Journal of The Gujarat Research Society

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

IMAGE ENCRYPTION FOR SECURE DATA TRANSMISSION BY APPLYING BIT-PLANE MATRIX ROTATION

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

Abstract

In this study, we are proposing a new algorithm for image encryption based on bit-plane matrix rotation and two hyper chaotic systems. First, the algorithm decomposes the plain image into eight-bit planes and builds a matrix of three dimensions (3D). The sub-matrix of the 3D bit-plane matrix is then rotated in various directions regulated by a hyper-chaotic system-generated PRNS. Finally, by using another main stream, the pixel values of the intermediate image are changed. In addition, the MD5 hash function of the plain-image, which improves the connection between the encryption method and the plain-image, provides the initial diffusion values and parameters relevant to generating chaotic sequences. In terms of key space, histogram, information entropy, key sensitivity and adjacent pixel correlation index, simulation experiments are presented to analyze the image encryption scheme. Theoretical research and experimental results show that the algorithm proposed has outstanding performance and a sufficient level of protection.

Keywords: *Data, Encryption, Internet, Image, Multimedia, Date protection, Safety issues.*

I. INTRODUCTION

With the rapid growth of multimedia technologies and the popularity of the Internet, intense attention has been paid to the protection of image transmission [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. Chaos is characterized by periodicity, ergodicity, pseudo-randomness, and elevated initial conditions and parameter sensitivity [2].

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

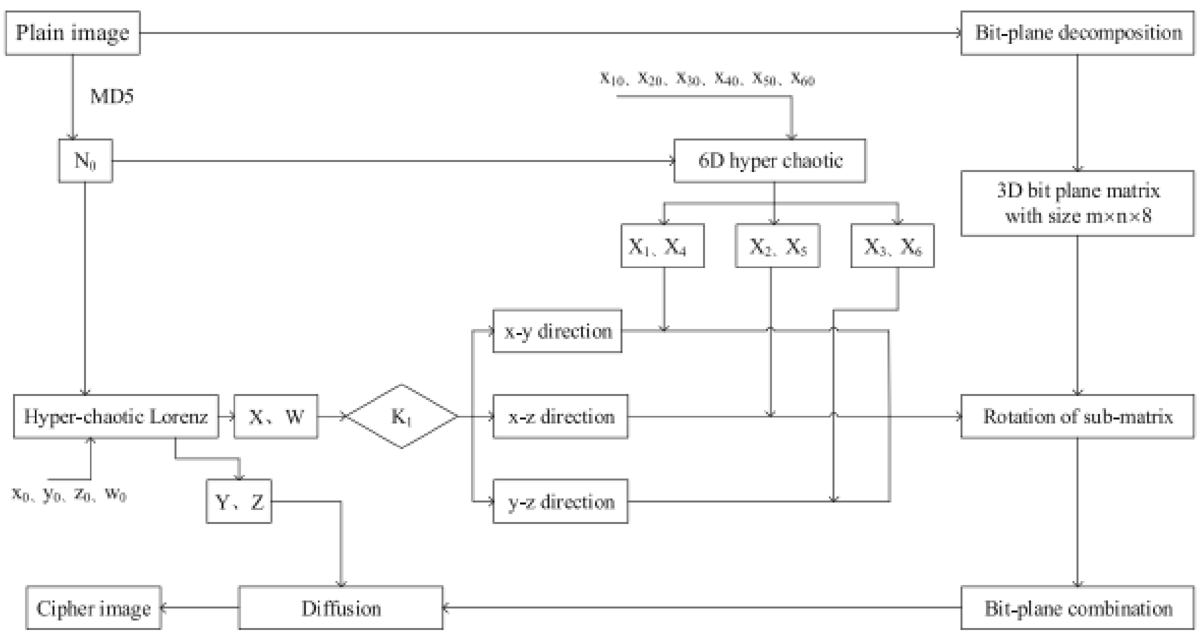

Fig. 2: Illustrates the flow chart of the encryption scheme procedure [3]

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

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

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

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

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

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

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

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 new encryption algorithm for image cryptosystems was proposed by Chang et al. The characteristics of text data and image data vary greatly 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 technique is used, plain data seldom allows loss, but image information does. We develop an effective cryptosystem for images in this paper. Our approach is based on the quantization of vectors, which is one of the common techniques of image compression. The following two targets can be attained through our methodology. One purpose is to design a cryptosystem with a high

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

security picture. The other objective is to reduce the encryption and decryption algorithms' calculation complexity [6].

III. DISCUSSION AND CONCLUSION

A novel image encryption algorithm is proposed in this paper using bit-plane matrix rotation and hyper chaotic systems. We first transform the plain-image into eight bit-planes in the cryptosystem. Then, a method of bit-plane matrix rotation is implemented. The method scrambles bits efficiently with PRNS created by the hyper chaotic systems in the bit-plane matrix. Besides, to get some parameters used in the encryption process, the MD5 hash value of the plain-image is used. Therefore, the algorithm has a clear link to the plain image. The results of simulation and performance tests both indicate that the proposed algorithm is extremely secure from converntial attacks.

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] 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.

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

[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.[7]

[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. 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.