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

INVESTIGATION OF A NEW DIGITAL PICTURE ENCRYPTION ALGORITHM: A STATE OF THE ART SURVEY

Dr. A. Vijay Kumar
Faculty of Engineering and Technology,
Jain (Deemed-to-be University), Ramnagar District, Karnataka – 562112
Email Id: ak.vijay@jainuniversity.ac.in

Abstract

A new image encryption scheme using a 144-bit secret key is introduced in this paper. The image is divided into blocks and subsequently into colour components in the scheme replacement process. By conducting bitwise operations, each colour component is changed based on the secret key as well as a few most essential bits of its previous and next colour component. Three rounds are taken to complete the process of substitution. A feedback mechanism is also implemented to make the cypher more stable by changing the secret key used after each block is encrypted. In addition, the resulting image is partitioned into several dynamic sub-images based on the key. Each sub-image uses a created magic square matrix to move through the scrambling process where sub-image pixels are reshuffled within themselves. For the scrambling process, five rounds are taken. The proposed system is straightforward, quick and sensitive to the secret key. Popular attacks such as linear and differential cryptanalysis are infeasible due to the high order of substitution and permutation. The experimental results indicate that the encryption approach proposed is effective and has strong security characteristics.

Keywords: *Digital Data, Image Encryption, Image, Information Technology, Bitwise operation.*

I. INTRODUCTION

A massive amount of digital data is being shared over unsecured platforms with the exponential growth of computer networks and developments in information technology. A large part of the information exchanged, whether confidential or private, requires security mechanisms to provide the protection needed [1]. During the storage and transmission of digital data, protection has therefore become a significant concern [2].

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

Fig. 1: Illustrates the Real Images and Encrypted Images

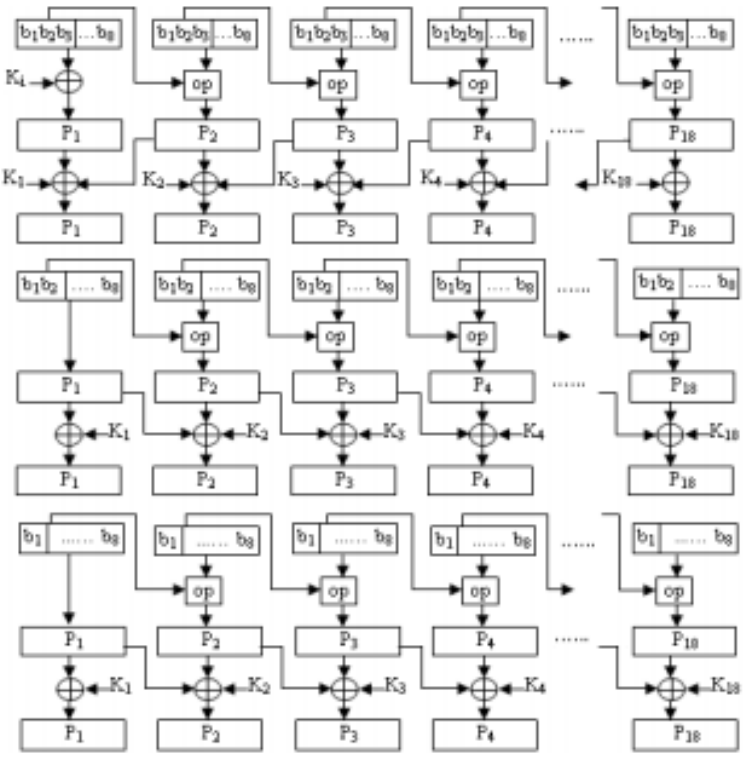

Fig. 2: Illustrates the encryption scheme procedure

To evaluate the similarity between adjacent pixels before and after the encryption, we select the vertical and horizontal directions of the plain image and its ciphered image and randomly choose 3000 pairs of adjacent pixels in the opposite angle direction. It adopts the resulting formulas [3].

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

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

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

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

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

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

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

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

A survey was carried out by Li et al. on different encryption methods. This paper focuses mainly on the various forms of current encryption techniques and frames all the techniques together as a

literature review. The aim is a thorough experimental analysis of the implementation of different encryption techniques that are usable. It also focuses on techniques for image encryption, information encryption techniques, double encryption, and encryption techniques based on Chaos. This research covers the performance standards used in encryption processes and explores their safety issues [6].

III. DISCUSSION AND CONCLUSION

This paper introduces a new encryption algorithm based on a hyper-chaotic fractional-order method that can effectively improve the security of the cryptosystem. In detail, the scheme is defined. Security tests are performed to check the security of the proposed encryption scheme, including correlation analysis, histogram analysis, and key sensitivity analysis. The experimental results indicate that there is high security in the encryption algorithm. Chaos results from nonlinear deterministic schemes. Chaotic systems have many intrinsic attributes, such as extreme vulnerability to original conditions, broadband power range, and random-like behaviors, as is well known. Chaos has been applied to a number of disciplines due to the aforementioned features, and the most promising use of chaos is in safe communication. A variety of researchers have suggested several methods of image encryption based on chaotic structures in recent years.

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] F. Walter, G. Li, C. Meier, S. Zhang, and T. Zentgraf, “Ultrathin Nonlinear Metasurface for Optical Image Encoding,” *Nano Lett.*, 2017, doi: 10.1021/acs.nanolett.7b00676.

[3] E. Setyaningsih and R. Wardoyo, “Review of Image Compression and Encryption Techniques,” *Int. J. Adv. Comput. Sci. Appl.*, 2017, doi: 10.14569/ijacsa.2017.080212.

[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] 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.

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