International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/IJSRCSEIT

Gray-Scale Image Encryption Using DNA Operations

*1 M Sravanthi,2 B Bhavana, 3 B Keerthana

[1]Assistant Professor, Department of Information Technology, Bhoj Reddy Engineering College for Women, Hyderabad, India

[2,3]Students, Department of Information Technology, Bhoj Reddy Engineering College for Women, Hyderabad, India

ARTICLEINFO

Article History:

Accepted: 10 April 2023
Published: 30 April 2023

Publication Issue
Volume 9, Issue 2
March-April-2023

Page Number
680-684

ABSTRACT

In recent days, DNA cryptography is gaining more popularity for providing better security to image and text data. This paper presents a DNA based cryptographic solution for image and textual information. Image encryption involves scrambling at pixel and bit levels based on hyperchaotic sequences. Both image and text encryption involves basic DNA encoding rules, key combination, and conversion of data into binary and other forms. This new DNA cryptographic approach adds more dynamicity and randomness, making the cipher and keys harder to break. The proposed image encryption technique presents better results for various parameters, like Image Histogram, Correlation co-efficient, Information Entropy, Number of Pixels Change Rate (NPCR), and Unified Average Changing Intensity (UACI), Key Space, and Sensitivity compared with existing approaches. Improved time and space complexity, random key generation for text encryption prove that DNA cryptography can be a better security solution for new applications.

Keywords : DNA cryptography, image encryption, text encryption, DNA digital coding, DNA sequences

I. INTRODUCTION

Security is often a crucial necessity for sensitive data transmission over communication networks. Various security techniques used to provide information privacy bring benefits to an organization or individual businesses [1]. There exist many benchmarks symmetric and asymmetric cryptographic algorithms such as Advanced Encryption Standard (AES), IDEA (International Data Encryption Algorithm), and RSA (Proposed by Rivest, Shamir, and Adleman) to provide security to text data. But the survey provides evidence that these algorithms are not suitable for image encryption [2, 3]. Image data characteristics like pixel correlation, bulk space, and high redundancy among pixel values make image encryption more challenging compared to text encryption [3,10]. Image Encryption plays a vital role in secured multimedia communication but the existing symmetric and asymmetric algorithms suffer from side-channel attack, Brute Force attack, Differential attack, and other statistical attacks [4].

There is a marked lack of better image cryptographic system. The proposed DNA based image Cryptosystem makes use of chaotic sequences to overcome existing limitations of symmetric and asymmetric cryptographic systems along with its confusion and diffusion properties [3]. To bring dynamicity, better storage, and time complexity, high parallelism, and low power consumption Adleman introduced DNA computing in 1994, which makes DNA cryptography the right choice for today's Internet applications [5]. DNA computing is still an area of interest for many researchers for its massively parallel processing capabilities and high resistance to brute force attacks [6]. The existing image encryption standards and mathematical models combined with DNA cryptography show defects in terms of CPU time, memory consumption, and battery usage . The proposed DNA based approach for image encryption employs a chaotic sequence, which is deterministic and can produce a non-linear sequence [7]. It brings the advantages of unpredictability, pseudo randomness, and extremely sensitive to system control parameters and initial values [4, 7, 10]. Also, Chaos systems can eventually return to the original state from the proceeded state [8-10]. The proposed approach involves a sequence of steps, such as the use of five-dimensional hyperchaotic sequences that produce a strong ciphered image, scrambling at the pixel level and bit level. The analysis of various parameters like Image Histogram, Correlation coefficient, Information Entropy, NPCR, and UACI, Key Space, and Sensitivity shows that the proposed technique overcomes the limitations of the existing image encryption techniques.

This paper also presents DNA based text encryption technique, which is based on the motivation of Kerckhoff's principle, which states that secrecy of transmitted message depends on key during decryption and not on an algorithm for encryption and decryption. At a high level, the algorithm is secure if the cryptanalyst is unable to deduce the key to obtain plaintext from the corresponding ciphertext. This DNA based text encryption method uses the knowledge of random key generation to produce different sequences for the same input to achieve enhanced security performance. The proposed text encryption method outperforms the existing encryption techniques in terms of time and space complexities [11]. In this paper, Section 2 presents a preliminary study of the proposed approach; Section 3 covers image encryption in detail with result analysis. Section 4 discusses text encryption with two cases and time and space requirement analysis.

II. RELATED WORK

Traditional algorithms, including symmetric and asymmetric, are having many drawbacks concerning the exchange or use of a key. Compared to these, DNA cryptography can provide multifold security. It provides an enriched security level. Conventional block cipher algorithms are not suitable for secured multimedia communication over public networks [2, 9]. On the other hand, DNA cryptography is gaining more attention with a variation of chaos-based substitution permutation architecture [8]. It can run with lesser memory and reduced computational overhead when compared with other standards like Elliptic Curve Cryptography, Packet wavelet, Fourier transform, Cellular automata, etc. [3, 8]. The chaos method combined with DNA cryptography proved secure against a chosen-plaintext attack and differential attacks based on the previous studies [3]. Boriga et al. proposed a 1D chaotic image encryption map that would be found weaker. As there is a single variable is used, which makes easy prediction of initial values. Fidrich proposed use of 2D chaotic maps proved better diffusion properties. But, the use of a limited key space makes it easy to decode. Chen et al. proposed 3D chaotic maps proved better confusion and diffusion properties. Chen et al. presented a high complex 4D hyperchaotic system that brought many security advantages. However, lower dimensional chaotic systems can be crackable as computer machines having limited precision. Understandably, only a portion of plaintext or ciphertext will help to get the key back. Hence these are weaker against differential attacks. The following are the demerits of previous works identified:

 Low dimensional chaos methods face difficulty in providing high security.

 Existing image encryption techniques work well only for a homogeneous image dataset, like medical or satellite images.

 There is no such practically used chaos-based DNA cryptography that exists worldwide in different application areas [4].

A. Our Contributions

The following are the major contributions of this proposed work:

 Capable of encrypting and retrieving highly sensitive images those are heterogeneous. The main features of these images are continuity, the large volume of data, and the strong association of adjacent pixels.

 During image encryption, pixel-level and bit-level permutation will render stronger cipher, which is difficult for an attacker to crack.

 The use of a 5D hyperchaotic system can ensure enhanced complexity and hence able to achieve improved security.

 Both image and text encryptions are possible over a single framework with better CPU latency.

III. PROPOSED SYSTEM

Four basic processes are involved in DNA-based picture encryption algorithms:

(i) Using a chaotic sequence to scramble the image pixel position

(ii) The scrambled image matrix is encoded to the DNA sequence.

(iii) Using a chaotic sequence paired with add, subtract, EX-OR, complement, or combining operations to disrupt the DNA sequence matrix

(iv)Recombination and DNA decoding to acquire the encrypted image.

A block diagram of these processes is shown in fig. 1 and fig.2.

Encryption Scheme:

1) Before we begin the encryption strategy, we must first build the bit stream that will encrypt the image from the chaotic map: PWLCM. To construct the bit stream from the chaotic map, the user must give the initial parameters (u0, x0). We use this equation to ensure that values are between 0 and 255 after the bit stream has been generated: X1=$mod(floor(X \times 1014)$, 256) (2)

Let's say the image is P x Q pixels in size. Then we must iterate through (P x Q + N0) values. To avoid any invalid values in the stream, we discard the first N0. We decompose the values into bitplanes once we obtain them in integer form. The bitplanes b(0) ,b(1) ,b(2) ,b(3) ,b(4) ,b(5) , b(6), and b(7) are required. These bitplanes must be divided into two groups, b1 and b2, with higher bitplanes in one group and lower bitplanes in the other.

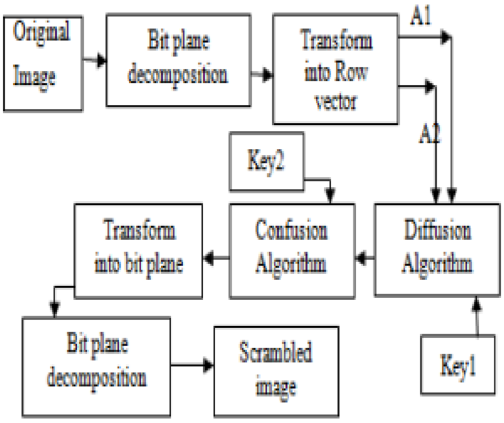

Fig 1: Block diagram

2) We read the image and decompose into bitplanes and form 2 groups A1 and A2.

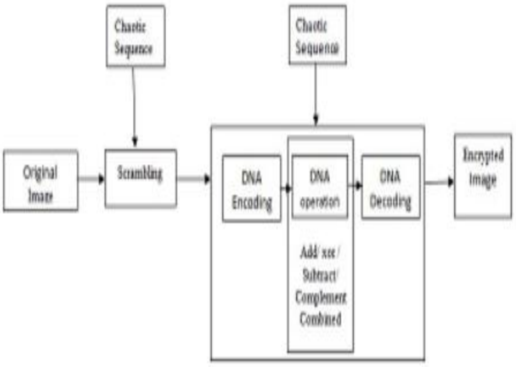

Fig 2: Block Diagram of proposed image encryption using DNA coding

A DNA chain is made up of 4 information-carrying nucleotides (A, C, G, and T). Encoding is the process of converting information into a DNA nucleotide chain. Decoding is the process of transforming a DNA nucleotide into information. Figure 2 depicts these processes.

Decryption scheme:

It is the reverse of the encryption scheme The substitution process uses this equation

$$R_i(j) = B_i(j - 1) \oplus B_i(j) \oplus (\lfloor S_k(i, j) \times 1010 \rfloor \mathrm{mod} 256) \quad (3)$$

IV. RESULTS

Experiments are conducted to test the suggested encryption framework's resistance against statistical, differential attacks. MATLAB R2014a is used to model the suggested framework. Encrypting a 256 x 256 picture with the proposed technique took 0.339571s. The scrambled image appears to be difficult to recognize, but only from a visual perspective. Here both grayscale image and rgb are scrambled and the results are shown in fig.3 to fig.6.

HISTOGRAM ANALYSIS:

In the histogram analysis, we obtain the histogram of the image which gives the intensity of the image over a spectrum. We check the histogram of the encrypted image to ensure that it is uniform the spectrum to avoid the attacker decrypting the image.

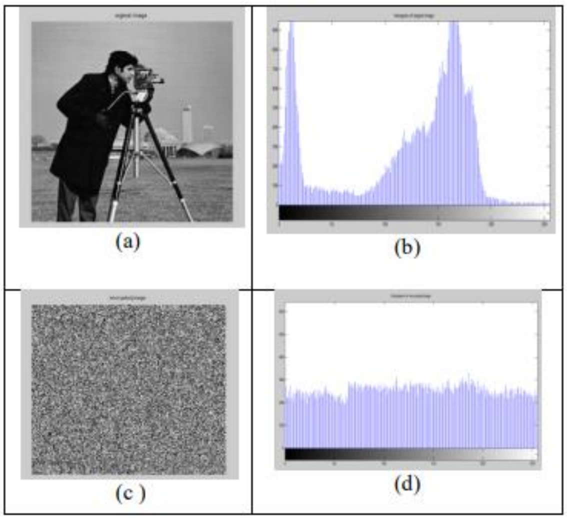

Fig 3(a) grayscale test image1(b)Histogram of test image (c) encrypted image (d)Histogram of encrypted image

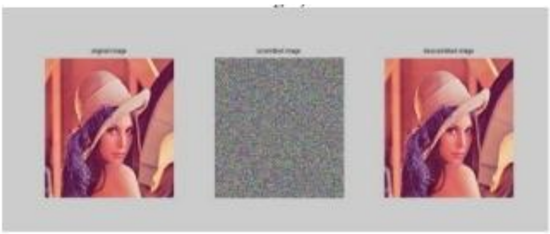

Fig 4. Original image, scrambled and descrambled RGB image((from left to right)

V. CONCLUSION

The input image is scrambled with the use of a piecewise linear chaotic map in the first stage of the proposed approach. To begin, we partition the original picture into two equal-sized binary sequences. The sequences are then put through a mutual diffusion process. The method successfully diffuses the two binary sequences, ensuring that even a minor change in the plain picture can modify a huge number of binary values in the cipher sequences. During the confusion phase, the PWLCM map, which can permute bits in one bit plane into any other bit plane, is employed to interchange binary elements between the two sequences. We can utilize more performance analysis methods in the future to establish that the suggested algorithm is secure and dependable for image encryption, such as correlation test, key space assessment, differential measurement, entropy evaluation, and sensitivity analysis.

VI. REFERENCES

[1]. Lima, J. B., Madeiro, F., & Sales, F. J. (2015). Encryption of medical images based on the cosine number transform. Signal Processing: Image Communication, 35, 1-8.

[2]. Peng, H., Tian, Y., Kurths, J., Li, L., Yang, Y., & Wang, D. (2017). Secure and energy-efficient data transmission system based on chaotic compressive sensing in body-to-body networks. IEEE transactions on biomedical circuits and systems, 11(3), 558-573.

[3]. Li, S., Li, C., Chen, G., Bourbakis, N. G., & Lo, K. T. (2008). A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. Signal Processing: Image Communication, 23(3), 212-223.

[4]. Xiang, T., Hu, J., & Sun, J. (2015). Outsourcing chaotic selective image encryption to the cloud with steganography. Digital Signal Processing, 43, 28-37.

[5]. Kiran, P. and Parameshachari, B.D., 2022. Resource Optimized Selective Image Encryption of Medical Images Using Multiple Chaotic Systems. Microprocessors and Microsystems, 91, p.104546.

[6]. Cui, H., Yuan, X., & Wang, C. (2016). Harnessing encrypted data in cloud for secure and efficient mobile image sharing. IEEE Transactions on Mobile Computing, 16(5), 1315-1329.

[7]. El-Bakary, E. M., El-Rabaie, E. S. M., Zahran, O., & E Abd El-Samie, F. (2017). DRPE encryption with chaotic interleaving for video communication. Wireless Personal Communications, 97(1), 1373- 1384.

[8]. Wang, W., Peng, D., Wang, H., Sharif, H., & Chen, H. H. (2007). Energy-constrained quality optimization for secure image transmission in wireless sensor networks. Advances in Multimedia, 2007.

[9]. Chen, R. J., Sun, Y. L., & He, D. (2012). Video encryption based on generalized cat mapping and h. 264. Internet Things Technol, 1, 017.

[10]. Nagy, G., Seth, S., & Einspahr, K. (1987). Decoding substitution ciphers by means of word matching with application to OCR. IEEE Transactions on Pattern Analysis and Machine Intelligence, (5), 710-715.

[11]. Wang, X., & Zhang, H. L. (2015). A color image encryption with heterogeneous bit-permutation and correlated chaos. Optics Communications, 342, 51-60.

[12]. Zhou, Y., Cao, W., & Chen, C. P. (2014). Image encryption using binary bitplane. Signal processing, 100, 197-207.

[13]. Naskar, P. K., Bhattacharyya, S., Mahatab, K. C., Dhal, K. G., & Chaudhuri, A. (2021). An efficient block-level image encryption scheme based on multi-chaotic maps with DNA encoding. Nonlinear Dynamics, 105(4), 3673-3698.

[14]. Yang, Z., Yuan, S., Li, J., Bai, X., Yu, Z., & Zhou, X. (2022). An encryption method based on computational ghost imaging with chaotic mapping and DNA encoding. Journal of Optics, 24(6), 065702.

[15]. Pai, A., Pareek, P. K., Guru Prasad, M. S., Singh, P., & Deshpande, B. K. (2021). Image Encryption Method by Using Chaotic Map and DNA Encoding. NVEO-NATURAL VOLATILES & ESSENTIAL OILS Journal| NVEO, 10391-10400.

Cite this article as :

M Sravanthi, B Bhvana, B Keerthana, "Gray-Scale Image Encryption Using DNA Operations", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 2, pp.680-684, March-April-2023.