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

A NOISE-RESISTIVE PICTURE ENCRYPTION BY APPLYING DNA SEQUENCE OPERATION

Mathiyalagan R
Faculty of Engineering and Technology, Jain (Deemed-to-be University), Ramnagar District, Karnataka – 562112
Email Id: r.mathiyalagan@jainuniversity.ac.in

Abstract

Using the combination of chaos, hyper-chaos, and DNA sequence operation, this paper proposes an image encryption method. Three phases of encryption operations are carried out by the suggested method. Such are selection-level hyper-chaotic DNA-shuffling operation based on sequence, key-image-based DNA-diffusion operation, and DNA-shuffling operation based on hyper-chaotic sequence. The benefits of this scheme are higher key space, higher uncertainty or randomness of pixels, higher sensitivity to the keys and plaintext pixels, greater resistivity to the noises, and lossless encryption and decryption. In addition, the selection-level hyper-chaotic DNA-shuffling operation based on sequence produces more complexities in the process of uncertainty that increases the strength of encryptions and decryptions. The computer simulation and security tests confirm the good results of the proposed system's encryption results and high resistivity to the attacks commonly used

Keywords: *Shuffling operation, Encryption, AES, DNA, DES, Picture, RSA, Data protection.*

I. INTRODUCTION

With the rapid advancement in internet and multimedia technology, all cryptographic researchers are challenged by the security of transmitting large numbers of multimedia data, particularly image data over the internet. Many picture encryption strategies have been developed to meet the security challenge[1][2]. There are conventional encryption techniques such as Rivest-Shamir-Adleman (RSA), Advanced Encryption Standard (AES), Triple DES (3DES), Data Encryption Standard (DES), etc., but the encryption of images is not so effective. This is because images have data in bulk, high adjacent pixel similarity, high redundancy etc.

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

Figure 1: Illustrates the real and encrypted images [3]

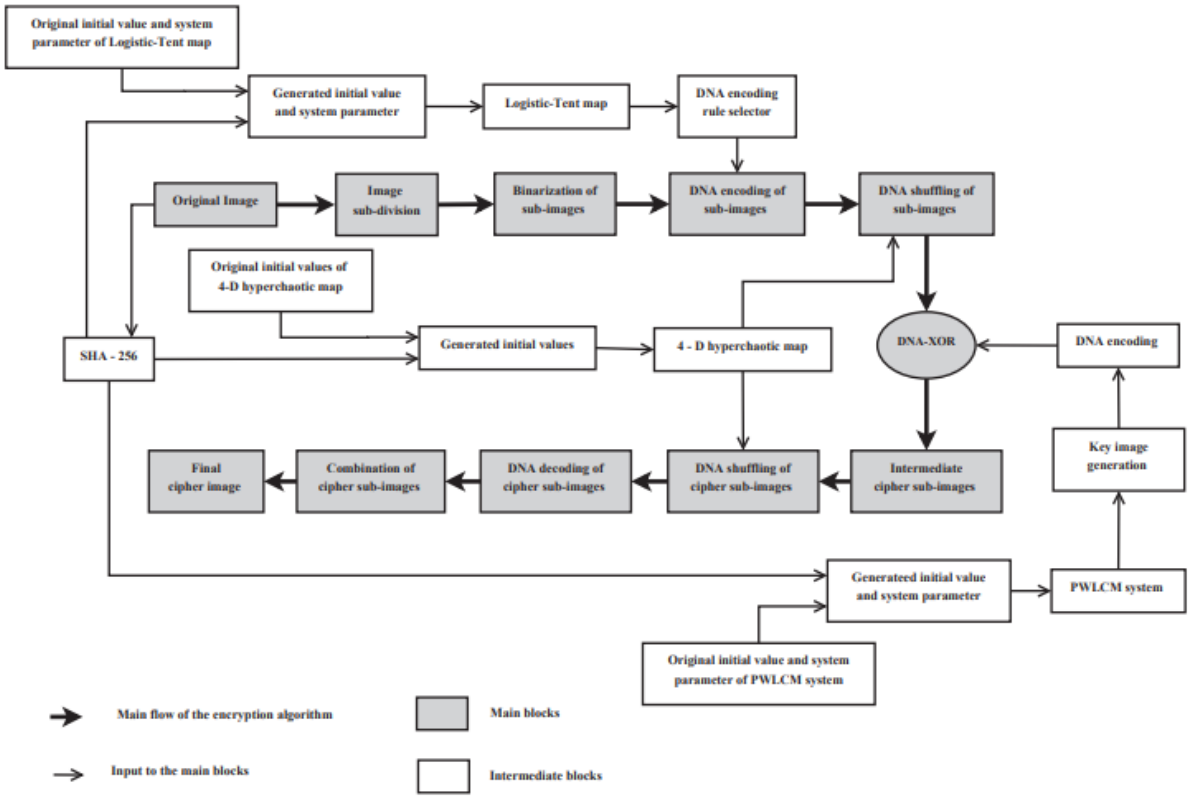

Figure 2: Illustrates the general schematic diagram of the encryption procedure

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

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

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

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

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

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

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

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

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

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

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].

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

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

II. LITERATURE REVIEW

A study based on chaotic sequences was carried out by Nasr et al. on different watermarking algorithms. Multiple digital watermarking techniques can address the problems of multiple copyright claims and preserve traces of digital products in the different phases of printing, sale and usage. In this paper, a multiple digital watermarking algorithm based on chaotic sequences is proposed. In the unpredictable sequences, there are the advantages of enormous, high security, and weakest correlation. Huge and independent digital watermark signals are generated by 1-D chaotic charts, which are determined by various initial conditions and parameters [6].

III. DISCUSSION AND CONCLUSION

This paper uses the combination of chaotic and hyper-chaotic maps to suggest a DNA sequence operation-based image encryption method. To complete the encryption process, the proposed system performs two-fold hyper-chaotic map-based DNA shuffling operations and one-time DNA-XOR-based diffusion operations. The first operation of DNA-shuffling is based on hyper-chaotic sequences at the selection stage. The results of the simulation and safety analyses show that the proposed algorithm has a good encryption effect, broad secret key space, strong statistical attack resistivity, differential attack, entropy attack, high key sensitivity, resists known plaintext and selected plaintext attacks, and resists noise attacks strongly. The comparison results show that, compared to the other schemes mentioned, the proposed algorithm is more stable. All these features show that the proposed algorithm is secure and suitable for image encryption.

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] S. Kumar, A. Gupta, and A. Arya, Triple Frequency S-Shaped Circularly Polarized Microstrip Antenna with Small Frequency-Ratio. 2016.

[3] L. Sui, K. Duan, and J. Liang, "A secure double-image sharing scheme based on Shamir's three-pass protocol and 2D Sine Logistic modulation map in discrete multiple-parameter fractional angular transform domain," Opt. Lasers Eng., 2016, doi: 10.1016/j.optlaseng.2015.12.016.

[4] M. Ahmad, B. Alam, A. Jain, and V. Khare, "A novel octuple images encryption algorithm using chaos in wavelet domain," 2013, doi: 10.1007/978-1-4614-6154-8_50.

[5] Z. Zhong, H. Qin, L. Liu, Y. Zhang, and M. Shan, "Silhouette-free image encryption using interference in the multiple-parameter fractional Fourier transform domain," Opt. Express, 2017, doi: 10.1364/oe.25.006974.

[6] A. R. Elshazly, M. M. Fouad, and M. E. Nasr, "Secure and robust high quality DWT domain audio watermarking algorithm with binary image," 2012, doi: 10.1109/ICCES.2012.6408514.