Journal of The Gujarat Research Society
ISSN: 0374-8588
Volume 21 Issue 13, December 2019

A REVIEW PAPER ON COLOR IMAGE ENCRYPTION BY USING 3-D CHAOTIC CAT MAP

Shruthishree S H
Jain (Deemed-to-be University), Ramnagar District, Karnataka – 562112
Email Id: sh.shruthi@jainuniversity.ac.in

Abstract

Information security has become a big concern with the introduction of cloud and social networking networks. Photos are the most searched, uploaded, and exchanged data in multimedia. However, since digital images have a large data size, high redundancy, and a clear correlation between pixels, current encryption algorithms such as DES and AES may not be appropriate for image encryption. Using a generalized three-dimensional chaotic cat map and programmable complemented maximum length cellular automata (PC-MLCA) in this paper, we propose a new colour image encryption algorithm to solve these problems. We also design the PC-MLCA that can be hardware implemented and has a long period of time and can generate a nonlinear sequence as a pseudo random number generator (PRNG). The main sequence created by the proposed PC-MLCA changes the pixel value to an unpredictable value in the original image. And we build and use a generalized chaotic cat map to resist noise and delete attacks that can perform various modular operations to adjust the pixel location of colour images horizontally, vertically, and colour components of R, G, and B at the same time.

Keywords: *Cat Map, Encryption, Image, Information, Security, Digital, Data, Protection, Accuracy.*

I. INTRODUCTION

The development of internet communication technology has dramatically increased the number of Internet users all over the world [1]. In addition, with the increase of mobile phone penetration rate, various activities using SNS have increased. In particular, the emergence of smart terminals such as smart phones and multimedia content services provided by smart devices have become possible [2].

Journal of The Gujarat Research Society
ISSN: 0374-8588
Volume 21 Issue 13, December 2019

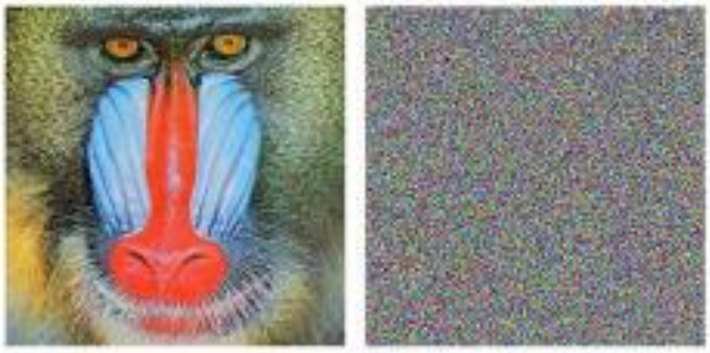

Figure 1: Illustrates the Real Images and Encrypted Image

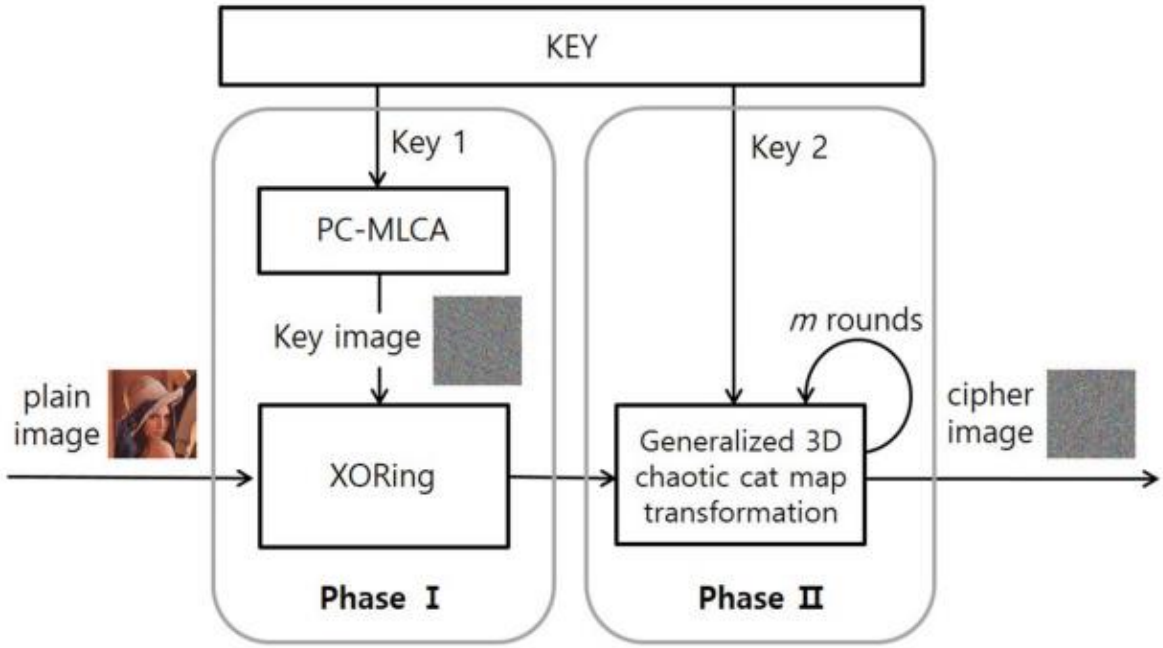

Figure 2: Illustrates the outline of the proposed method

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

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

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

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

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

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

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

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

The correlation coefficient is another essential constraint to ensure that how much efficient is the encryption algorithm [3].

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

Where $C(x,y), D(x)$ and $D(y)$ can be evaluated by using the following equations [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 research using block BWT-MTF and hybrid fractal compression techniques was carried out by Choi et al. on near-lossless medical image compression. For efficient medical image transmission using block BWT-MTF with Huffman encoding and hybrid fractal encoding, a medical image compression model is proposed in this paper. Diagnosis of medical images requires close analysis of critical portions of the image. In medical image compression, a small loss in the critical portion leads to incorrect perception[5].

III. DISCUSSION AND CONCLUSION

We have presented a new encryption algorithm in this paper that can effectively encrypt colour pictures. The proposed algorithm was based on a 3-D chaotic cat map based on PC-MLCA and generalized. In particular, using a CA that can be implemented in hardware, we proposed a method for generating a key picture. A nonlinear key sequence that is much longer than the C-MLCA used in was created by the PC-MLCA built in this paper, and also extended the key space. We generated a key image using PC-MLCA to replace the pixel values of the original image with unpredictable pixel values and then performed an XOR operation on the generated key image and the original colour image. Additionally, to resist image modulation or deletion attacks that can occur during image transmission and storage, a

generalized 3-D chaotic cat map was suggested. Via different module operations, the suggested generalized 3-D chaotic cat map simultaneously modified the location of pixels in the R, G, and B colour image channels. Experimental findings and safety analysis have shown that the association between the image pixels encrypted by the proposed encryption algorithm is decreased and the encrypted image histogram is equally distributed.

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

[4] Y. P. Zhang, Z. J. Zhai, W. Liu, X. Nie, S. P. Cao, and W. Di Dai, "Digital image encryption algorithm based on chaos and improved DES," 2009, doi: 10.1109/ICSMC.2009.5346839.

[5] G. Mehta, M. K. Dutta, and P. S. Kim, "An efficient and lossless cryptosystem for security in tele-ophthalmology applications using chaotic theory," Int. J. E-Health Med. Commun., 2016, doi: 10.4018/IJEHMC.2016100102.