Journal of The Gujarat Research Society

ISSN: 0374-8588
Volume 21 Issue 9, September 2019

IMAGE ENCRYPTION USING CONVOLUTION OPERATION: A REVIEW PAPER

Dr. Krishnakant Singh
Faculty of Engineering and Technology,
Jain (Deemed-to-be University), Ramnagar District, Karnataka – 562112
Email Id: ks.krishna@jainuniversity.ac.in

Abstract

This paper introduces a new image encryption algorithm based on the operation of convolution. Several pseudo-random sequences are generated by Chen's chaotic method and general convolution operation using an external key of 300 bits in length, and then their statistical properties are checked. The proposed image encryption scheme contains one operation coverage module, two operation diffusion modules, and one operation uncertainty module. The covering module uses a pseudo-random sequence to cover a binary XOR operation of the original plain image. The diffusion modules are based on the multiplication of the GF finite field (28) and the windowed convolution with the summation of modulus 256, and on the dissemination to all the pixels of the diffused image of the information of any pixel in the original image. Each pseudo-random sequence value is used by the confusion module as the offset address of the pixel replacement to permit the scattered image. The simulation experiment and comparative analysis show that the image cryptosystem proposed has the advantages of fast processing speed, good sensitivity, and high strength of encryption, and can be used as a functional image cryptosystem candidate.

Keywords: *Advanced Encryption Standard (AES), Cypher Block, Encryption, Image, Diffusion module.*

I. INTRODUCTION

The Advanced Encryption Standard (AES) was issued by the National Institute of Standards and Technology (NIST) as the current standard for text data encryption in 2001 to replace the Data

Encryption Standard (DES) [1]. The AES is a block cypher with a 128-bit packet length and a 128, 192, or 256-bit key length. Image data has the characteristics of enormous data volume, good similarity between adjacent pixels, and high data redundancy compared with text data [2]. Image encryption thus involves a large number of key streams. AES can be used in image encryption in cypher block chaining (CBC) mode, but it is poor in encryption speed and sensitivity [3].

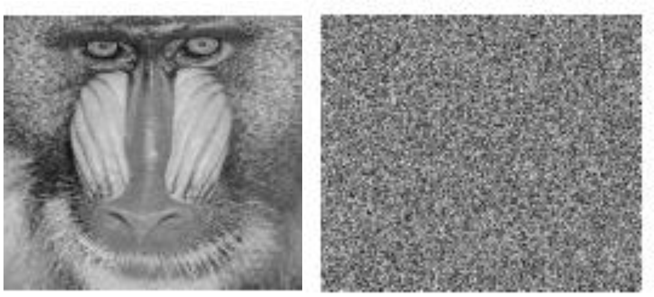

Fig 1: Illustrates the Real Images and Encrypted Image

IMAGE ENCRYPTION USING CONVOLUTION OPERATION

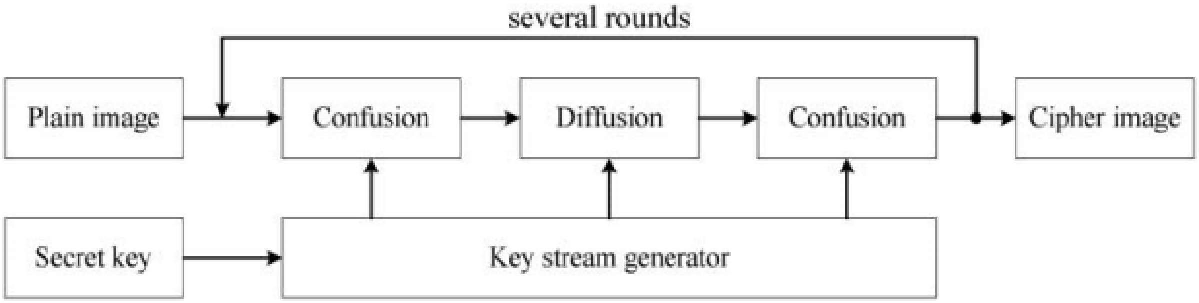

Fig 2: Illustrates the traditional picture encryption method by using on chaotic system [4]

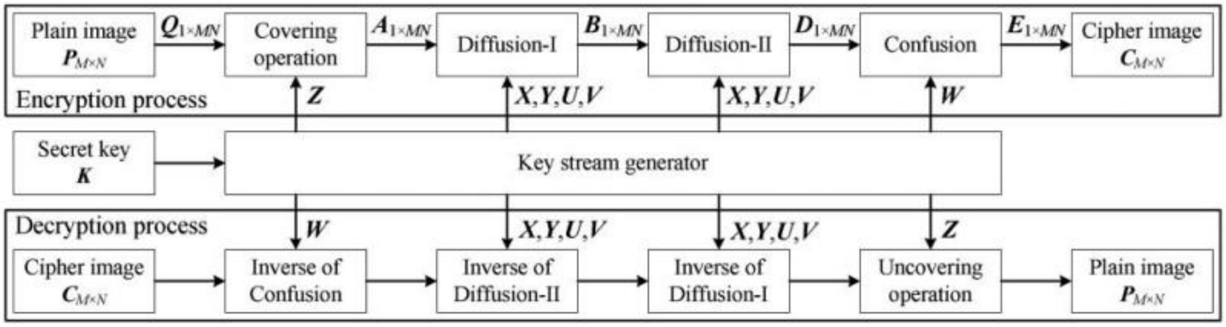

Fig 3: Illustrates the proposed picture cryptosystem

Figure 1: Illustrates the Real Images and Encrypted Image. Figure 2: Illustrates the traditional picture encryption method by using on chaotic system. Figure 3: Illustrates the proposed picture cryptosystem. The Haar wavelet transform can be expressed by matrix form as I = HIHT, where I is an image matrix of order M × M, H is Haar transform matrix of order M × M and I is the resulting transformed matrix of order M × M that contains the Haar basis function Hn(x), which is defined in x ∈ [0, 1], where n = 0, 1, 2, ... , M − 1 can be decomposed uniquely as:

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

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

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

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

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

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

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

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

The correlation coefficient is another essential constraint to ensure that how much efficient is the encryption algorithm [5].

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

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

Li et al. proposed a symmetric image encryption scheme based on 3D chaotic cat maps. Due to some inherent characteristics of images, such as bulk data capacity and high redundancy, which are usually hard to manage by conventional methods, image encryption varies from that of texts. Thanks to the extremely desirable properties of mixing and sensitivity to initial conditions and parameters of chaotic maps, Chaos-based encryption has suggested a new and efficient way to deal with the intractable problem of simple and highly protected image encryption. In this paper, for designing a real-time protected symmetric encryption scheme, the two-dimensional chaotic cat map is generalized to 3D [6].

III. DISCUSSION AND CONCLUSION

A new image cryptosystem based on convolution operation is presented in this paper. Different from the classical image cryptosystem, the proposed image cryptosystem employs the new structure of "covering– diffusion–diffusion–confusion". The windowed convolutions are used in diffusion operations to diffuse the image information. Simulate results and comparative analysis show that the proposed image cryptosystem has the advantages of fast processing speed, strong sensitivity, and high security intensity, and can be one of the candidates for practical image cryptosystems. In the proposed image cryptosystem, the windowed convolution operation has played the key role. The window length of the windowed convolution used in the simulation tests is 5. Obviously, the longer the window is, and the more complex the convolution, the better the diffusion effect is. So, our future work will focus on studying the fast diffusion algorithm based on convolution operation with longer window to further improve the security of the image encryption system.

IV. REFERENCES

[1] C. Pak and L. Huang, "A new color image encryption using combination of the 1D chaotic map," *Signal Processing*, 2017, doi: 10.1016/j.sigpro.2017.03.011.

[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] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI Randomness Tests for Image Encryption," *cyberjournals.com*, 2011.

[5] S. Hanis and R. Amutha, "Double image compression and encryption scheme using logistic mapped convolution and cellular automata," *Multimed. Tools Appl.*, 2018, doi: 10.1007/s11042-017-4606-0.

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