Image Encryption using Chaotic Maps and DNA Encoding

Nitya Ranjan Manihira
Dept. Of Electronics and Comm. Engg.
Sambalpur University Institute of Information Technology
Burla, Odisha, India

Alpesh Kumar Dauda
Dept. of Electronics and Comm.Engg.
Sambalpur University Institute of Information Technology
Burla, Odisha, India

***Abstract*—Image is used as a key component in information sharing in today's world technology. Security of image at risk while transmitting hence image encryption is needed. In cryptography chaotic maps play a vital role in making encryption strong and effective. Optimal DNA combined with chaotic map make an effective encryption technique. A couple of image encryption algorithms using chaos have recently been developed at the pixel level, but little study has been done at the bit level. With only one round, the suggested technique provides excellent encryption performance. The suggested approach for image encryption is both secure and dependable, according to simulation findings and performance. We exposed the flaws in previous research as well as potential directions for enhancing image encryption systems based on DNA coding and chaotic maps.**

Keywords - Digital Image Encryption; Chaotic maps; DNA coding

I. INTRODUCTION

With the development of social network and smart phone image become a vital part of the day to day life. Image is being used as a communication tool among users. Users send sensitive photos over internet. Digital image has become increasingly pervasive over the time. Due to the open nature of the medium the security of image being transmitted subjected to potential threats. The attacker can easily access the transmitting unauthorized image. To prevent this the technique used to hide information of the original image in some form is known as encryption .In field like medical treatment, commerce, military affairs digital image need to meet the highest level of confidentiality. Image encryption technology has become popular to protect the transmitting image effectively. Conventional encryption algorithms such as DES, IDEA, and AES may not be ideal for image encryption due to the bulk of the data and considerable redundancy among the raw pixels of the digital image. To avoid visual information leaks, a new image encryption algorithm based on chaos theory, random grid, compressed sensing, and DNA coding has been presented [1-3].

Chaotic encryption techniques have recently gotten a lot of interest. Simple implementation, robustness, rapid encryption, and good security are all advantages of the chaotic encryption technique. Because photos contain a significant degree of pixel correlation, designing an efficient image encryption technique is difficult. As a result, existing encryption methods may perform badly when the patterns of the input and encrypted images are identical. As a result, chaotic systems are extensively used to develop secret keys in the field of picture encryption. To obtain the encrypted photos, these security keys are employed to dilute and confuse the input images. The permutation operation is used to modify the pixel positions of an input image. An input image's pixel values are changed using the diffusion process. Bases of DNA nucleotides DNA computing uses Adenine (A), Guanine (G), Cytosine (C) and Thymine (T) coding sequences as information carriers; it has substantial advantages in terms of large capacity for storage, parallelism, and energy usage [4-9]. We employ DNA coding to transmit image data and combine chaotic mapping with other DNA coding methods to create an acceptable and effective encryption algorithm.

Periodicity, ergodicity, and pseudo-randomness are all great intrinsic aspects of chaotic systems, as is their sensitive to primary condition and control parameter. Researchers have considered using chaotic systems for image encryption because of these qualities. A variety of bits-level image encryption techniques have been developed due to the benefit of bits-level permutations, which can alter the location and value of a pixel at the same time. The logistic map's parameter exhibits periodic window in it's bifurcation diagram, indicating that the logistic map's key stream, which is formed from chaotic sequences, is vulnerable.

Researchers frequently increase the performance of encryption algorithms by changing DNA encoding-decoding methods and procedures, according to the literature. Past study only make use of DNA coding method, a DNA coding operations i.e. add, subtract, complement, XOR, etc. or a mixture of several coding operations to produce image encryption without thoroughly comparing or studying the methods or procedures. To put it another way, no existing study explains why an explicit DNA coding whether it is fixed or dynamic method, DNA operation, or a mix of various coding operations was chosen to achieve image encryption.

To address the aforementioned issues, based on cyclic shift, flipping, and PWLCM chaotic maps, this work established a bit-level picture encryption technique. In its bifurcation diagrams, the PWLCM process presents a uniform symmetric distribution, high ergodicity, and very few periodic windows. To account for these traits, the proposed technique employs PWLCM chaotic maps. The proposed method can also encrypt an image with a size of P * Q pixels (test image size is 256 x 256). The basic image is split into two binary sequences of equal size using the bit plane decomposition method before diffusion and confusion. A mutual diffusion method between the sequences is applied during the diffusion phase.

The method successfully diffuses these binary sequences, ensuring that even minor changes to the plain picture have a big impact on the cipher sequences' binary values. The binary elements are exchanged between the two sequences during the

confusion phase using the PWLCM map, which may permute bits from one bit-plane into any other bit-plane.

Furthermore, because the proposed confusion algorithm is tightly tied to both sequences, the cryptosystem can successfully survive differential attacks.

According on experimental and simulation results, the proposed system can do outstanding encryption performance with one round only, despite many current bit-level picture encryption algorithms. Whenever we combine the best DNA coding scheme with the PWLCM, we get a powerful encryption system.

The rest of the paper is structured as follows. The underlying principle of chaotic maps discussed in Section II. The fundamental principles of binary bit plane decomposition and PWLCM chaotic map are briefly discussed in Section III. We go over the suggested algorithm in depth in Section IV. Section V contains the simulation results and discussion. Finally, in the final section, the conclusions are presented.

II. CHAOS THEORY

In mathematics, chaos theory is the study of seemingly random or unpredictable behavior in deterministic systems. Deterministic chaos, a more correct word, indicates a paradox because it integrates two concepts that are widely thought to be irreconcilable; it deals with non-linear dynamic systems. Because of the many feedbacks between the system's components, the systems are termed non-linear. Because of the changes they exhibit as a result of their current state, the systems are termed dynamic.

"Chaotic maps" are a term used to describe such systems. Chaotic maps have chaotic behavior, non-convergence, and state ergodicity, and are highly dependent to their beginning values and control parameters. Because of these qualities, the researcher decided to employ chaotic maps for encryption.

Chaos maps must be constructed in such a way that the entropy generated by the map can produce the required Confusion and diffusion in order to properly employ chaos theory in cryptography. Cryptographic primitives and chaotic systems share similar features, allowing chaotic systems to be exploited in cryptography. It will be practically impossible for an opponent to locate the outputs without knowing the initial values if chaotic parameters and cryptographic keys can be symmetrically or asymmetrically mapped to yield acceptable and functioning outputs.

III. BIT PLANE DECOMPOSITION & PWLCM CHAOTIC MAP

A. Binary Bit-plane Decomposition (BBD)

Zhou et al. [12] described three bitplane decomposition algorithms in depth in. In our encryption algorithm, we use binary bitplane decomposition (BBD). A pixel value in a grayscale image can be represented in an 8-bit binary sequence. The BBD can divide a grayscale image into eight binary bit-planes, each of which is composed of the i^{th} bit of the binary representation of each pixel.

B. Piecewise linear chaotic map (PWLCM)

PWLCM is a map made up of numerous linear segments, as shown in Eq (1).

$$F(x,p)=\begin{cases}\dfrac{x}{p} & x\in[0,p)\\ \dfrac{x-p}{\frac{1}{2}-p} & x\in\left[p,\frac{1}{2}\right]\\ F(1-x,p) & x\in[\frac{1}{2},1]\end{cases} \quad (1)$$

Where the value of p is the interval (0, 0.5) and initial value of x should be in the interval (0, 1). The users can specify the values of p and x which serves as the secret key. Using these initial values, required length of key stream can be calculated. Because PWLCM has a uniform invariant distribution and high ergodicity, confusion, and determinacy, it may generate great random sequences that are suited for data encryption [11].

IV. PROPOSED IMAGE ENCRYPTION MODEL

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:

$X_1=mod(floor(X\times 10^{14}),256)$ (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.

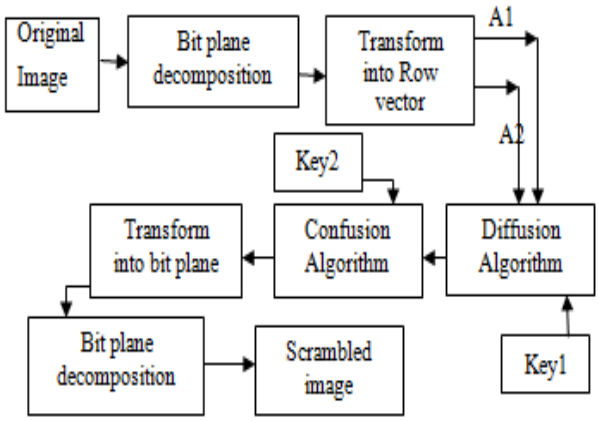

Fig 1: Block Diagram of image scrambling using chaotic map

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

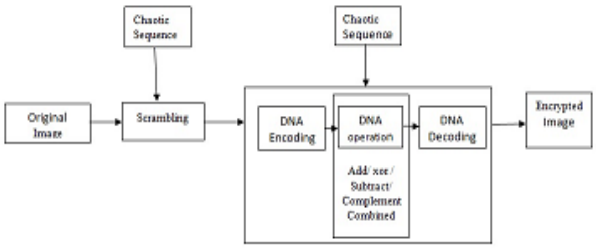

Fig 2: Block Diagram of proposed image encryption using DNA coding

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 [13-15]. 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

$$Ri(j) = Bi(j-1) \oplus Bi(j) \oplus (\lfloor Sk(i,j) \times 10^{10} \rfloor \bmod 256) \quad (3)$$

V. EXPERIMENTAL 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.

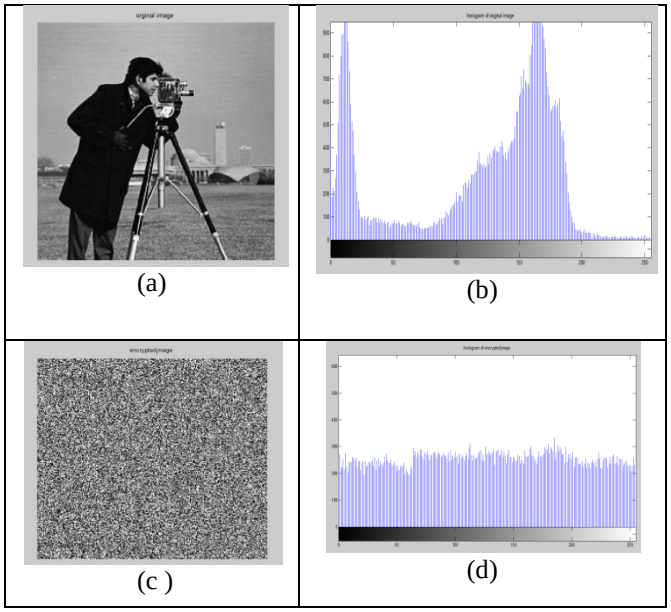

Fig 3(a) grayscale test image1(b)Histogram of test image (c) encrypted image (d)Histogram of encrypted image

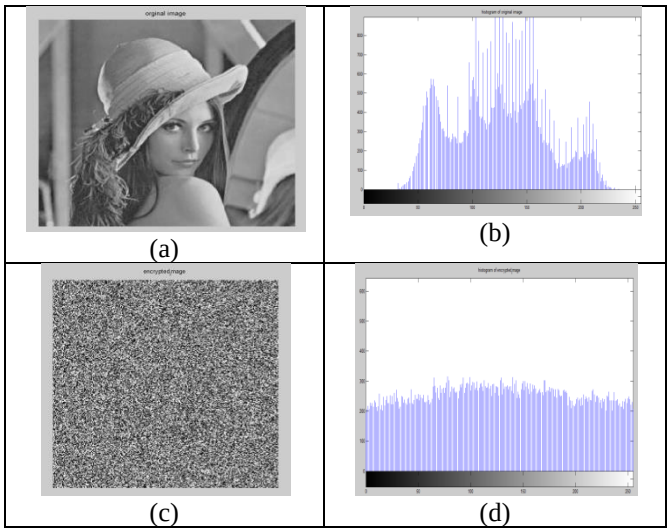

Fig 4(a) grayscale test image2(b)Histogram of test image (c) encrypted image (d)Histogram of encrypted image

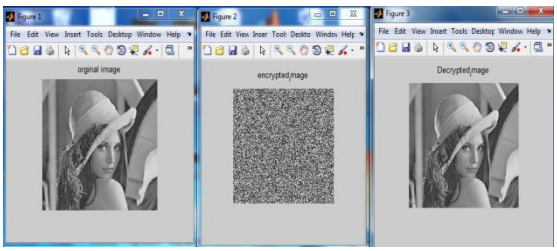

Fig 5. Original image, scrambled and descrambled grayscale image(from left to right)

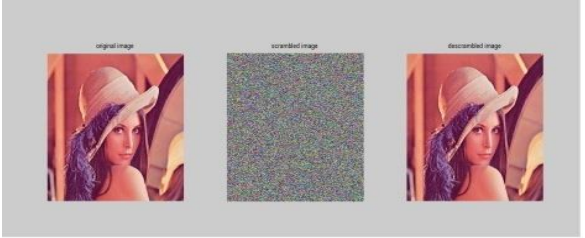

Fig 6. Original image, scrambled and descrambled RGB image((from left to right)

VI. CONCLUSIONS

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.

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.