International Academic Institute for Science and Technology

International Academic Journal of Science and Engineering
Vol. 12, No. 2, 2025, pp. 1-5.

ISSN 2454-3896

International Academic Journal of Science and Engineering

www.iaiest.com

Development of a Chaos Theory-Based Digital Image Encryption Algorithm for Enhanced Security in Modern Applications

Iqra Hussain [a] , Samarjeet Khanna [b]

[a] *Neural Symbolic Systems Lab, Bareilly AI Research Centre, India.*
[b] *Neural Symbolic Systems Lab, Bareilly AI Research Centre, India.*

Abstract

In recent years, image encryption, a critical domain of data security, has garnered considerable attention from researchers and scientists. Numerous studies have proposed innovative and effective methods to enhance secure picture encryption systems. Chaotic methodologies have been identified in multiple domains, including cryptosystem design and picture encryption. Digital picture encryptions using chaotic algorithms represent a fresh approach to image security. This technology employs random chaotic sequences for image encryption, providing a very secure and rapid way. This approach has limited precision as a drawback. This work investigates the chaotic sequence and the wavelet transform values to identify gaps. A fresh method for digital image encryption has been suggested, enhancing prior algorithms. The technique is executed in MATLAB, and a comparison is conducted based on several performance metrics, including the Number of Pixels Change Rates (NPCR), Peak Signal to Noise Rate (PSNR), correlation factor, and Unified Average Changing Illumination (UACI). The modeling and mathematical evaluation demonstrate the suggested scheme's efficacy, confirming that this technology is an appropriate option for the practical encryption of images.

Keywords: Chaos Theory, Digital Image, Image Encryption, Security.

DOI: 10.71086/IAJSE/V12I2/IAJSE1210
Received: Received: 03 March 2025/Revised: 15 April 2025/Accepted: 09 May 2025/Published: 27 June 2025

Introduction

In the past few years, image encryption has emerged as a compelling field of research. It is widely acknowledged as an effective method for secure communication. Each picture encryption method is designed to produce a high-quality, noisy image to maintain information confidentiality (Kaur & Kumar, 2020). Encryption of images is advantageous for ensuring safe transmission and image storage online. The rapid advancement of Internet technology has significantly expanded digital interaction. Individuals can transmit a digital image via the Internet anytime and from any location. This has led to the advancement of digital image cryptography. Various methodologies for digital picture encryption in research are linked to the growing demand for security. The chaos-based image encryption approach is an innovative technique that utilizes a random chaotic sequence to encrypt images, effectively addressing the challenges of achieving high security and rapid encryption (Umar et al., 2024). In recent years, multiple iterations of the chaotic method have been introduced.

This study focuses on the chaos order, the wavelet transformation values, and the incorporation of the picture encryption technique (Liu & Ko, 2021). These systems are mimicked by evaluating them to identify deficiencies. The method was improved. This approach employs two limited chaotic structures capable of utilizing even a basic non-linear equation to exhibit chaotic behavior. The primary objective, along with the rationale for using this type of map, is to identify a novel discrete-time series analogous to the chaotic outputs of the logistic map characterized by distinct variables and fundamental equations.

Background

Among all the aforementioned methodologies, chaos has garnered significant attention because of its straightforward structure and heightened sensitivity to initial circumstances. Mathews was the inaugural scientist to employ chaos in the encryption of images. Chaotic encryption of image algorithms can be categorized into two classifications (Pourasad et al., 2021). i) One-dimensional (1D) and ii) Multidimensional (MD). The MD chaotic mappings have demonstrated their efficacy in image security due to their intrinsic complicated topologies and numerous factors. However, MD chaotic maps exhibit inherent complexity and need significant time investment. Conversely, one-dimensional chaotic structures are simpler and are straightforward to carry out in hardware and software. The ID chaotic maps exhibit vulnerabilities such as brief, chaotic times, the non-uniform appearance of chaotic outputs, susceptibility to cryptanalysis by correlation coefficients, and minimal computational evaluation (Zia et al., 2022). The study employed the SHA-256 hash operation, and the bit fields of pictures were encrypted in three dimensions. The Galois area of order 256 creates boxes for substitution using Linear Fractional Conversion. In replacement, the Forward Substitution Procedure (FSP) and Reversal Substitution Procedure (RSP) are applied to the cells in the picture (Ur Rehman et al., 2021).

Despite identifying specific vulnerabilities through the cryptography of chaos-based picture encryption techniques, the existing image encryption solutions remain inadequate in resisting attacks. One such assault is the selected plaintext assault on encryption systems, which operates independently of the private keys associated with the unencrypted. The investigation cryptanalyzed the method via a selected plaintext assault (Pak et al., 2024). The research team exploited vulnerabilities in the suggested encryption approach through a chosen plaintext assault, successfully breaching the cipher by utilizing the same process to retrieve the initial picture without access to the private key. The researchers cryptanalyzed the method established for the study with a chosen textual assault. The proposed technique alters the private keys autonomously, with no user intervention, through minimal modifications to the plaintext. This requirement arises from the SHA-512 hash operation, which ensures the plaintext's resilience against selected unencrypted attacks (Rahul et al., 2023). The suggested design employs chaotic mappings to enhance sensitivity to initial circumstances and system variables within a simple and fundamental architecture.

Proposed Chaos Theory-Based Digital Image Encryption

This section can be subdivided into subsections. The summary must be succinct and accurate, encompassing the study's findings, their meaning, and the inferences that can be derived from them. Fig. 1 illustrates the suggested method. The procedures for executing the proposed algorithm are as follows:

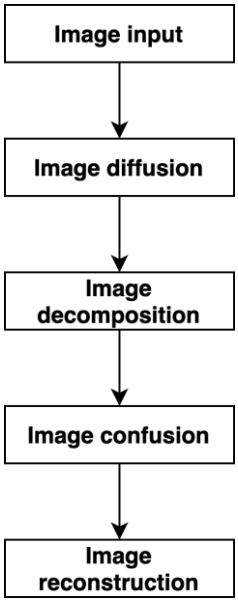


Fig. 1: Encryption of the Proposed Model

3.1. Encryption Assessments Metrics

The research evaluated the efficiency of the cryptography system by picking essential variables to analyze the method. The use of sight is a primary criterion for evaluating encrypted pictures. Feature diffusion surveys are another metric used to assess the selection technique. The examination identifies the divergence of a product from a specific set of characteristics. Humans typically do the examination; machine vision is employed to automate this process. The effective dissemination of an algorithm renders the relationship between the original picture and the encrypted image too complex and unpredictable. This study examined the Peak Signal Noise Ratio (PSNR) computation parameters and the correlation between the encrypted image and the key picture. The research evaluated the specification dispersion by computing two metrics: the Uniform Average Changing Illumination (UACI) and the Quantity of Pixels Change Rates (NPCR).

3.2. PSNR

PSNR is an electronic metric derived from Mean Square Error (MSE). It is commonly employed for the assessment of quality of images in the following way:

$$SNR = 10 \log \left(\frac{255^2}{MSE(x,x')} \right) \quad (1)$$

where $x(i,j)$ and $x'(i,j)$ indicate the pixel counts of the m x n actual and rebuilt pictures.

3.3. NPCR

Diffusion is characterized by the quantity of the most essential variables for evaluating the randomness of the encryption technique. NPCRs are utilized to assess the safety of picture encryption techniques. Given K_1 and K_2, both of size N × M, the research established an array, D, with dimensions identical to those of pictures K_1 andK_2, as follows:

$$D(x,y) = \begin{cases} 0 & If\ K_1(x,y) = K_2(x,y) \\ 1 & If\ K_1(x,y) \neq K_2(x,y) \end{cases} \quad (2)$$

The NPCR calculates the proportion of pixels between two distinct images, and it is computed using the following method:

$$NPCR = \frac{\sum_{x=0}^{N \times M} D(x,y)}{N \times M} \quad (3)$$

3.4. UACI

UACI calculates the mean luminosity of the disparity between the two decrypted pictures (K_1 and K_2) utilizing the following formula. It is used to assess the robustness of the encryption technique. The image's style and dimensions determine the value. UACI evaluates the mean brightness fluctuation between the encrypted and original pictures. The

highest UACI signifies that the proposed method exhibits resilience against many attacks. The UACI for a grayscale picture of dimensions M x N is calculated as follows:

$$UACI = \frac{1}{N \times M}\left(\sum_{x=0}^{N \times M} \frac{K_1(x,y) - K_2(x,y)}{\max(K_2)}\right) \quad (4)$$

3.5. Correlation Coefficient

Digital Image Correlation (DIC) is a pivotal and widely employed non-contact technique for quantifying material distortion. The past few decades have witnessed substantial advancements in creating innovative empirical DIC techniques and enhancements in the efficiency of associated computer algorithms. A Normalized Correlation (NC) is established between the identical pixels of the encryption and initial pictures as follows:

$$NC = \frac{\sum_{x=0}^{N-1} m \sum_{x=0}^{N-1} (P_{mn} - \bar{P})(Q_{mn} - \bar{Q})}{\sqrt{(P_{mn} - \bar{P})^2 (Q_{mn} - \bar{Q})^2}} \quad (5)$$

P and Q represent the original picture, the encrypted one, and its components. A smaller correlation coefficient number is preferable.

Results and Discussions

4.1. Histogram Examination

The initial assessment involves the histogram evaluation of the hidden, decoded, and initial pictures. The picture histograms of the respective photographs illustrate the significant disparities between the encrypted and original pictures despite their similarity. The analysis of the test picture's statistical and the histogram post-encryption reveals that the encrypted image exhibits a consistent distribution over the full statistical range. The pattern of distribution regularity of the initial picture is obscured. The encryption is executed proficiently.

4.2. Complexity

Employing the suggested method, encrypting an image A of dimensions M × N should yield an M x N array of random integers R1 through the chaotic mapping. Therefore, the difficulty of generating M x N number generators is O(m). By extending the duration of the exact chaotic mapping, the method is expected to create an arbitrary chaos sequence comprising M x N bits. The difficulty is reiterated in generating M x N bits as random as O(m). it constructs a series (M × N) of chaotic sequence changes or additions with a degree of complexity O(m). it constructs a chain of XOR procedures with an O(m) complexity. The overall difficulty of the method is O(n).

4.3. Resilience

The research assessed the association among two downward, two downwards, and two horizontally positioned pixels in both the input and encrypted images alongside a histogram analysis presented in Fig. 1. The numerical values of two contiguous pixels in the picture are denoted by the x- and y-axes. The Pearson correlation values for the plain picture and the cipher image are 0.98 and 0.03, respectively. Both the diagonal and vertical orientations produce comparable outcomes.

To assess the durability of the suggested technique, the test pictures are subjected to four kinds of computational image processing assaults: movement, noise with Gaussian distribution, median filtering, and histogram equalization. The findings indicate that the proposed architecture exhibits enhanced robustness and normalized correlations. The findings suggest that input attacks do not influence the encryption of images and decoding. The NC values for several images suggest that median filtering, rotation, and Gaussian noise yield elevated NC values. The resilience of the proposed technique withstands several forms of attacks. The effect of equalizing the histogram is significant (Table 1).

Table 1: Performance Analysis

Picture	Median Filtering	Histogram Equalisation	Rotations	Gaussian Noise
Leena	0.785	0.973	0.987	0.989
Peppers	0.684	0.324	0.943	0.954
Barara	0.942	0.532	0.989	0.932
Baboon	0.975	0.743	0.996	0.975
Boats	0.985	0.852	0.998	0.996

Conclusion

Recently, numerous chaos-based picture cryptosystems have been introduced. This study addresses a chaotic-based method utilizing the properties of chaotic maps and wavelet transforms. This method's encryption method is comprised of two parts. Initially, the research executed the image dispersion procedure. Applying the wavelet transform to data significantly diminished the computational burden associated with confusion through hyper-chaotic sequences. The simulation outcomes utilizing standard measures indicate that the suggested approach significantly relies on keys. This method exhibits satisfactory encryption efficacy. It is capable of withstanding noise and mitigating cutting assaults. The histograms for the input and encryption photos are illustrated. The criteria for analyzing encryption efficiency, including PSNR, NPCR, UACI, and NC, are documented. To assess the robustness of the suggested approach, the test pictures are subjected to four categories of image processing assaults: movement, Gaussian disturbances, median filtering, and equalization of histograms.

The findings indicate that the design suggested exhibits enhanced robustness and reduced correlations. The findings indicate that input attacks do not influence the encryption of images and decoding. The NC values for several images suggest that median filtering, movement, and Gaussian noise yield elevated NC values. The resilience of the proposed technique withstands such attacks.

References

Kaur, M., & Kumar, V. (2020). A comprehensive review on image encryption techniques. *Archives of Computational Methods in Engineering*, *27*(1), 15-43. https://doi.org/10.1007/s11831-018-9298-8.

Umar, T., Nadeem, M., & Anwer, F. (2024). Chaos based image encryption scheme to secure sensitive multimedia content in cloud storage. *Expert Systems with Applications*, *257*, 125050. https://doi.org/10.1016/j.eswa.2024.125050.

Liu, Y., & Ko, Y. C. (2021). Image processing method based on chaotic encryption and wavelet transform for planar design. *Advances in Mathematical Physics*, *2021*(1), 7511245. https://doi.org/10.1155/2021/7511245.

Pourasad, Y., Ranjbarzadeh, R., & Mardani, A. (2021). A new algorithm for digital image encryption based on chaos theory. *Entropy, 23*(3), 341. https://doi.org/10.3390/e23030341.

Zia, U., McCartney, M., Scotney, B., Martinez, J., AbuTair, M., Memon, J., & Sajjad, A. (2022). Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains. *International Journal of Information Security*, *21*(4), 917-935. https://doi.org/10.1007/s10207-022-00588-5.

Ur Rehman, A., Liao, X., & Wang, H. (2021). An innovative technique for image encryption using tri-partite graph and chaotic maps. *Multimedia Tools and Applications*, *80*(14), 21979-22005. https://doi.org/10.1007/s11042-021-10692-8.

Pak, C., Jong, C., Pang, R., Ri, S., & Kim, J. (2024). A new image encryption algorithm using 2D infinite collapse coupling map. *Multimedia Tools and Applications*, *83*(17), 50619-50643. https://doi.org/10.1007/s11042-023-17493-1.

Rahul, B., Kuppusamy, K., & Senthilrajan, A. (2023). Dynamic DNA cryptography-based image encryption scheme using multiple chaotic maps and SHA-256 hash function. *Optik*, *289*, 171253. https://doi.org/10.1016/j.ijleo.2023.171253.