Journal of The Gujarat Research Society

ISSN: 0374-8588
Volume 21 Issue 8, August 2019

A STATE OF THE ART SURVEY ON CHAOS BASED IMAGE ENCRYPTION FOR SECURE DATA TRANSMISSION

Archana Jyothikiran
Faculty of Engineering and Technology,
Jain (Deemed-to-be University), Ramnagar District, Karnataka – 562112
Email Id: j.archana@jainuniversity.ac.in

Abstract

Digital images represent a big part of multimedia communication in the present data transfer scenario. Their welfare, therefore, is a great area of concern. Different chaotic maps, used in image encryption, are analyzed in this paper and their merits and demerits are discussed. For image encryption, the properties of chaotic maps such as stochastic, ergodicity, and highly sensitive to initial situations make them secure. Low-dimensional chaotic maps were used for many of the earlier proposed image encryption methods, showing the lowest degree of security and having very little ability to withstand brute force and statistical attacks. Researchers have created numerous high dimensional chaotic maps to solve this problem. An attempt has been made to illustrate the characteristics and techniques of various chaotic maps used for image encryption in this review article.

Keywords: *Cryptography, Digital Images, Encryption, Image Encryption, Multimedia Communication.*

I. INTRODUCTION

Due to rapid developments in internet technology, a vast amount of data that is distributed over the internet is images. The security of these photos is, therefore, a major area of concern. Various methods of steganography and cryptography have been suggested to deal with these problems [1]. Cryptography is the investigation of devices beyond the sight of the intruder for safe conversation.

It handles problems such as encryption, authentication, etc. In cryptography, before storing or transmitting it, native information is coded into an indistinct cypher picture [2].

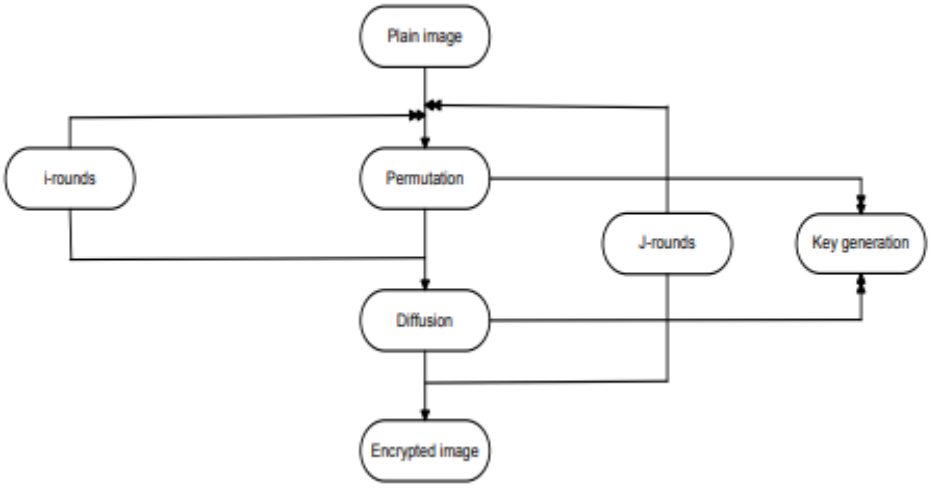

Fig. 1: Illustrates Chaotic Image Encryption Approach.

Using the following formulas, the relationship analysis of the images is carried out. Correlation plays a key role in assessing the resemblance between the two neighboring pixels of the plain image as well as the cypher image. By applying the formulas below, the correlation coefficient of the images can be determined [3].

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2$$

$$cov\ (x,y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))\ (y_i - E(y))$$

$$r_{xy} = \frac{cov\ (x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

$$\sqrt{D(x)}\ \neq 0, \sqrt{D(y)} \neq 0$$

The NPCR and UACI can be calculated by utilizing the following equation [4].

$$NPCR = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \times 100\ \%$$

$$UACI = \left[\sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|C1(i,j) - C2(i,j)|}{255} \right] \times \frac{100\%}{M \times N}$$

$$r_{x,y} = \frac{C(x,y)}{\sqrt{D(x)}.\sqrt{D(y)}}$$

Where $C(x,y), D(x)$ and $D(y)$ can be evaluated by using the following equations.

$$C(x,y) = \frac{\sum_{i=1}^{K}(x_i - E(x))(y_i - E(y))}{K}$$

$$D(x) = \frac{1}{K} \sum_{i=1}^{K} (x_i - E(x))^2$$

$$D(y) = \frac{1}{K} \sum_{i=1}^{K} (y_i - E(y))^2$$

II. LITERATURE REVIEW

Pareek et al. conducted a survey on image encryption using chaotic logistic map. In recent years, several new and effective ways of developing stable image encryption techniques have been suggested by chaos-based cryptographic algorithms. We suggest a new approach to image encryption in this communication, based on chaotic logistic maps, in order to satisfy the requirements of safe image transfer. An external secret key of 80-bit and two chaotic logistic maps are used in the proposed picture encryption scheme. Using the external secret key, the initial conditions for the two logistic maps are obtained by supplying all bits with distinct weighting [5].

III. DISCUSSION AND CONCLUSION

When we share data over an unpredictable communication medium, information security turns out to be increasingly important. Few techniques can be used to provide a safe data trade, and one of them is data encryption, set up to be moved in a mixed manner and decoded when the information should be used. The paper addressed various maps of chaos used in image encryption and analyzed their advantages and disadvantages. In both encoding and decoding procedures, our attention should be on the encryption keys in a fine encryption algorithm. The calculation of key space is the aggregate amount of a distinctive key that can be used as part of the encryption. In the general channel, the cypher text images are passed while the security key is transmitted via the private channel. In this way, the security key should have a valid size and must be vulnerable to attack by brute force.

IV. REFERENCES

[1] E. N. Kumar and E. S. Kumar, "A Simple and Robust EVH Algorithm for Modern Mobile Heterogeneous Networks- A MATLAB Approach," 2013.

[2] S. Kumar, A. Gupta, and A. Arya, Triple Frequency S-Shaped Circularly Polarized Microstrip Antenna with Small Frequency-Ratio. International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)/ISSN(Online): 2320-9801, 2016.

[3] T. Gao and Z. Chen, "A new image encryption algorithm based on hyper-chaos," Physics Letters, Section A: General, Atomic and Solid State Physics, 2008, doi: 10.1016/j.physleta.2007.07.040.

[4] C. Li, G. Luo, K. Qin, and C. Li, "An image encryption scheme based on chaotic tent map," Nonlinear Dynamics, 2017, doi: 10.1007/s11071-016-3030-8.

[5] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," Image and Vision Computing, 2006, doi: 10.1016/j.imavis.2006.02.021.