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

IMAGE ENCRYPTION BY USING THE OPTIMIZED SUBSTITUTION BOX: A REVIEW ARTICLE

M S Sowmya
Faculty of Engineering and Technology,
Jain (Deemed-to-be University), Ramnagar District, Karnataka - 562112
Email Id: ms.sowmya@jainuniversity.ac.in.

Abstract

This paper introduces a modern hybrid chaotic map and a different way to enhance the efficiency of encryption algorithms by using optimization techniques. The suggested chaotic map establishes an outstanding efficiency and sensitivity to randomness compared to other chaotic functions. The characteristics of the new mathematical function are better than those of classical maps on the basis of its Lyapunov exponents and entropy index. We suggest a new image cypher based on the Shannon properties of confusion/diffusion. The replacement step of the proposed encryption algorithm, which relies on a new optimized replacement box, was carried out to generate S-boxes according to their nonlinearity score via the chaotic Jaya optimization algorithm. The purpose of the optimization process is to have a high nonlinearity rating bijective matrix.

Keywords: *Chaotic Map, Communication, Multimedia, Technology, Cypher, Optimization techniques.*

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].

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

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

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

Figure 1: Illustrates the general schematic system prototypical for the picture encryption.

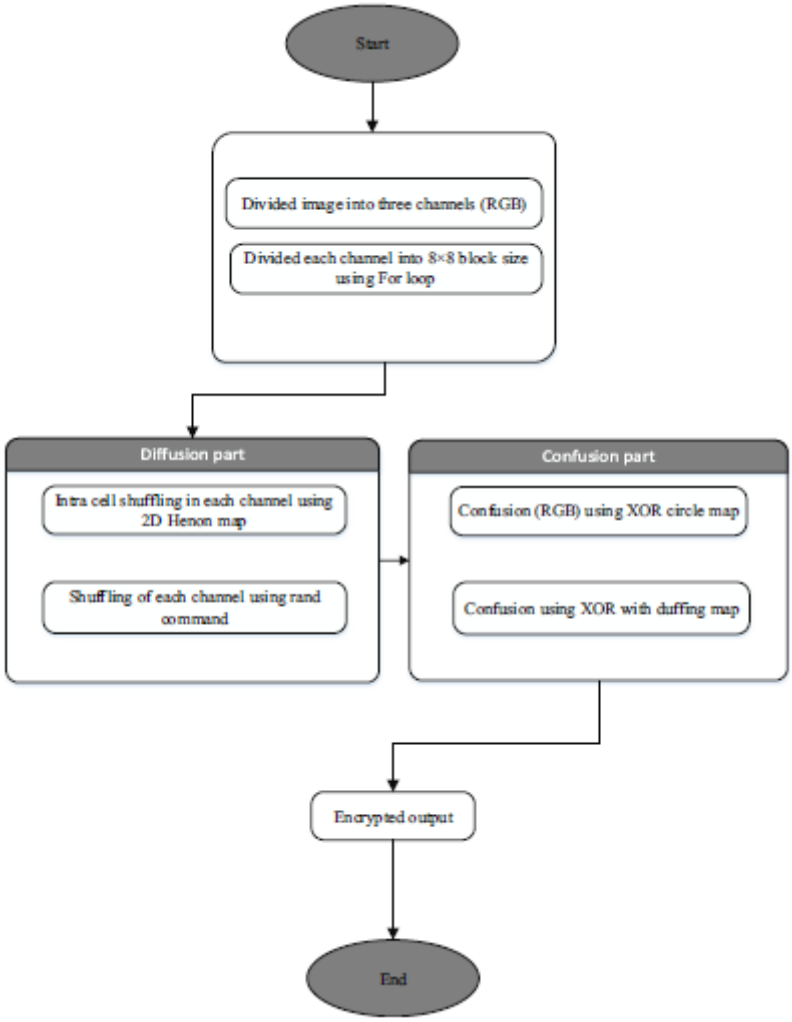

Figure 2: Illustrates the outline of the proposed method

Figure 1: Illustrates the general schematic system prototypical for the picture encryption. Figure 2: Illustrates the outline of the proposed method [3].

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

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

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

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

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

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

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

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

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].

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

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

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

II. LITERATURE REVIEW

Khan et al. investigated a novel chaotic image encryption technique based on many discrete dynamical maps. One of the most critical aspects of the technologically advanced era is the dissemination of information over an unreliable communication channel. In the form of binary bits, electronic knowledge moves. One of the most critical issues in today's world is the privacy of such digital content. We have used several messy iterative maps in this article to suggest a novel technique of image encryption. Confusion and diffusion in the provided method were applied to the proposed encryption, which is one of the most fundamental aspects of the encryption technique. We have checked and compared our anticipated method with current findings against various performance analysis. The developed scheme is capable of providing an excellent privacy to digital images.

III. DISCUSSION AND CONCLUSION

We suggested a new hybrid chaotic function in this paper by merging various 1D maps. Based on its Lyapunov exponents and entropy variance, the robustness of the proposed

technique was proved. Based on optimized Sbox and dynamic keys, we presented an encryption algorithm. The S-boxes used in the permutation phase of our cryptosystem were created. The proposed encryption algorithm has outstanding performance in terms of complexity and time speed and can withstand numerous attacks: twelve steps demonstrated the performance of the proposed method that can be used to protect private networks and applications for web protection. By researching the effect of changing the chaotic position on robustness and protection, our approach could be strengthened. By evaluating the management of the keys in various protocols, a further development of our algorithm could be envisaged. In short, before implementing the encryption scheme on the hardware, the suggested solution could be strengthened.

IV. REFERENCES

[1] [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. 2016.

[3] J. Ahmad and S. O. Hwang, "Chaos-based diffusion for highly autocorrelated data in encryption algorithms," Nonlinear Dyn., 2015, doi: 10.1007/s11071-015-2281-0.

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

[5] 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.