IMAGE ENCRYPTION USING CHAOTIC MAPS OF VARIOUS DIMENSIONS: REVIEW

Rekha Raj[1], Salim Paul[2]

[1]*M Tech Scholar, Department of Electronics and Communication, SCT College of Engineering, Kerala,India*
[2]*Assistant Professor, Department of Electronics and Communication, SCT College of Engineering, Kerala, India*

Abstract

Information Security is an important problem in communication. Information includes text, audio, video, image etc. When information is transferred through various networks, there is high chance of unauthorized access. In many fields such as medical science, military, geographic satellite images etc, high security of information is guaranteed using encryption. As a result, the data confidentiality, integrity, security, privacy as well as the authenticity has become an important issue for communication and storage of data via insecure channel like internet. The available encryption algorithms which are mainly used for textual data maynot be suitable for multimedia data like images. Image encryption can be done in different ways. Most of the encryption techniques have some security and performance issues. Nowadays many algorithms related to image encryption based on the chaotic method have been put forward to improve security during transmission of images. Chaos based encryption systems are mostly used because of their better performance and certain features like sensitivity to initial conditions, state ergodicity, randomness etc. The confusion and diffusion in image is increased using chaos. Chaotic maps have several advantages like enormous key space and high security. In order to reach higher performance, these chaotic based methods take advantage of the more and more complex behavior of chaotic signals. There are different dimensions of chaotic maps used for chaotic encryption like one dimensional, multidimensional and cascade chaotic system. The performance of each systems is determined by the statistical and security analysis. This work is a review of chaos based image encryption algorithms using chaotic maps of different dimensions.

Keywords: *Encryption, Chaotic maps, Cryptography, Confusion, Diffusion*

----------***----------

1. INTRODUCTION

As network technology has developed so fast, data transmission over the networks also increased. This data includes text, image, audio, video etc. The Security of the transmitting data is very important since sometimes it contains valuable and secret things. At present, image transmission over networks is most common. While transmitting images for secure transmission, encryption techniques are applied.

The Image encryption differs from text encryption due to the bulk size, correlation among pixels etc. That is why traditional encryption techniques are not suitable for image encryption. There are several image encryption methods which includes chaos based and non chaos based encryption.. Among them chaos based image encryption is more promising. The complex behavior of chaotic systems helps its higher performance in encryption. Thus many chaotic maps of different dimensions are developed which help in image encryption.

1.1 Chaotic Image Encryption

The word Chaotic means a condition of great disorder. The systems that exhibit chaotic behavior are chaotic systems. Chaotic systems contain two portions 1). a chaotic system and2). an image encryption system. The properties of the chaotic system like sensitivity to initial conditions, state ergodicity, randomness etc make these systems suitable for image encryption. Image encryption is the process ofconverting image information using an algorithm to make it unreadable without the key.

1.2 Chaotic Systems in Cryptography

Chaotic system can be classified into one dimensional and multidimensional systems. 1 D chaotic systems are simple and easy to implement whereas multi-dimensional chaotic maps have complex structures and multiple parameters. 1D maps have certain limitations like limited or discontinuous chaotic range, non-uniform data distribution in the output chaotic sequence and the vulnerability to low computation-cost analysis using iteration and correlation functions.

Both one dimensional and multidimensional systems have their own advantages and disadvantages. Hence new coupled chaotic maps—combination of two one dimensional maps— with better performance are developed.Various image encryption techniques have been proposed based on one-dimensional, multidimensional, coupled chaotic maps etc. Because of better security and lower computational complexity, chaotic cryptography is gaining more importance than others. Chaotic theory deals with deterministic systems whose behavior can be predicted for a while and then they become random. Various studies based on chaotic encryption are conducted in recent years.

2. LITERATURE REVIEW

2.1 . Yicong Zhou, Long Bao, and C.L.Philip Chen proposed an encryption scheme in which a new chaotic system [1] is used for image encryption. In this system, two one dimensional chaotic maps are integrated and a number of new chaotic maps are generated. A novel image encryption algorithm which has the excellent confusion and diffusion properties for withstanding different attacks, especially the chosen-plaintext attacks was introduced by them to demonstrate its applications. A completely different image is obtained whenever the algorithm is applied to an original image with similar set of security keys. This ensures that the algorithm proposed is able to withstand the chosen-plaintext attacks. This can be simulated using matlab.

2.2 An image encryption algorithm based on three dimensional (3D) chaotic map, namely Arnold Cat Map is proposed by A. Kanso, and M. Ghebleh [2] in "A Novel Image Encryption Algorithm Based on a 3D Chaotic Map." This algorithm is able to overcome several attacks. There are three phases in this algorithm facilitating essential properties for a safe image encryption algorithm with confusion and diffusion properties. As per a search rule based on the 3D chaotic map, the image pixels are shuffled in phase I. 3D chaotic maps are used in phase II and III to scramble shuffled pixels through mixing and masking rules, respectively. This algorithm accepts an input image of any size, say M×N×3, where the third dimension represents the RGB values, and uses M and N in the encryption/decryption processes.

2.3 G.A. Sathishkumar, Dr.K. Bhoopathybagan and Dr.N. Sriraam [3] proposed "Image Encryption Based on diffusion and Multiple Chaotic Maps". In this paper, image encryption is based on a technique using multiple chaotic based circular mapping. There are three stages in this algorithm. In the first stage, chaotic logistic maps are used to give a pair of sub keys. In the second stage, logistic map sub keys are used to encrypt image and as a result, diffusion is achieved. In the third stage, four different chaotic maps are used to generate the sub keys. Various random numbers are produced by each map from orbits of the maps on the basis of the initial conditions. From those random numbers, a key is selected for encryption. On the basis of the key controlling the encryption algorithm, a binary sequence is generated. With the help of the two different scanning patterns (raster and Zigzag), the input image is converted into a 1D array and divided into various sub blocks. After that, the permutations are applied to each binary matrix based on the chaotic maps. Finally the image can be decrypted using the same sub keys.

2.4 A novel algorithm for image encryption and decryption is developed by Shoaib Ansari, Neelesh Gupta and Sudhir Agrawal [4] in **"**An Image Encryption Approach Using Chaotic Map in Frequency Domain." In this algorithm the chaotic map used for encryption is 2D Bakers map. First, the 2D discrete cosine transform of the image is calculated. Then the image is shuffled using 2D Bakers map. Here two bakers maps are used. One of them with initial set keys and the other one with Gaussian image created with mean and variance. The DCT transformed image and the diffusion image are XORed iteratively. The random number generator based on Gaussian distribution is used to create the diffusion template. The advantage of this method is that it can provide a key length of 128 bits and above. This technique can be simulated using matlab..

2.5 Xiaoling Huang, Guodong Ye, and Kwok Wo Wong in their paper "Chaotic Image Encryption Algorithm Based on Circulant Operation"[5] proposes the image encryption scheme based on the time-delay Lorenz system and Circulant matrix. In this algorithm time delay Lorenz system is used to generate the chaotic sequence and using this sequence permutation of pixels can be performed along the diagonal and antidiagonal directions.The chaotic system is again used to create a pseudorandom matrix.. Block based diffusion is done using modular operation. As per the plain image the control parameter is generated in diffusion. Security analysis shows that this algorithm can provide a large key space to resist various attacks. After encryption, the correlation between adjacent pixels are zero. Thus this method shows an excellent way of encryption

2.6 "Image Encryption Based on the General Approach for Multiple Chaotic Systems" [6], by H.Alsafasfeh and A.A.Arfoa proposed a new image encryption technique based on new chaotic system . In this system the two chaotic systems: the Lorenz system and the Rössler system are added to form the new chaotic system The first step is setting the initial conditions and parameters (key) Then depending on the image size, a chaotic mask is generated and XORed with the original image. A second mask is generated if the image is not encrypted. The second mask is XORed with the previous image and again if the image is not encrypted, the third mask is generated and XORed with the previous image. Then the encrypted image is obtained. This algorithm has several advantages like large key space, high speed, better security etc.

2.7 "A Designed Image Encryption Algorithm Based on Chaotic Systems" by Huang [7] introduced a new method of image encryption using multi-chaotic systems in which two logistic maps and a 2-D chaotic spatial map are considered. The encryption algorithm consists of permutation and diffusion stages. The initial conditions in 2D discrete spatial system are two chaotic logistic sequence streams. A new preprocess for chaotic sequences and a new diffusion function is designed. Any change in pixels of original image will spread over the whole cipher image. As per various experiments and analysis, the proposed algorithm gives better results.

2.8 Gururaj Hanchinamani and Linganagouda Kulakarni proposed "Image Encryption Based on 2-D Zaslavskii Chaotic Map and Pseudo Hadmard Transform"[8]. In this paper a new type of image encryption based on a 2-D

Zaslavskii Chaotic Map and Pseudo Hadmard transform is proposed. The permutation stage of the encryption process is done by scrambling the rows and columns of the image by chaotic values. In the next stage of encryption, that is diffusion, the avalanche effect is achieved with Pseudo Hadmard transform followed by diffusion in two directions with multiple additions and XOR operations. This method offers high security and high speed.

2.9 "New Approach for Fast Color Image Encryption Using Chaotic Map" [9] by Kamalesh Gupta and Sanjay Silakari presented a new technique in which encryption is done by cascading a 3D standard map and 3D cat map. 3D standard map is used to generate the diffusion template. Using different planes of the input image, the image is rotated. The three planes of the image-red, green and blue- are rearranged using the two maps. After XORing the shuffled image and diffusion template, the image is encrypted. . Various analysis show that the new algorithm can withstand several attacks and gives better encryption.

2.10 Re Boriga, Ana Cristina and Adrian Viorel proposed "A New Fast Image Encryption Scheme Based on 2D Chaotic Maps" [10] that presented an encryption technique based on a new symmetric key stream . This technique uses three 2D chaotic maps which are derived from some plans curves equations. . This method yields large key space which helps to resists several attacks. Bimodular architecture is used in this scheme. Random pixel permutations and diffusion are done for shuffling the pixels and pixel values respectively using the new algorithm.

2.11"A Novel Chaotic Map and an Improved Chaos-Based Image Encryption Scheme"[11] by Xianhan Zhang and Yang Cao suggested a one-dimensional chaotic map which exhibits a larger maximal Lyapunov exponent, indicating better properties of the chaotic map. A new algorithm based on this new chaotic map is used in image encryption, providing a brand new way to encrypt images. It also entails another classical map:Arnold's Cat Map, through which the coordinates of the target image's grey value matrix will be changed to another. Here, the safety of the image is largelystrengthened and guaranteed.

3. CONCLUSIONS

In this paper, many encryption algorithms using different chaotic maps are discussed. Each algorithm has its own advantages and disadvantages depending upon the encryption performance of these algorithms. By analyzing the above mentioned research papers some features of the image encryption techniques are understood. Each of them are using chaotic maps of different dimensions for the secure encryption of images. Image can be encrypted in different ways in different speed by using chaotic maps of various dimensions. The above algorithms are also resistive against various attacks which can be proven by security analysis..

REFERENCES

[1].Yicong Zhou, Long Bao and C.L.Philip Chen"A New 1D Chaotic System for Image Encryption", Signal Process. 97(2014) 172-182

[2] A. Kanso and M. Ghebleh "A Novel Image Encryption Algorithm Based on a 3D Chaotic Map,"Commun Nonlinear SciNumerSimulat17 (2012) 2943–2959.

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

[4] Shoaib Ansari, Neelesh Gupta and SudhirAgrawal, "An Image Encryption ApproachUsing Chaotic Map in Frequency Domain",International journal of Emerging Technologyand Advanced Engineering-Volume 2, Issue 8, August 2012

[5] Xiaoling Huang,Guodong Ye, and Kwok-Wo Wong, "Chaotic Image Encryption Algorithm Based on Circulant Operation", Abstract and Applied Analysis,Volume2013

[6] H.Alsafasfeh, and, A.A.Arfoa, "Image Encryption Based on the General Approach forMultiple Chaotic Systems", Journal of Signaland Information Processing, 2011, 2, 238-244

[7] X Huang, " A Designed Image EncryptionAlgorithm Based on Chaotic Systems", Journalof Computational and Theoretical Nanoscience,Volume 9, Number 12, December 2012,pp. 2130-2135(6)

[8] GururajHanchinamani and LinganagoudaKulakarni, "Image Encryption Based on 2-DZaslavskii Chaotic Map and Pseudo Hadmard Transform", International Journal of HybridInformation Technology Vol.7, No.4 (2014),pp.185-200

[9] Kamalesh Gupta and Sanjay Silakari, " New Approach for Fast Color Image Encryption Using Chaotic Map", Journal of InformationSecurity, 2011, 2, 139-150

[10] RaduEugen BORIGA, Ana Cristina DĂSCĂLESCU, and Adrian Viorel DIACONU, "A New Fast Image Encryption Scheme Based on 2D Chaotic Maps" , IAENG InternationalJournal of Computer Science, 41:4, 2014

[11] Xianhan Zhang and Yang Cao, "A Novel Chaotic Map and an Improved Chaos-Based Image Encryption Scheme", The ScientificWorld Journal Volume 2014(2014).