SHODH SANGAM -- A RKDF University Journal of Science and Engineering

Review of Recent Advanced Image Encryption Techiques

[1]Shivhari Arya,[2]Dr. Akant Kumar Raghuwanshi, [3]Dr. Balajeee Sharma
[1]M. Tech Scholar, [2]Associat Professor, [3]Associat Professor
[1]Department of Electronics and Communication Engineering, Vedica Institute of Technology Bhopal, (M.P.)
[2]Department of Electronics and Communication Engineering, Vedica Institute of Technology Bhopal,, (M.P.)
[3]Department of Electronics and Communication Engineering, Vedica Institute of Technology Bhopal,, (M.P.)
Email-: [1]shivhari.arya7@gmail.com, [2]akantthakur7@gmail.com, [3]sharmabalajee@gmail.com

Abstract:- This paper presents a detailed survey of image encryption techniques existing in the literature. It also describes an advanced methodology based on Optimized Piecewise Linear Chaotic Map (OPWLCM). The methodology involves the use of an OPWLCM for image encryption and decryption. The OPWLCM generates chaotic sequences based on control parameters, which act as secret keys. The encryption process consists of two main phases: diffusion and confusion. In the diffusion phase, chaotic sequences modify pixel values through XOR operations, ensuring that small input changes cause significant alterations in the encrypted image. The confusion phase permutes bit-planes using chaotic sequences, disrupting spatial relationships to enhance security. After these phases, the bit-planes are recombined to form the final encrypted image. Particle Swarm Optimization (PSO) optimizes the OPWLCM parameters to maximize encryption quality, typically evaluated by entropy. The decryption process reverses these steps, using the same chaotic sequences to restore the original image.

Keywords:-Image Encryption, Particle Swarm Optimization, Chaotic maps, Cryptanalysis

I. INTRODUCTION

Image encryption is essential for digital security, safeguarding images from unauthorized access, theft, and tampering. As digital imagery becomes more prevalent in fields like personal communication, social media, medical imaging, and satellite imagery, the need for robust security measures grows. Image encryption ensures sensitive visual data remains confidential by transforming it into an unreadable format, accessible only with the correct decryption key [5]. Image encryption is crucial for preventing unauthorized access and tampering of digital images. As cyber threats grow more sophisticated, encryption adds an essential layer of security by converting images into a meaningless format that only authorized users with the decryption key can access. This ensures that even if intercepted, the information within the encrypted images remains secure [7].

Image encryption is particularly important due to the unique challenges posed by digital images, such as their size, complexity, and the need to preserve visual characteristics. Images contain large amounts of data with highly correlated pixel values, making them vulnerable to attacks like differential cryptanalysis. As a result, specialized encryption techniques are needed to secure digital images effectively while maintaining their quality and usability [8][9].To address the challenges of image encryption, various methods have been developed, ranging from traditional algorithms like AES to more advanced techniques involving chaotic maps, fractals, and quantum cryptography. Traditional methods, such as AES, convert image data into binary values, which are then encrypted using a secret key [10].While traditional encryption methods like AES are effective, they can be computationally intensive for large images and may not always meet security needs for specific applications [11]. Chaotic maps have become a promising tool in cryptography due to their blend of deterministic behavior and sensitivity to initial conditions.

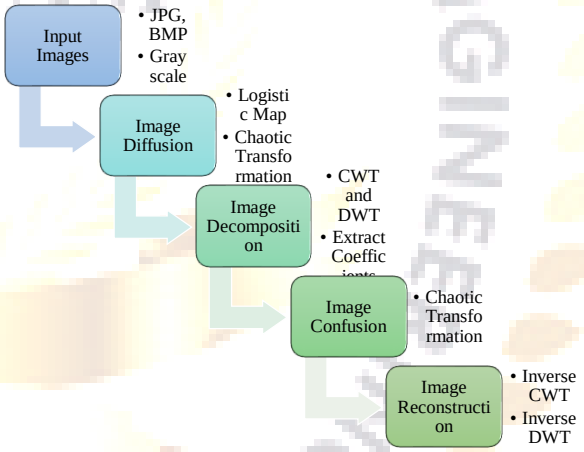

Figure 1: Image Encryption [6]

II. LITERATURE REVIEW

Li et al. [1] propose a novel image encryption algorithm that enhances security by increasing sensitivity to plain images. The algorithm uses SHA-256 for initial values, key matrices through permutation, and Cellular Automata to transform scrambled images into cipher-images, effectively resisting various attacks.

Pradeep et al. [2] utilize Henon chaotic maps for image encryption, comparing them with conventional algorithms. Their security analysis and simulations demonstrate the robustness and simplicity of the proposed algorithm, while also identifying a new combination of maps for encryption applications.

Kolivand et al. [3] propose an image encryption framework that eliminates statistical information, making cryptanalysis infeasible. The framework uses Equal Pixel Values Quantization (EPVQ) to enhance confusion and diffusion through chaotic maps and additive white Gaussian noise. EPVQ idealizes the histogram and entropy, minimizing pixel correlation and extending the key space to resist brute-force attacks.

Liu et al. [4] introduce a Logistic-Sine-Coupling Map (LoSCM) with improved chaos and an image encryption algorithm using improved Radial Diffusion (ImRD). The algorithm incorporates SHA-512, RSA, and other models, effectively countering known-plaintext attacks.

Hikal et al. [5] present a novel palm print image encryption scheme using hybrid chaotic maps, offering robust defense against statistical, brute force, and differential attacks, with fast processing suitable for real-time applications.

Kumar et al. [6] introduce SOCIET, a lightweight image encryption technique using Second-Order Cellular Automata (SOCA) for pixel shuffling and XOR operations, with a chaotic map generating the key image, resulting in high encryption speed and robustness against attacks.

Saklia et al. [7] provide efficient and robust security leveraging high initial condition sensitivity and low computational power.

Patel et al. [8] propose a method combining chaotic logistic mapping and DNA encoding to improve security and key space, showing better results in PSNR and SSIM.

Fridrich et al. [9] develop symmetric block encryption schemes using chaotic 2D maps for large data encryption, such as digital images.

Azzari et al. [10] present a grayscale image encryption method using Fibonacci Transformation and discrete wavelet transforms, achieving strong statistical results and quick processing times.

Wong et al. [11] enhance encryption efficiency by introducing a diffusion effect in the substitution stage, reducing the number of operation rounds needed while improving resistance to attacks.

Akraam et al. [12] present an image encryption cryptosystem using multiple chaotic maps and random integers linked to plain image pixels, providing robustness against attacks and ample key space for secure communication.

Alrubaie et al. [13] propose the 2DNALM algorithm, which combines double-dynamic DNA sequence encryption and chaotic 2D logistic maps, offering strong encryption and resistance to common attacks.

Benaissi et al. [14] introduce a hybrid chaotic map-based algorithm that uses a key image mask and ExtraParam from the original image, achieving excellent performance and privacy.

Hussain et al. [15] combine 3DES and AES with chaotic maps for enhanced encryption.

III. PROPOSED METHODOLOGY

The Piecewise Linear Chaotic Map (PWL-CM) generates chaotic sequences, which are used for the encryption and decryption processes. The chaotic map is defined as follows: Let x_n be a sequence of real numbers in the interval (0,1), and let n∈(0,0.5) be a control parameter. The map is given by the following piecewise linear functions:

$$F(x,y) = \begin{cases} x_n/n & x \in [o,n] \\ (x_n - n)/(\frac{1}{2} - n) & x \in [n,1/2] \\ 1 - x_n & x \in [1/2,1] \end{cases} \quad (1)$$

Where the parameter n lies in the interval (0, 0.5), and the initial value of x_n is within the range (0, 1). These values, n and x , act as secret keys for encryption. By using these initial values, the necessary length of the key stream can be generated. PWLCM is known for its uniform invariant distribution, strong ergodicity, and confusion properties, making it highly suitable for generating random sequences for encryption purposes.

Encryption and Decryption Process: The encryption process involves two main steps: diffusion and confusion. Both steps use chaotic sequences generated by PWL-CM, with parameters x_0 and n_0 optimized by PSO.

Bit-Plane Extraction: Given an image I of size $M \times N$, the pixel values $I(i,j)$ are decomposed into their bit-planes. Each pixel $I(i,j)$ is represented in binary form, and its bit-planes are extracted as:

$$I(i,j) = b_1(i,j) \times 2^0 + b_2(i,j) \times 2^1 + \cdots .. + b_8(i,j) \times 2^7 \quad (2)$$

Where, $b_k(i,j) \in \{0,1\}$ is the k-th bit of the pixel at position (i,j).

Diffusion Phase: During the diffusion phase, a chaotic sequence X_n is generated using the OPWL-CM:

$$X_{n+1} = OPWLCM(X_n, n_0) \quad (3)$$

This sequence is then used to modify the pixel values by XORing the pixel bits with the chaotic sequence, ensuring that small changes in the input image result in significant changes in the encrypted image.

Confusion Phase: In the confusion phase, the bit-planes are permuted using a chaotic sequence generated by the PWL-CM. The permutation is applied to create confusion by changing the positions of the bit-plane values. This ensures that the spatial relationships between neighboring pixels are destroyed, increasing the security of the encryption.

Recombination of Bit-Planes: After the confusion and diffusion steps, the permuted bit-planes are recombined to form the final encrypted image.

PSO based PWL-CM: PSO is used to optimize the parameters x_0 and n_0 of the PWL-CM to improve the encryption process. The optimization goal is to minimize a fitness function that reflects the encryption quality, such as the entropy of the encrypted image. The fitness function evaluates the quality of the encryption.

Decryption Process: The decryption process reverses the confusion and diffusion steps using the same chaotic sequences generated by the optimized PWL-CM. The bit-planes are permuted back to their original order, and the chaotic sequence is XORed with the encrypted bit-planes to restore the original image.

1. Performance Parameters

PSNR (Peak Signal-to-Noise Ratio): A measure of the quality of reconstruction in image processing. Higher values generally indicate better quality.

$$PSNR = 10.log_{10}(\frac{Max_i^2}{MSE}) \quad (4)$$

MSE (Mean Squared Error): Measures the average of the squares of the errors between the estimated and actual values. Lower MSE values generally indicate better image quality.

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(O_i - P_i)^2 \quad (5)$$

Where, N is the total number of pixels, O_i is the original image and P_i is the decrypted image.

Enc Time (in Sec): The time taken in seconds to encrypt the image. Lower times indicate more efficient performance.

Dec Time (in Sec): The time taken in seconds to decrypt the image. Lower times indicate more efficient performance.

Number of Pixels Change Rate (NPCR): Mathematically it is evaluated as:

$$NPCR = \frac{\text{Number of Different Pixels}}{\text{Total Number of Pixels}} * 100 \quad (6)$$

Unified Average Changing Intensity (UACI): An ideal UACI value is theoretically is 33.4635. Mathematically, UACI is evaluated as:

$$UACI = \frac{1}{n*m}\sum_{i=1}^{n}\sum_{j=1}^{m}\frac{P_{ij} - C_{ij}}{L} * 100 \quad (7)$$

P_{ij} is the original image and C_{ij} is the encrypted image.

IV. CONCLUSION

In conclusion, the proposed Optimized Piecewise Linear Chaotic Map (OPWLCM) provides a robust and efficient approach for image encryption and decryption. The Optimized Piecewise Linear Chaotic Map (OPWLCM) is a robust and efficient method for image encryption and decryption. It leverages chaotic sequences' inherent properties for high security.

REFERENCES

[1] S. Liu and G. Ye, "Asymmetric image encryption algorithm using a new chaotic map and an improved radial diffusion," *Optik (Stuttg).*, vol. 288, p. 171181, 2023, doi: https://doi.org/10.1016/j.ijleo.2023.171181.

[2] D. A. Pradeep, A. Harsha, and J. Jacob, "Image Encryption Using Chaotic Map And Related Analysis," in 2021 International Conference on Advances in Computing and Communications (ICACC), 2021, pp. 1–5. doi: 10.1109/ICACC-202152719.2021.9708189.

[3] H. Kolivand, S. F. Hamood, S. Asadianfam, M. S. Mohd Rahim, and W. Hurst, "Image encryption framework based on multi-chaotic maps and equal pixel values quantization," Multimed. Tools Appl., 2024, doi: 10.1007/s11042-024-19771-y.

[4] L. Li, Y. Luo, S. Qiu, X. Ouyang, L. Cao, and S. Tang, "Image encryption using chaotic map and cellular automata," Multimed. Tools Appl., vol. 81, no. 28, pp. 40755–40773, 2022, doi: 10.1007/s11042-022-12621-9.

[5] N. A. Hikal and M. M. Eid, "A new approach for palmprint image encryption based on hybrid chaotic maps," J. King Saud Univ. - Comput. Inf. Sci., vol. 32, no. 7, pp. 870–882, 2020, doi: https://doi.org/10.1016/j.jksuci.2018.09.006.

[6] K. Kumar, S. Roy, U. Rawat, and A. Shandilya, "SOCIET: Second-order cellular automata and chaotic map-based hybrid image encryption technique," Multimed. Tools Appl., vol. 83, no. 10, pp. 29455–29484, 2024, doi: 10.1007/s11042-023-16735-6.

[7] M. Saikia and B. Baruah, "Chaotic Map Based Image Encryption in Spatial Domain: A Brief Survey," 2017, pp. 569–579. doi: 10.1007/978-981-10-2035-3_58.

[8] S. Patel, B. K. P, and R. K. Muthu, "Image Encryption Decryption Using Chaotic Logistic Mapping and DNA Encoding," 2020, [Online]. Available: http://arxiv.org/abs/2003.06616

[9] J. Fridrich, "Image encryption based on chaotic maps," in 1997 IEEE International Conference on Systems, Man, and Cybernetics. Computational Cybernetics and Simulation, 1997, vol. 2, pp. 1105–1110 vol.2. doi: 10.1109/ICSMC.1997.638097.

[10] D. E. Azzari, X. Fu, Y. Xian, and X. Wang, "A Novel Image Encryption Scheme Using Chaotic Maps and Fuzzy Numbers for Secure Transmission of Information," Appl. Sci., vol. 13, no. 12, 2023, doi: 10.3390/app13127113.

[11] K.-W. Wong, "Image Encryption Using Chaotic Maps," in Intelligent Computing Based on Chaos, L. Kocarev, Z. Galias, and S. Lian, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 333–354. doi: 10.1007/978-3-540-95972-4_16

[12] M. Akraam, T. Rashid, and S. Zafar, "A Chaos-Based Image Encryption Scheme Is Proposed Using Multiple Chaotic Maps," Math. Probl. Eng., vol. 2023, no. i, pp. 1–13, 2023, doi: 10.1155/2023/2003724.

[13] A. H. Alrubaie, M. A. A. Khodher, and A. T. Abdulameer, "Image encryption based on 2DNA encoding and chaotic 2D logistic map," J. Eng. Appl. Sci., vol. 70, no. 1, p. 60, 2023, doi: 10.1186/s44147-023-00228-2.

[14] S. Benaissi, N. Chikouche, and R. Hamza, "A novel image encryption algorithm based on hybrid chaotic maps using a key image," Optik (Stuttg)., vol. 272, p. 170316, 2023, doi: https://doi.org/10.1016/j.ijleo.2022.170316.

[15] A. Z. Hussain and K. Maisa'a Abid Ali, "Securing Medical Images Using Chaotic Map Encryption and LSB Steganography," Rev. d'Intelligence Artif., vol. 38, no. 1, pp. 313–321, 2024, doi: 10.18280/ria.380133.

[16] Raghuvanshi, Kamlesh Kumar, et al. "Investigation of piecewise linear chaotic map as a diffusion model for image encryption." Multimedia Tools and Applications 82.23 (2023): 36325-36342.