RESEARCH ARTICLE OPEN ACCESS

Review: Image Encryption Using Chaos Based algorithms

Er. Ankita Gaur*, Er. Maneesha Gupta**
*(M.tech scholar, Electronics and communication Engineering department, SKIET, kurukshetra)
** (Lecturer, Electronics and communication Engineering Department, SKIET, Kurukshetra)

ABSTRACT
Due to the development in the field of network technology and multimedia applications, every minute thousands of messages which can be text, images, audios, videos are created and transmitted over wireless network. Improper delivery of the message may leads to the leakage of important information. So encryption is used to provide security. In last few years, variety of image encryption algorithms based on chaotic system has been proposed to protect image from unauthorized access. 1-D chaotic system using logistic maps has weak security, small key space and due to the floating of pixel values, some data lose occurs and proper decryption of image becomes impossible. In this paper different chaotic maps such as Arnold cat map, sine map, logistic map, tent map have been studied.

***Keywords* –** Arnold cat map, Encryption, logistic map, sine map, tent map, 1-D chaotic system.

I. Introduction

Protection of multimedia contents from unauthorized access is necessary nowadays. With the help of cryptography readable form of message is converted to the non readable form. And reverse of cryptography in which non readable form of message is converted back to readable form, is called cryptanalysis. The combination of these two techniques is referred as Cryptology.

Communication in human language referred as Plain Text which can be easily understandable by anyone else. In order to provide security plain text is coded with suitable encryption shames and the codified message is referred as cipher text. Fig.1 represents the block diagram of encryption, where K_e is the encryption key.

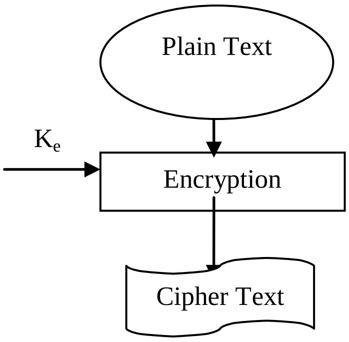

figure 1:block diagram of encryption

Encryption key K_e is implemented on plain text to convert it to cipher text.

Fig. 2 represents the basic decryption technique, where K_d is the decryption key. Similarly K_d is implemented on cipher text to convert back it to the plain text.

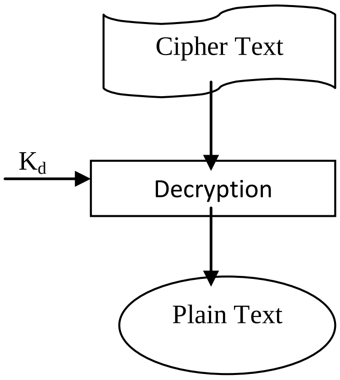

figure 2: block diagram of decryption

Encryption techniques can be classified on the basis of key, structure of algorithms and percentage of encrypted data.

On the basis of key encryption can be symmetric encryption and asymmetric encryption, on the basis of structure encryption can be block cipher and stream cipher. And on the basis of basis of percentage of encrypted data encryption can be full encryption and partial encryption.

II. Literature Review

Varsha S.Nemade et.al discussed that text encryption algorithms which have been already developed are not suitable for the image encryption, because image containing large amount of data means it contains number of pixels. Image encryption techniques scrambled the pixels of the image and decrease the correlation among the pixels, so that we will get lower correlation among the pixel and get the encrypted image. In this paper survey of different image encryption techniques has been discussed

Jolly Shah et.al stated that image applications have been increasing in recent years. Encryption is used to provide the security needed for image applications. In this paper, we classify various image encryption schemes and analyze them with respect to various parameters like tunability, visual degradation, compression friendliness, format compliance, encryption ratio, speed, and cryptographic security.

Haojiang Gao et.al discussed that recent researches of image encryption algorithms based on chaotic systems, but the drawbacks of small key space and weak security in one-dimensional chaotic cryptosystems are obvious. This paper presents a new nonlinear chaotic algorithm (NCA) which uses power function and tangent function instead of linear function. Its structural parameters are obtained by experimental analysis. And an image encryption algorithm in a one-time-one password system is designed. The experimental results demonstrate that the image encryption algorithm based on NCA shows advantages of large key space and high-level security, while maintaining acceptable efficiency. Compared with some general encryption algorithms such as DES, the encryption algorithm is more secure.

Yicong Zhou et.al introduced a new parametric switching chaotic system (PSCS) and its corresponding transforms for image encryption. The proposed PSCS has a simple structure and integrates the Logistic, Sine and Tent maps into one single system. The PSCS shows more general properties, including the Sine and Tent maps as special instances. It has complex chaotic behaviors. A novel image encryption algorithm is introduced using the proposed PSCS and its transforms. Simulation results and security analysis are given to demonstrate that the proposed algorithm can encrypt different types of images with a high level of security.

III. Methodology

Text encryption algorithms such as Advanced Encryption Standard (AES) or Data Encryption Standard (DES) cannot be used for image encryption because image is made up of pixels or in other words image has large data as compared to text. Image encryption can be done by chaos theory. Fig.3 shows the image before and after the encryption.

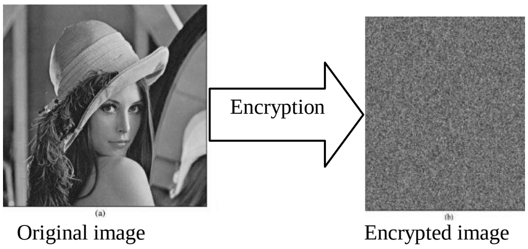

figure 3: image encryption

3.1 Chaotic system: Chaotic system can be considered as source of randomness and chaos is randomness of a deterministic dynamical system. Mathematically A chaotic map can be defined as

$X_{n+1}= f(X_n)$ …………………………….. ……..(1)

Where $0<X_n<1$ and n=0, 1, 2…

Chaotic sequence can be used as random number sequence and spread spectrum sequence. The chaotic systems are characterized by the non linear and unpredictable. They appear to have irregular order but infect there is a sense of order. Chaotic systems are sensitive to initial conditions, small change in starting point can cause different outcomes. Chaos has many applications in modulation, compression, and encryption. In image encryption, 1-D chaotic system using logistic maps has simplicity and high efficiency but it has weak security and small key space. Different Chaotic maps can be used for this purpose. Generally in chaos based algorithm, pixels of image are scrambled and correlation among pixels is decreased to get encrypted image. Figure 2 represent the basic image encryption flow chart of chaos based algorithms. Where k and iv are the key and initial vector generated by chaotic system.

3.1.1 Arnold cat map: it was demonstrated by Vladimir Arnold in 1960s by using an image of a cat. Arnold cat map uses the concept of linear algebra to change the position of pixels of original image. Original image is divided into blocks and then Arnold transformation is done.

Let X is a vector, $X=\begin{bmatrix}x\\y\end{bmatrix}$, then Arnold cat map

transformation is, $\Gamma\textbf{:} \begin{bmatrix}x\\y\end{bmatrix} \to \begin{bmatrix}1 & p\\ q & 1+q\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix} \; mod\ n$

Some conditions such as p and q are positive integers and

$$\begin{vmatrix}1 & p\\ q & 1+q\end{vmatrix}=1$$

This makes it area-preserving. Original image can be shuffled by applying Arnold map operation iteratively. But shuffled image can return to original form after several iterations.

3.1.2 Logistic map: 1-D logistic map was proposed by RM may. This map is simplest non linear chaotic system which can be defined as

$z_{n+1}= \lambda\, z_n(1-z_n)$……………………………………..(2)

Where z_0 is initial condition, n is number of iterations and λ is system parameter.

For 3.57 < λ < 4 map is considered as chaotic .And z $_{n+1}$ belong to (0, 1) for all n. equation 1 is used to encrypt the shuffled pixels.

3.1.3 Sine map: sine map is defined as

X $_{n+1}$=a $x_n^{\,2}$ sin(π x_n) …………………………..(3)

when x_0 = 0.7 and a=2.3, equation 2 has the simplified form . for the interval (0,1) it generates chaotic sequence .

3.1.4 Tent map**:** tent map resembles the logistic map. It generates chaotic sequences in (0,1) assuming the following equation

$$Xn+1=\begin{cases}\mu Xn, & Xn<1/2\\ \mu(1-Xn), & Xn\geq 1/2\end{cases}$$

Where µ is a positive number and depending on its value tent map exhibit dynamic behavior ranging from predictable to chaotic.

3.1.5 Circle map: it is defined as

$X_{n+1}= X_n + d - (c/2\pi)\sin(2\pi X_n) \bmod(1)$………(4)

Where *d* = 0.2, *c* = 0.5, and *x*0 € [0,1] generates

Chaotic sequence in [0,1].

IV. Conclusion

In order to provide security to the image, cryptography is used which converts an image into another form (non readable form). Chaotic systems have many applications in image processing such as image compression and image encryption. Combination of chaos theory with cryptography may provide security of high level. Chaotic maps like Arnold cat map, tent map, sine map, logistic map are used in image encryption. Two or more maps can also be used in combination. Arnold cat map cannot be efficient alone for image encryption so it can be used with other maps for efficient encryption.

REFERENCES

[1] Ljupcˇo Kocarev, Chaos-Based Cryptography:A Brief Overview, *IEEE,* 1531-636X/10/$10.00©2001,

[2] Shiguo Lian, Jinsheng Sun, Zhiquan Wang, Security Analysis of A Chaos-based Image Encryption Algorithm, The paper was accepted by Phisica A, Elsevier Science, 2005.

[3] Haojiang Gao , Yisheng Zhang, Shuyun Liang, Dequn Li, A new chaotic algorithm for image encryption, ©2005 Published by Elsevier Ltd.

[4] Mohammad Ali Bani Younes and Aman Jantan, Image Encryption Using Block-Based Transformation Algorithm, *International Journal of Computer Science*, 35:1, IJCS_35_1_03, Issue 19, February 2008

[5] Alireza Jolfaei and Abdolrasoul Mirghadri, Survey: Image Encryption Using Salsa20, *International Journal of Computer Science*, *Vol. 7*, Issue 5, September 2010 ,*ISSN (Online): 1694-0814*

[6] Mao-Yu Huang et .al, Image Encryption Algorithm Based on Chaotic Maps, 978-1-4244-7640-4/10/$26.00 ©2010 *IEEE* .

[7] Jolly Shah and Dr. Vikas Saxena, Performance Study on Image Encryption Schemes, *International Journal of Computer Science*, *Vol. 8*, Issue 4, No 1, July 2011

[8] Yicong Zhou, Long Bao, C. L. Philip Chen, Image Encryption Using a New Parametric Switching Chaotic System, ©2011 Published by Elsevier Ltd.

[9] Mintu Philip et.al, Survey: Image Encryption using Chaotic Cryptography Schemes, *International Journal of Computer Applications*, Special Issue on Computational Science - New Dimensions & Perspectives, NCCSE, 2011

[10] Varsha S.Nemade and R.B.Wagh, Review of different image encryption techniques, *Proc. of National Conference on Emerging Trends in Computer Technology (NCETCT-2012)* Held at R.C.Patel Institute of Technology, Shirpur, Dist. Dhule,Maharashtra,India. April 21, 2012

[11] Ruisong Ye and Wenping Yu, An Image Hiding Scheme Using 3D Sawtooth Map and Discrete Wavelet Transform, I.J. Image, Graphics and Signal Processing, 2012, 6, 52-60

[12] Pankesh et al., Image Encryption Using Pixel Shuffling, *International Journal of Advanced Research in Computer Science and Software Engineering 2 (12)*, December - 2012, pp. 279-282 © 2012, All Rights Reserved Page | 279 *Volume 2*, Issue 12, December 2012 *ISSN: 2277 128X*

[13] Shubhangini P.Nichat, Prof.Mrs.S.S.Sikchi, Image Encryption using Hybrid Genetic Algorithm, *International Journal of*

Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 1, January 2013 *ISSN: 2277 128X*.

[14] Rajinder Kaur1, Er.Kanwalprit Singh, Image Encryption Techniques: A Selected Review, *IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727,Volume 9,* Issue 6 (Mar. - Apr. 2013), PP 80-83

[15] Mohammed A. Shreef and Haider K. Hoomod, Image Encryption Using Lagrange-Least Squares Interpolation, *International Journal of Advanced Computer Science andInformation Technology ,Vol. 2,* No. 4, 2013, Page: 35-55, *ISSN: 2296-1739*

[16] Pia Singh, Prof. Karamjeet Singh, Image Encryption And Decryption Using Blowfish Algorithm In Matlab, *International Journal of Scientific & Engineering Research, Volume 4,* Issue 7, July-2013.

[17] Vani et al., *International Journal of Advanced Research in Computer Science and Software Engineering 3(9),* September - 2013, pp. 1210-1215

[18] Prachi Junwale , R. Manasa Annapurna, G.Sobha,A Review on Image Encryption Technique based on Hyper Image Encryption Algorithm, *International Journal of Advanced Research in Computer Science and Software Engineering 3(11),* November - 2013, pp. 614-618.

[19] Sukhjeevan Kaur et al , A Review of ImageEncryption Schemes Based on the Chaotic Map , *International Journal of Computer Technology & Applications,Vol 5 (1)*,PP144-149, 2014, *ISSN:2229-6093*