Journal of The Gujarat Research Society
ISSN: 0374-8588
Volume 21 Issue 9, September 2019

ENCRYPTION OF IMAGES BY APPLYING THE CHAOTIC MAPPING: A COMPREHENSIVE SURVEY

Trishie Sharma
Faculty of Engineering and Technology,
Jain (Deemed-to-be University), Ramnagar District, Karnataka – 562112
Email Id: s.trishie@jainuniversity.ac.in

Abstract

A novel image encryption algorithm based on the combination of pixel shuffling and three chaotic maps is proposed in this paper. This algorithm is based on pixel scrambling, where the location of the data is scrambled by the randomness of the chaos. Shuffling is used to expand image diffusion and dissipate the high correlation between pixels of the image. Chaotic maps have good potential for designing dynamic permutation maps due to their sensitivity to initial conditions. The plain image is first decomposed into 8x8-size blocks in the proposed algorithm, and then the block-based image shuffling is carried out. After that, using a chaotic sequence generated by another chaotic map, the shuffled image is encrypted. The algorithm proposed was measured through a series of tests in order to evaluate performance. Experimental results show that the system is highly sensitive to key issues and shows good resistance to brute-force and statistical attacks.

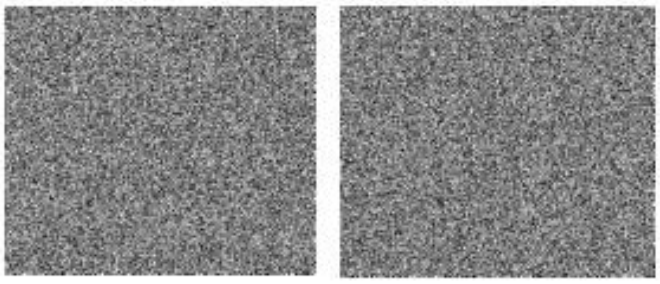
Keywords: *Algorithm, Bandwidth, Cryptography, Encryption, Image, Dynamic permutation.*

I. INTRODUCTION

The symmetrical encryption is not ideal for instances where such documents have to be exchanged individually-to-many, because the exchange of the secret key between the sender and the recipient is not secure as private key can be intercepted in an open network resulting in confidentiality loss. The cryptography of the public key is more suitable since the exchange of the secret key is not involved. Instead of using symmetric encryption to encrypt the image, most existing public key cryptosystems do not use public key cryptosystems to encrypt an image, and a public key cryptosystem is used as a key exchange protocol [1].

(a) Real Images

For image encryption, there are certain important properties that can be highlighted as critical, particularly overhead bandwidth and computational costs. Photos are typically transmitted in the form of compression nowadays. Therefore, by combining encryption with compression while keeping image communication secret, it is a good strategy to reduce bandwidth and compute load [2]. Figure 1: Illustrates the (a) Real Images (b) Encrypted Images (c) Recovered Real Images. Figure 2: Illustrates the encryption scheme procedure.



(b) Encrypted Images

(c) Recovered Images

Fig. 1: Illustrates the (a) Real Images (b) Encrypted Images (c) Recovered Real Images

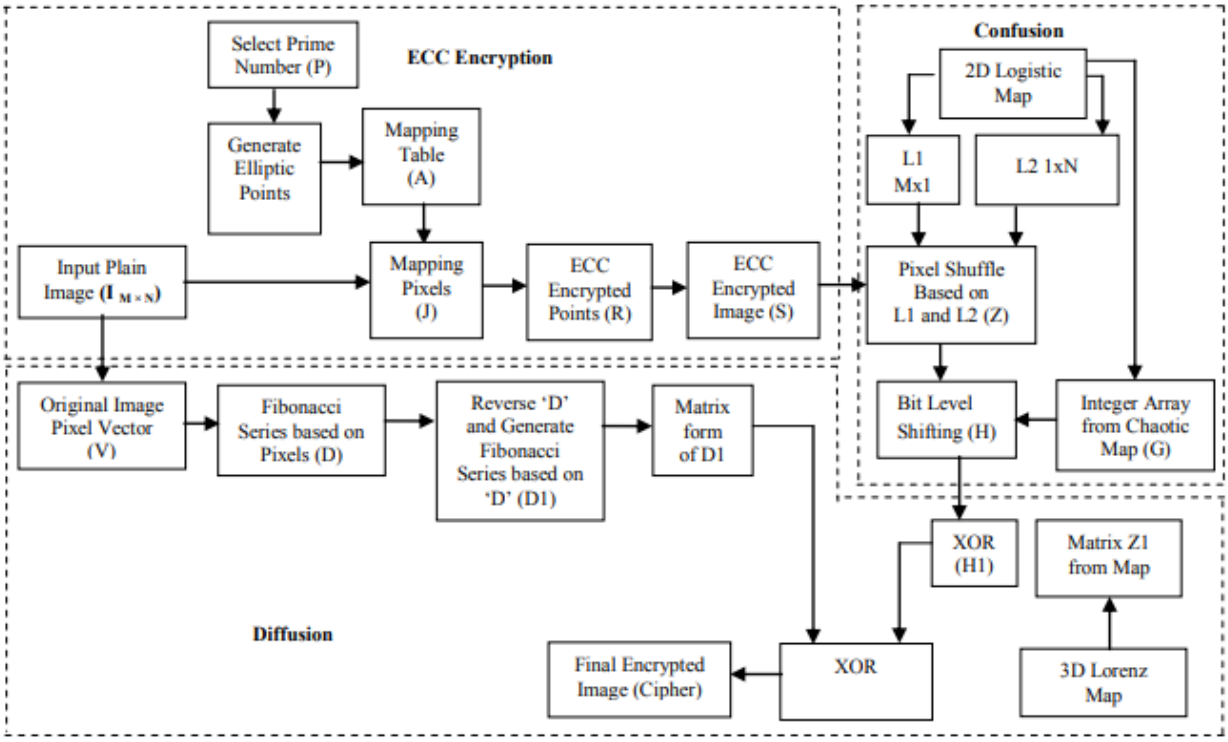


Fig. 2: Illustrates the encryption scheme procedure

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

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

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

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

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

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

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

Another critical constraint is the correlation coefficient to ensure that the encryption algorithm is very accurate. The expression is given below [3].

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

Where $C(x,y), D(x)$ and $D(y)$ may be evaluated by utilizing the following equations[4].

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

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

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

II. LITERATURE REVIEW

A survey was performed on various encryption methods by Priya et al. This paper focuses primarily on the different types of existing encryption techniques and, as a literature review, frames all the techniques together. The aim is a detailed experimental study of the implementation of various available encryption techniques. It also focuses on image encryption techniques, techniques for information encryption, double encryption, and Chaos-based encryption techniques. This thesis relates to the efficiency criteria that are used in encryption processes and discusses their security concerns [5].

III. DISCUSSION AND CONCLUSION

A new way of image encryption scheme using two messy logistic maps and an external 80-bit key has been suggested in this correspondence. Using the external secret key, the initial conditions for both the logistic maps are obtained by providing weighting to their bits corresponding to their place in the key. Eight different types of operations are used in the proposed encryption method to encrypt the pixels of an image and the result of the logistic map determines which operation will be used for a specific pixel. To make the cipher more resilient against any attack, after encrypting a block of sixteen pixels of the image, the secret key is changed. To demonstrate the security of the latest image encryption method, we have carried out statistical analysis, key sensitivity analysis

and key space analysis. Finally, we conclude with the remark that it is anticipated that the proposed method would be useful for applications for real time image encryption and transmission.

IV. REFERENCES

[1] C. C. Chang, M. S. Hwang, and T. S. Chen, "A new encryption algorithm for image cryptosystems," *J. Syst. Softw.*, 2001, doi: 10.1016/S0164-1212(01)00029-2.

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

[3] 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.

[4] M. Khan and T. Shah, "A Literature Review on Image Encryption Techniques," *Autoimmunity Highlights*. 2014, doi: 10.1007/s13319-014-0029-0.

[5] P. R. Sankpal and P. A. Vijaya, "Image encryption using chaotic maps: A survey," 2014, doi: 10.1109/ICSIP.2014.80.