Review on Image Encryption Using Chaotic Methods

[1]Nazeema H, [2]Ashok Babu, [3]Jayaram. P

[1]Mtech Student, School of Computer Science, M G University, Kottayam, Kerala, India
[2] Assistant Professor, School of Computer Science, M G University, Kottayam, Kerala, India
[3]Principal Engineer, CDAC, Kochi, Kerala, India.

Abstract : Security is a major concern of the public network during information exchange. Image encryption has gained more attention due to the vast improvements in computation speed, storage capacity and bandwidth. So the fundamental issue of image security has become a major concern. This paper discusses the general study of various image encryption / decryption techniques and performance factors such as entropy, correlation, execution time and histogram. Also given a model of image encryption / decryption technique based on chaotic schemes this can enhance security and efficiency of image encryption.

***IndexTerms*-- cryptography, image encryption, security, chaos theory, confusion and diffusion, chaotic methods.**

I. INTRODUCTION

Cryptography [1] is an important aspect when we are dealing with network security. Crypto or cryptography means secret or hidden. Cryptography is the science of secret writing with the purpose of keeping data confidential. Cryptanalysis, on the other hand, is the science or sometimes art that breaks down cryptosystems. These two terms are a subset of what we call cryptology. In today's corporate world that requires access to information in a short amount of time with the aim of making the enterprise run smoothly and efficiently, it is very important to provide the right people with the right information at the right time. The information actually received should be the same information has been sent. Suppose a person creates an important file in a website's workplace and when he sends, it passes through an unsafe channel. There are chances someone in the middle retrieves and modify the message and then transfers to the final destination. This can lead to many undesirable side effects and result in huge losses for the company financially. Cryptography plays a very important role in keeping the message secure during the data in transit. This ensures that the message sent from one end remains confidential and is received by the desired receiver only, in the other end. Cryptography converts the original message to an unreadable format and sends the message over an unsafe channel. Illegal people try to break the message that they can't read, but it's hard to do. Only an authorized person has the ability to convert an unreadable message into a readable one.

In recent years, a good range of image cryptography schemes [2] supported by chaotic maps are planned. Some well-known chaotic maps, like Arnold cat map, logistic map, chaotic skew tent map, hen's chaotic map etc., are successfully used within the cryptosystems. Chaotic maps show quick and delicate response towards initial conditions and control parameters. Therefore most of the cryptosystems directly use the initial conditions /parameters of chaotic maps as the secret key. During in this paper, the present analysis efforts in image cryptography techniques supported by chaotic schemes are discussed.

1.1 IMAGE ENCRIPTION

Images [3] have an important role in many applications, including remote sensing, biomedical, and video conferencing. Importance of digital image processing methods comes in major application areas viz. improving image information for human interpretation; Image data processing for machine storage and transmission to understand the machine. Two major issues need to be resolved when we want to exchange a picture. The image should be included in the bandwidth cover and other pictures also should be taken safely. Image compression and image encryption are two basic image processing techniques for efficient use of bandwidth and security.

Image encryption means turning the image into unreadable format. It can be changed according to image pixels (position and value) to protect information. There may be many techniques for encrypting an image that includes image encryption or image clamping, but basically an image is described by its pixel-level. It is the value of the pixels or the location of the original array. The image is encrypted in the following steps to change its positions. This process may include scrambling, chaotic mapping, and inversion. This procedure can be followed depending on the sequence of this algorithm to follow the encryption. If there are pixels in the image, it may be vulnerable to attacked by a crypto analyst's attacks, but security can be increased by using a variable length key. Here the correlation between the pixels decreases.

1.2 CHAOS THEORY

The Chaotic System [4] exhibits one of the most legitimate features of cryptography applications that have been developed in recent years, like image ciphering, data hiding, watermarking, and steganography in digital multimedia applications. In 1960, Edward Lawrence introduced the study of chaotic dynamics. The development of chaos theory has been demonstrated by its ability to generate high levels of confusion and diffusion [5] in the alternative and systematic network.

Chaotic dynamical system is any settled system which is very irregular and highly responsive to initial conditions. They are identical to noisy systems since both are uncertain in nature. Cryptography has uses for chaotic systems [6] because they are uncertain, irregular and high sensitive in nature. These characteristics of chaotic systems make it useful for encryption and also allow a basis for decryption. The key dissimilarity between chaos maps and chaos cryptography is that the former is defined by real numbers and the latter is finite sets. Each chaos maps got their own specifications and encryption key.

The basic characteristics of chaotic maps are Ergodicity, broadband spectrum and high sensitivity has attracted the attention of researchers who+ use high security encryption algorithms to incorporate early communications into modern communication. Over the past few years, we have learned many tricky encryption algorithms.

1.3 CHAOS BASED IMAGE ENCRYPTION

Most of the data encryption techniques are based on chaotic maps because they are simple to interpret and also broadly accepted in many applications. There are two stages in the chaos based image cryptosystem [7] viz. the confusion stage and the diffusion stage. Fig 1 describes the block diagram of the architecture.

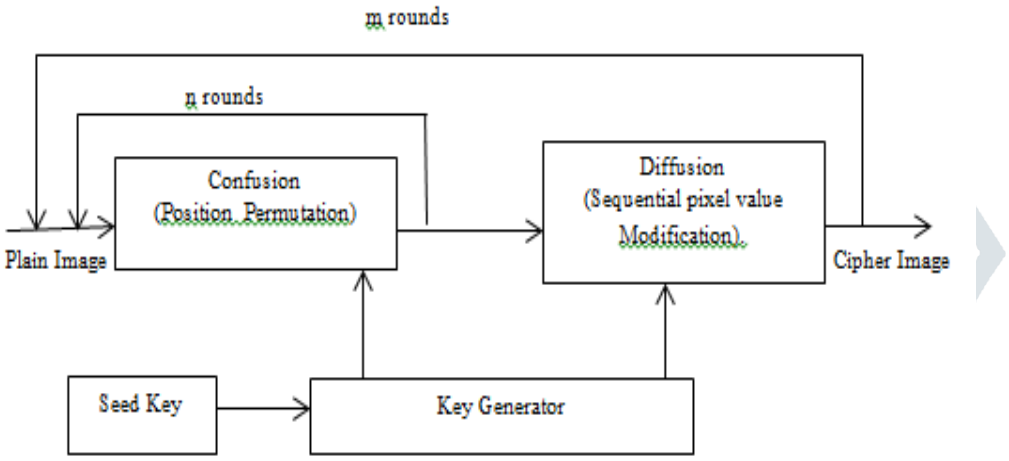

Fig. 1. Chaos based image encryption architecture

In confusion stage, positions of an image's pixels are crawled without damaging its values. This is called pixel permutation, which make the image unrecognizable. However, there are good chances of vulnerability in this process, as it can be broken by any attack. The second stage of encryption process which is the diffusion stage resolves this issue and enhances the security. In diffusion stage, the sequences generated by chaotic system modify the values of each pixel in a well-organized manner. This is repeated several times in order to satisfy the level of security.

2. LITERATURE SURVEY

In this section, we present a study of various research papers based on image encryption / decryption techniques and performance parameters that can play an important role in improving algorithm efficiency and security.

In [8], the author presents a comparative study of the three-block cipher (RC6, MRC6, and Rijandale) algorithm. This paper contains different types of bitmap images using the above three encryption algorithm, the maximum difference between the original and encrypted images, the correlation coefficient between the encrypted and the original images, measuring the pixel value of the original image and its variance, the pixel value of the encrypted one, the encryption time and the throughput. These elements have been applied in three encryption algorithms to evaluate both: images with several high-frequency components and images containing large areas of the same color as examples of binary images.

This article [9] recommends using this secure clinical image transmission. Attackers are limited their work to scientific films. Producing a noisy signal using the Chaotic Henon map is the first step in this work. Signals both in x and y axis used to create the Henon equation. It promises to send clinical pictures to two patients in one transmission. For example, the first patient is inserted into the 'x' axis and the other is inserted into the 'y-axis'.

In this document (10) a novel method of image cryptography is introduced. Here chaotic logistics maps are used to meet high level of security during image transfer. This is done by using an external secret key of 80 bit and two chaotic logistics maps. The initial conditions of the two logistic maps give an era in which all of its bits are assigned different weight with the external secret key.

The proposed algorithm [11] uses the Rossler chaotic system and the Lawrence chaotic system for encryption. It is unfamiliar to use two or more chaotic systems in an algorithm. The long term chaotic behavior is recurring and relies on initial variables. The Rossler and Lawrence schemes rely on three variables each, increasing the security of the proposed chaotic system because the total number of parameters depends on the six variables, making it very secure. This algorithm changes the pixels of an image and changes its gray scale values for a certain number of iterations. XOR functions are used for encryption and

decryption. In our view, the main point of the proposed algorithm is good with regard to the total number of initial parameters that grow from three to six for each chaotic system. The interconnection of the resulting cipher is also excellent.

An algorithm to create random bit sequences on the basis of chaotic maps is suggested by [12]. These random bit sequences are created from tent and chaotic maps logistics. These chaotic functions performed permutation of the plain image pixels, and then dividing the image into eight-bit map planes. The bits were replaced by different bits value according to the chaotic ergodic matrix. From our perspective the algorithm showed good with regard to key sensitivity and key space. Hence, this algorithm is highly combatable against brute force attacks and statistical attacks.

In this document [13], the cryptography of the image is created using a new technique that uses several circular mappings. This algorithm is divided into 3 different phases. The first phase consists of generating a pair of sub keys using chaotic logistic map. These sub keys are used in the second phase to encrypt the image and thus to acquire diffusion. The third phase is more elaborative where the sub keys are generated using four different chaotic maps. Based on the initial conditions, each map from its orbits produces various random numbers. The key for encryption is selected from these random numbers. Again a binary sequence is produced in accordance with the selected key for encryption. The input image is transformed into a 1D matrix and other several sub-blocks with the help of Raster and Zigzag scanning models. Then, the alignment is applied to each binary matrix based on the latched maps. Eventually it is possible to decrypt the image using the same sub key.

3. CONCLUSION

The use of digital communication is increased with the growth of internet. And data protection became an essential concern of digital communication. Images are broadly used for communication. A safe and unthreatened image encryption became inevitable. Chaotic based image encryption is optimal way of image encryption. This document discusses several cryptographic algorithms that use different chaotic maps. Each algorithm has its advantages and disadvantages depending on its encryption performance. For secure encryption of images, they use different size maps. It is possible to encrypt an image in various methods and speeds using chaotic maps of different sizes. The algorithm depicted here is immune to any attack that can be proved using security analysis. Image security can also be enhanced through multiple chaotic image encryption methods.

REFERENCES

[1] D. STINSON. CRYPTOGRAPHY: THEORY AND PRACTICE. CHAPMAN & HALL/CRC, ONTARIO, CANADA, THIRD EDITION, 2006.

[2] Chetana Singh, Binay Kumar Pandey, DR.H.L.Mandoria, Ashok Kumar " A Review Paper on Chaotic Map Image Encryption Techniques", International Research Journal of Engineering and Technology (IRJET) - Volume: 05, Issue: 04, Apr-2018

[3] Bhatti, U. and Hanif. M. 2010. Validity of Capital Assets Pricing Model.Evidence from KSE-Pakistan.European Journal of Economics, Finance and Administrative Science, 3 (20).

[4] Sankpal, Priya R, PA Vijaya. Image Encryption Using Chaotic Maps: A Survey. Signal and Image Processing (ICSIP). Fifth International Conference on. IEEE, Jan 8 2014: 102-107

[5] Asia Mahdi, Naser Alzubaidi, "Selective Image Encryption with Diffusion and Confusion Mechanism", International Journal of Advanced Research in Computer Science and Engineering (IJARCSSE) -Volume 4, Issue 7, July 2014

[6] .H.L.Mandoria,Samridhi Singh et al(2017)" A Review on Image Encryption Technique and to Extract Feature from Image" IJCA International Journal of Computer Application.

[7] Jolfaei Alireza, AbdolrasoulMirghadri. An image encryption approach using chaos and stream cipher. Journal of Theoretical and Applied Information Technology. 2010; 19(2): 117-125.

[8] Nawal El-Fishawy and Osama M. Abu Zaid "Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms" published in International Journal of Network Security, Vol.5, No.3, PP.241–251, Nov. 2007.

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

[10] Mirzaei, O., Yaghoobi, M., & Irani, H. (2012). A new image encryption method: parallel sub-image encryption with hyper chaos. Nonlinear Dynamics, 67(1), 557-566.

[11] Shoaib Ansari, Neelesh Gupta and SudhirAgrawal, ―An Image Encryption Approach Using Chaotic Map in Frequency Domain‖, International journal of Emerging Technology and Advanced Engineering-Volume 2, Issue 8, August 2012

[12] HimanKhanzadi, Mohammad Eshghi, ShahramEtemadiBorujeni. Image encryption using random bit sequence based on chaotic maps. Arabian Journal for Science and engineering. 2014; 39(2): 1039-1047.

[13] G.A.Sathishkumar ,Dr.K.Bhoopathybagan and Dr.N.Sriraam ―Image Encryption Based on Diffusion and Multiple Chaotic Maps‖, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, March2011,181-194.

[14] Monika Agrawal and Pradeep Mishra "A Comparative Survey on Symmetric Key Encryption Techniques "International Journal on Computer Science and Engineering (IJCSE) Vol. 4 No. 05 May 2012

[15] Bremnavas1, B.Poorna2 and I.Raja Mohamed, "Secured medical image transmission using chaotic map", Computer Science and Engineering Elixir Comp. Sci. Engg. 54 (2013) 12598-12602

[16] Rajinder Kaur1, Er. Kanwalpreet Singh, "Comparative Analysis and Implementation of Image Encryption Algorithms", International Journal of Computer Science and Mobile Computing (IJCSMC) - Vol. 2, Issue. 4, April 2013, pg.170 – 176