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

IMAGE ENCRYPTION BY USING THE BLOCK SCRAMBLING: A REVIEW PAPER

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

Abstract

The pictures are now transferred via open networks that are subject to possible attacks, so the sharing of image data in many areas, such as medical, military, banking, etc., requires additional protection. In preventing the system from brute force and differential attacks, safety factors are important. Although using chaotic maps and simple encryption techniques, such as block scrambling, modified zigzag transformation for encryption phases, including permutation, diffusion, and key stream generation, we propose an Enhanced Logistic Map (ELM) to withstand attacks. While using the histogram, correlation analysis, Number of Pixel Change Rate (NPCR), Unified Average Change Intensity (UACI), Peak-Signal-to-Noise Ratio (PSNR), and entropy, the encryption results are evaluated. The safety, reliability, performance, and versatility of the proposed method are demonstrated by our results.

Keywords: *Network, Number of Pixel Change Rate (NPCR), Peak-Signal-to-Noise Ratio (PSNR), Unified Average Change Intensity (UACI),*

I. INTRODUCTION

Recently, the growing use of the internet and networking media has rapidly increased image encryption [1]. However, conventional encryption algorithms, such as the data encryption standard (DES), the foreign data encryption algorithm (IDES) and the advanced encryption standard (AES), are not appropriate for realistic image encryption because of the data size and high redundancy between the pixels of a digital image [2]. Chaos is characterized by periodicity, ergodicity, pseudo-randomness, and elevated initial conditions and parameter sensitivity [3].

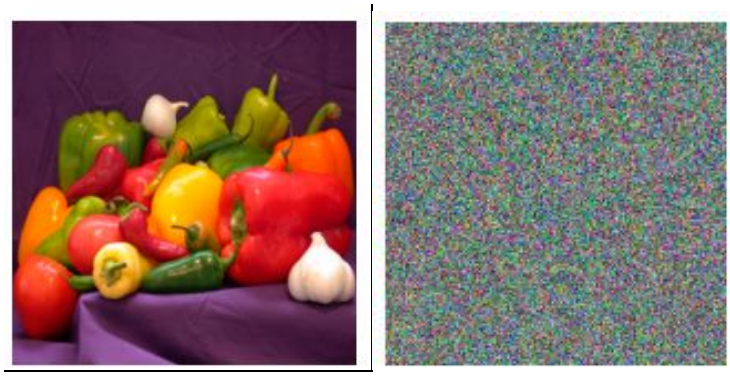

Fig. 1: Illustrates the Real Images and Encrypted Images.

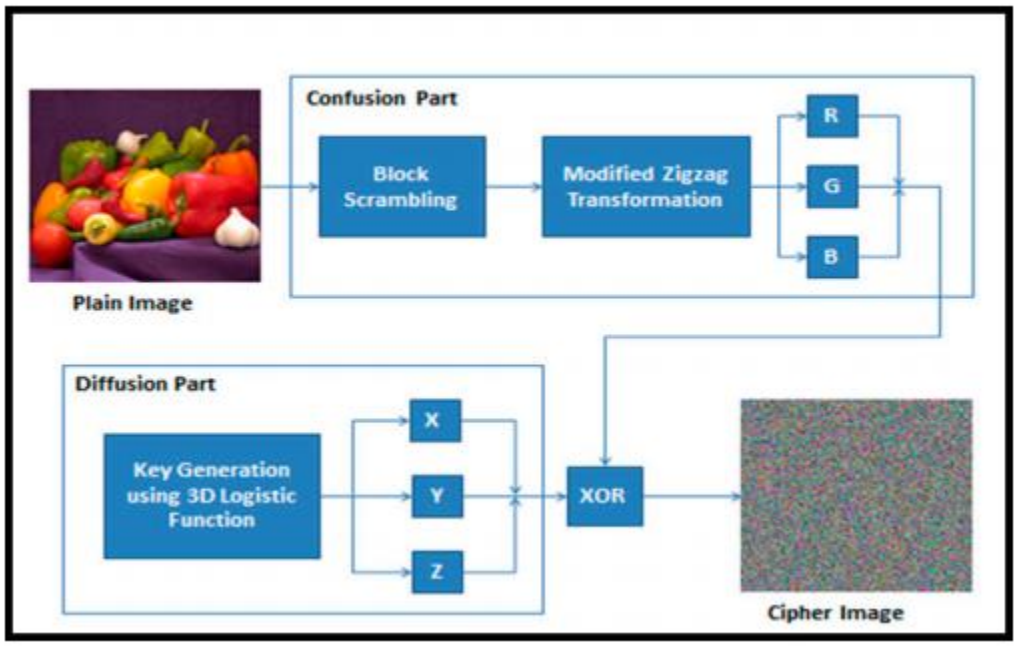

Fig. 2: Illustrates the flow chart of the encryption scheme procedure [2]

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

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

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

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

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

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

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

Another critical constraint is the correlation coefficient to ensure that the encryption algorithm is very accurate. The expression is given below [4].

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

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

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

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

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

II. LITERATURE REVIEW

John et al suggested a new encryption algorithm for image cryptosystems. In two ways, the characteristics of text data and image data differ greatly. One difference is that the size of the image data is usually much bigger than that of text data. The other is that plain data never enables loss when a compression method is used, but image information does. In this paper, we are developing an efficient cryptosystem for images. Our approach is based on vector quantization, which is one of the traditional image compression techniques. Via our approach, the following two goals can be accomplished. One aim is to build a cryptosystem with an image of high security. The other aim is to lower the calculation complexity of the encryption and decryption algorithms [6].

III. DISCUSSION AND CONCLUSION

We introduced a method of image encryption which is based on a chaotic map with a new system of symmetric key generation. The scheme uses Block Scrambling and Modified Zigzag Transformation, while the improved logistic-tent map uses key generation. Pixel shuffling achieves uncertainty and diffusion. It gives priority to resisting the proposed algorithm's brute-force attack. The experimental results revealed that the method proposed produced the encrypted images in pixel histograms with uniform distribution. In addition, the suggested algorithm has shown that data entropy is close to 8 in the encrypted images. It can resist selected/known plaintext attacks robustly, is resistant to salt and pepper noise, and can withstand an occlusion attack of up to 50 percent. Comparison experiments with other recent algorithms were carried out. The results of the statistical testing suggest that file encryption/decryption protection can be supported by the new pseudo-random bit combiner. Based on the study of the proposed method, we argue that the method is stable and computer-efficient. The algorithm proposed is simple, fast, and has a strong practical value for application.

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] M. Bani Younes and A. Jantan, “Image Encrytion Using Block Based Transformation Algorithm,” *IAENG Int. J. Comput. Sci.*, 2008.

[3] 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.

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

[6] J. M. Justin, “A Survey on Various Encryption Techniques,” *Int. J. Soft Comput. Eng.*, 2012.