.Yaghoobi, "Color Image Encryption using Hyper Chaos Chen", International Journal of Computer Applications (0975 – 8887) Volume 110 – No. 4, January 2015 .*

4. *Alireza Jolfaei, Abdolrasoul Mirghadri, "An Image Encryption approach using chaos and Stream cipher", journal of theoretical and applied information technology***.**

5. *William stallings, ―Cryptography and Network Security: Principles & Practices‖, second edition.*