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

PICTURE ENCRYPTION METHOD BY APPLYING COSINE-TRANSFORM-BASED CHAOTIC SYSTEM: A REVIEW PAPER

Dr. P. Pradeepa
Associate Professor, Department of EEE, Faculty of Engineering and Technology, Jain (Deemed-to-be University), Ramnagar District, Karnataka – 562112
Email Id: p.pradeepa@jainuniversity.ac.in

Abstract

Due to its properties such as unpredictability and initial state sensitivity, Chaos is recognized as a natural candidate for cryptography applications. Some chaos-based cryptosystems, however, have been shown to exhibit different security defects because their chaotic maps used do not have complex dynamic behaviors. This paper introduces a cosine-transform-based chaotic framework to solve this problem (CTBCS). The CTBCS can generate chaotic maps with complex dynamical behaviors using two chaotic maps as seed maps. For example, using the CTBCS, we create three chaotic maps and evaluate their chaos complexity. We further propose an image encryption scheme using one of the generated chaotic maps. To separate adjacent pixels, the encryption scheme uses high-efficiency scrambling and uses random order substitution to distribute a slight shift in the plain image to all cipher-image pixels. The performance appraisal shows that the chaotic maps generated by the CTBCS exhibit significantly more complex chaotic behaviours than the current ones

Keywords: *Chaotic Maps, Digital Information, Encryption, Image, Data safety, Protection.*

I. INTRODUCTION

A large amount of digital information is produced and distributed every moment across different networks at present. A commonly used data format is the digital image, since it carries information in a visualized way. Some are hidden images among the images distributed through networks that owners do not want others to access without permission. A common example may be the hidden picture of the military [1].

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

Figure 1: Illustrates the real and encrypted images [2]

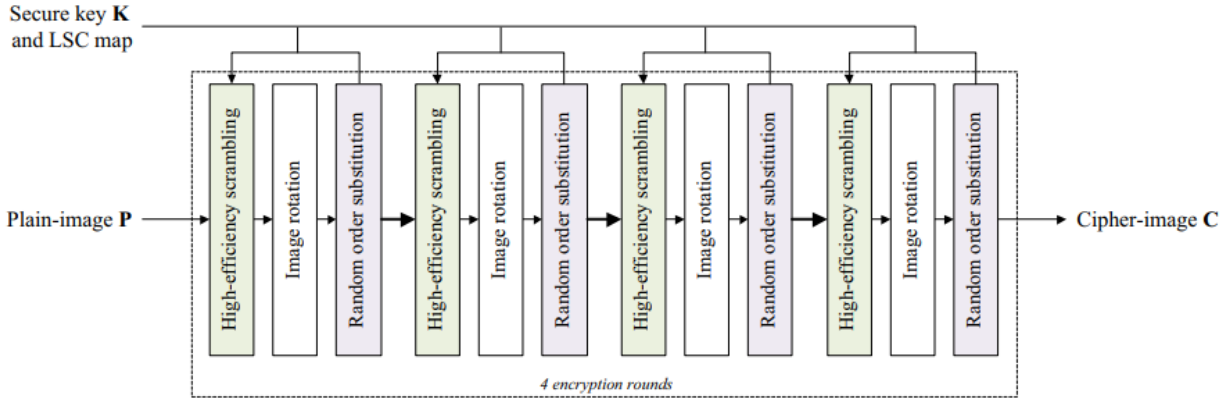

Figure 2: Illustrates the general Structure of LSC-IES [3]

$$MSE = \frac{\sum_{i=1}^{H}\sum_{j=1}^{W}[P(i,j) - E(i,j)]^2}{W \times H}$$

$$MAE = \frac{1}{W \times H}\sum_{i=1}^{H}\sum_{j=1}^{W}|p(i,j) - E(i,j)|$$

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

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

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

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

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

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

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

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

The correlation coefficient is another essential constraint to ensure that how much efficient is the encryption algorithm [4].

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

Where $C(x,y)$, $D(x)$ and $D(y)$ can be evaluated by using the following equations [5].

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

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

II. LITERATURE REVIEW

An experiment was performed using interference in the multi-parameter fractional Fourier transform domain by Zhong et al. on Silhouette-free image encryption. A new semi-fragile image-watermarking technique based on Center-Symmetric Local Binary Patterns (CSLBP) in the integer wavelet domain is suggested in this research. In the phases of the proposed process, Integer Wavelet Transform (IWT), block division, Center Symmetric Local Binary Pattern (CSLBP) based watermark embedding and extraction, watermarking key creation, watermarking key encryption using Advanced Encryption Standard (AES) based logistic map and watermarking key decryption methods were used.

III. DISCUSSION AND CONCLUSION

First of all, this paper proposed a chaotic cosine-transform-based method known as the CTBCS, which uses the cosine transform to generate new chaotic maps with complex chaos output as a nonlinear transform. Three new chaotic maps have been created as examples to illustrate the efficiency of the CTBCS. The performance assessments showed that the CTBCS's chaotic maps exhibit significantly superior chaos performance over the chaotic maps generated by other techniques and their seed maps. We further proposed an image encryption scheme known as LSC-IES using the LSC map created by the CTBCS. The well-known diffusion-confusion principle is followed by the LSC-IES and we simulated it using various digital images. The security review showed that the LSC-IES is very sensitive to its secret keys, and has a higher degree of security than many competing algorithms for image

encryption. This work will facilitate the development of chaos theory and encryption based on chaos. We will explore the further use of LSC-IES in video encryption.

IV. REFERENCES

[1] A. R. Elshazly, M. M. Fouad, and M. E. Nasr, "Secure and robust high quality DWT domain audio watermarking algorithm with binary image," 2012, doi: 10.1109/ICCES.2012.6408514.

[2] L. Sui, K. Duan, and J. Liang, "A secure double-image sharing scheme based on Shamir's three-pass protocol and 2D Sine Logistic modulation map in discrete multiple-parameter fractional angular transform domain," Optics and Lasers in Engineering, 2016, doi: 10.1016/j.optlaseng.2015.12.016.

[3] J. Wu, X. Liao, and B. Yang, "Color image encryption based on chaotic systems and elliptic curve ElGamal scheme," Signal Processing, 2017, doi: 10.1016/j.sigpro.2017.04.006.

[4] 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.

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