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

Image Encryption by Applying Double Chaotic S-Boxes: A Comprehensive Review

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

Abstract

A novel chaotic S-box based image encryption scheme is proposed to enhance the security and efficiency of image encryption schemes comprehensively. First, to expand the chaotic spectrum and enhance the chaotic efficiency of 1D discrete chaotic maps, a new compound chaotic system, the Sine-Tent map, is proposed. As a consequence, for cryptosystems, the current compound chaotic method is more fitting. Secondly, an effective and easy method is proposed to produce S-boxes that can significantly improve the efficiency of the output of S-boxes. Thirdly, a novel image encryption algorithm based on double S-box is proposed. The proposed cryptosystem can avoid the four classical types of attacks by adding identical key sequences {r, t} linked to image cypher text, which is an advantage over other S-box based encryption schemes. In addition, two rounds of forward and backward confusion-diffusion operation with double S-boxes increased the system's resistance to differential analysis attack. The results of the simulation and the security review check the feasibility of the scheme proposed. The new scheme has clear efficiency benefits, which means that in real-time image Encryption It Has Greater Application Potential.

Keywords: *Encrypted images, Image Encryption, Network Communication, Real Images.*

I. INTRODUCTION

With the rapid growth of network communication, image encryption in the area of image processing and information security has become a research hotspot [1]. Since image data has the characteristics of large quantities of data, good redundancy and high correlation between adjacent pixels, image encryption algorithms not only require high protection, but also fast encryption speed. If the encryption speed is poor, because of the large amount of picture data, the time spent would be too long. Security and efficiency should be considered comprehensively for encrypting multimedia information with large volumes of data [2].

Fig. 1: Illustrates the Real Images and Encrypted Images

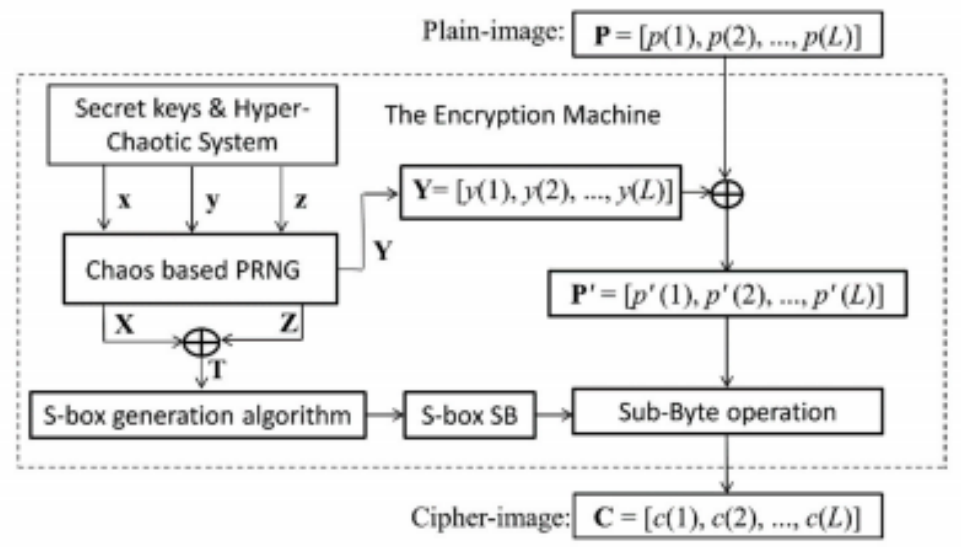

Fig. 2: Illustrates the flow chart of the encryption scheme procedure [3]

A strong diffusion mechanism is implemented in the proposed encryption algorithm to resist the differential cryptanalysis attack triggered by the opponent. As a consequence, the cypher text is vulnerable to the noise of the transmission channel, so noise and occlusion robustness is lacking in the algorithm [4]. The lack of such robustness, however, often renders it difficult for the opponent to correctly decode the plaintext, which can guarantee that the image content's confidentiality is preserved [5].

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

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

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

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

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

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

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

Another critical constraint is the correlation coefficient to ensure that the encryption algorithm is very accurate. The expression is given below [2].

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

Where $C(x,y), D(x)$ and $D(y)$ may be evaluated by utilizing the following equations [6].

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

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

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

II. LITERATURE REVIEW

For image cryptosystems, Ziad et al. proposed a new encryption algorithm. The features of text data and image data vary significantly in two respects. One distinction is that the image data size

is typically much larger than that of text data. The other is that when a compression method is used, plain data never allows for loss, but image information does. We are designing an effective cryptosystem for images in this paper. Our method is based on the quantization of vectors, which is one of the conventional techniques for image compression. Via our plan, the following two objectives can be achieved. One purpose is to create a cryptosystem with a high-security picture. The other aim is to lower the encryption and decryption algorithms' calculation complexity [7].

III. DISCUSSION AND CONCLUSION

An effective and stable image encryption scheme is introduced in this paper. This paper's key contributions are as follows: First, a new compound chaotic system is proposed, the Sine-Tent map, which has a wider chaotic range and better chaotic efficiency than any of the old ones. And for cryptosystems, the current compound chaotic method is more fitting. Second, an effective and safe technique for manufacturing S-boxes is suggested, which has less execution time than the other ones. Third, a novel image encryption algorithm based on double S-boxes is suggested. The proposed cryptosystem can avoid the four classical types of attacks by adding identical key sequences {r, t} linked to image cypher text, which is an advantage over other S-box based encryption schemes. It overcomes the security vulnerabilities of some old encryption algorithms based on S-boxes. Furthermore, the sensitivity of the algorithm is enhanced by two rounds of forward and backward confusion-diffusion operation. The results of the simulation and the security review check the feasibility of the scheme proposed. The new scheme has clear efficiency benefits, which means that in real-time image encryption it has greater application potential. By linking three colour channels of colour images to grey images, the proposed scheme is also suitable for colour images.

IV. REFERENCES

[1] C. C. Chang, M. S. Hwang, and T. S. Chen, “A new encryption algorithm for image cryptosystems,” *J. Syst. Softw.*, 2001, doi: 10.1016/S0164-1212(01)00029-2.

[2] 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.

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

[4] M. Kumari, S. Gupta, and P. Sardana, “A Survey of Image Encryption Algorithms,” *3D Res.*, 2017, doi: 10.1007/s13319-017-0148-5.

[5] K. Muhammad, J. Ahmad, N. U. Rehman, Z. Jan, and M. Sajjad, “CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method,” *Multimed. Tools Appl.*, 2017, doi: 10.1007/s11042-016-3383-5.

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

[7] Z. E. Dawahdeh, S. N. Yaakob, and R. Razif bin Othman, "A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher," *J. King Saud Univ. - Comput. Inf. Sci.*, 2018, doi: 10.1016/j.jksuci.2017.06.004.