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

ENCRYPTION OF IMAGE BY PLAINTEXT-RELATED SHUFFLING: A COMPREHENSIVE REVIEW

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

Abstract

This paper suggested a method of image encryption similar to plaintext, which used the hyper chaotic system to establish the hidden code streams used for encryption. Two plaintext-unrelated diffusion operations and one plaintext-related shuffling are involved in the encryption algorithm. The suggested encryption scheme will resist the chosen/known plaintext attacks because of the use of plaintext-related shuffling. Simulation results show that there are many good characters in the proposed method, such as fast encryption speed, wide key space, high sensitivity of the key, successful resistance to differential attack, noise-like cipher-text picture, etc., and can therefore be used in real communications. This review article provides a detailed review on the image encryption by applying the plaintext-related shuffling.

Keywords: *Differential Attack, Encryption, Image Encryption, Plaintext, Speed, Diffusion operation.*

I. INTRODUCTION

One of the most powerful means to ensure the protection of image information shared on the internet is image encryption. Traditional encryption algorithms, such as DES, AES, IDEA, etc., are not suitable for image encryption due to the enormous data volume and high information redundancy of the image [1]. Scientists have suggested a number of picture encryption schemes based on chaotic systems in recent years [2]. These image encryption systems used chaotic systems to create the secret code streams for image encryption and convert the plain images through chaos and diffusion operations into noise-like cipher-text images [3].

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

Fig 1: Illustrates the Original Images and Encrypted Image [4]

ENCRYPTION OF IMAGES

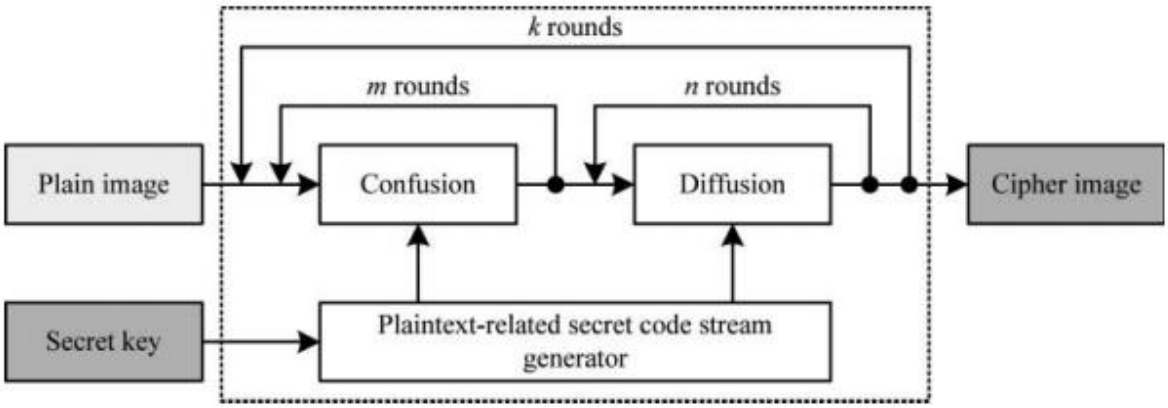

Fig 2: Illustrates the procedure of the image encryption method [5]

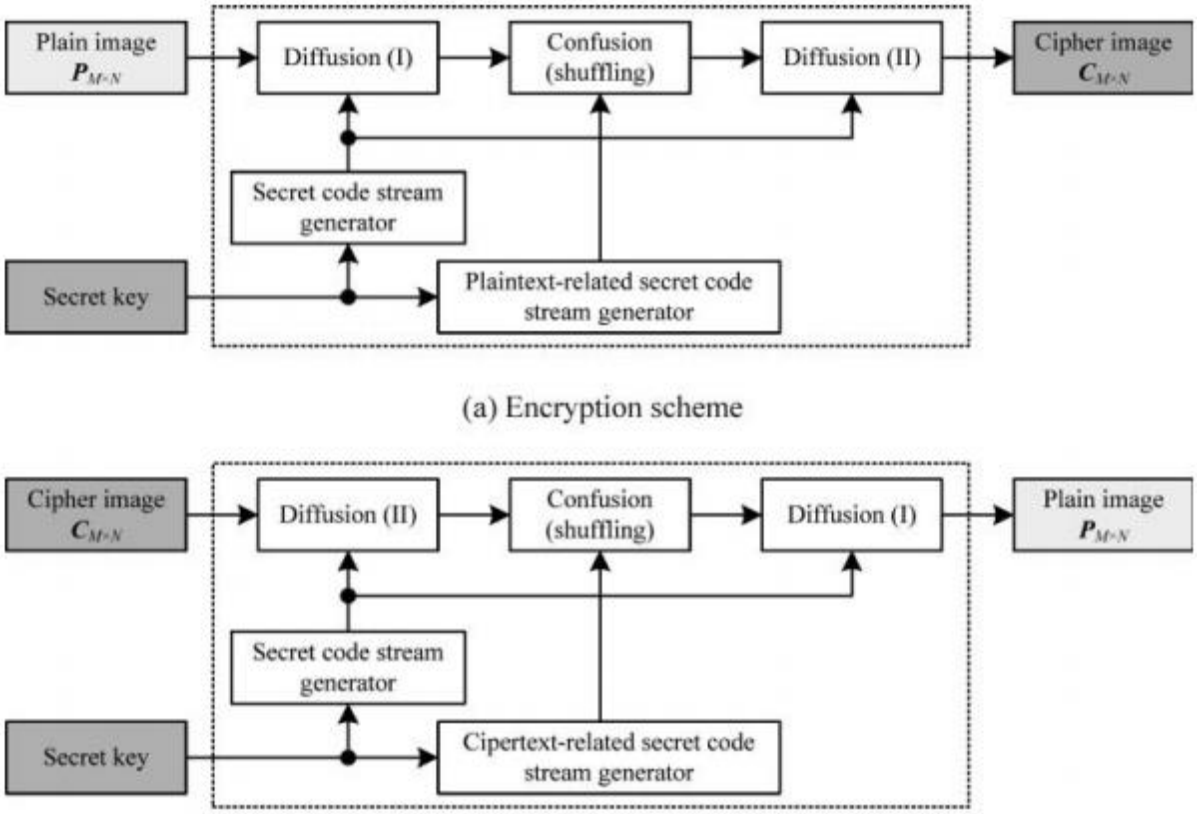

Fig 3: Illustrates the procedure of the image decryption method [6]

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

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

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

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

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

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

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

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

II. LITERATURE REVIEW

A research by Liu et al. was performed on the Chaos-based image encryption algorithm. A new image encryption scheme is introduced in this letter, in which shuffling the locations and adjusting the grey values of the image pixels are combined to confuse the cipher-image and plain-image relationship. Firstly, the Arnold cat map is used for shuffling the spatial-domain locations of the image pixels. The discrete output signal of the Chen chaotic device is then preprocessed to be adequate for grayscale image encryption, and the shuffled image is encrypted by the preprocessed signal pixel by pixel. The experimental results show that the key space is large enough to withstand the attack of brute force and there is a random-like behavior in the distribution of the grey values of the encrypted image [7].

III. DISCUSSION AND CONCLUSION

This paper has introduced a new plaintext-related image encryption method. This involves the forward diffusion of plaintext-unrelated, plaintext-related shuffling, and backward diffusion of plaintext-unrelated. In order to encrypt various plain images, the proposed system has different equivalent keys due to the use of plaintext-related shuffling. As a consequence, the device proposed will resist the attacks of selected/known plaintext. In addition, the simulation results show that the proposed system has good characteristics, such as fast encryption/decryption speed, large key space, strong key sensitivity, effective resistance to differential attack, noise-like cipher-text image, ideal entropy value for information, etc. and can therefore be used in practical communications.

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] X. Zhang and W. Chen, “A new chaotic algorithm for image encryption,” 2008, doi:

10.1109/ICALIP.2008.4590187.

[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] R. Enayatifar, A. H. Abdullah, and I. F. Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence," *Opt. Lasers Eng.*, 2014, doi: 10.1016/j.optlaseng.2013.12.003.

[5] A. Achuthshankar, A. Achuthshankar, K. P. Arjun, and N. M. Sreenarayanan, "Implementation of reversible Data Hiding in Encrypted Image using A-S Algorithm," 2016, doi: 10.1109/ICGCIoT.2015.7380662.

[6] S. Lian, J. Sun, and Z. Wang, "Security analysis of a chaos-based image encryption algorithm," *Phys. A Stat. Mech. its Appl.*, 2005, doi: 10.1016/j.physa.2005.01.001.

[7] W. Liu, K. Sun, and C. Zhu, "A fast image encryption algorithm based on chaotic map," *Opt. Lasers Eng.*, 2016, doi: 10.1016/j.optlaseng.2016.03.019.