Image Encryption and Decryption Using Chaotic Maps and Scan Pattern

Authors:
Mrs. Nita Meshram – Associate Professor of CSE Dept. KSSEM [Naveen Kanth S – naveenkanths73@gmail.com
Yashu V D – yashuvdyashuvd01@gmail.com
Yashwanth Saibaba H – yashkrish21042003@gmail.com Yashwin Kumar R – yashwinkumar.ravikumar@gmail.com
Students of 8th Sem CSE Dept. KSSEM, Bengaluru, India]

Abstract

In the era of digital communication, image security has become a paramount concern, particularly with the proliferation of multimedia applications over insecure networks. This project proposes a robust image encryption and decryption method utilizing a combination of scan patterns and chaotic maps to enhance security and complexity. Specifically, the encryption process integrates Zeta and Spiral Scan Patterns for pixel rearrangement, followed by confusion using the Arnold Cat Map, and further strengthened by a Logistic Map-based diffusion mechanism. The scan patterns disrupt the pixel positioning, while the Arnold Cat Map introduces confusion through spatial transformation. The Logistic Map, known for its high sensitivity to initial conditions, ensures strong diffusion by altering pixel values based on chaotic sequences.

The decryption process reverses these operations in sequence to accurately retrieve the original image. Experimental results demonstrate that the proposed hybrid approach significantly improves the resistance against statistical and differential attacks, providing a high level of security and reliability. This method is especially suitable for secure image transmission and storage in applications demanding confidentiality and integrity.

I. Introduction

With the rapid growth of digital communication, securing image data has become increasingly important. Traditional encryption techniques are often not optimized for images due to their high redundancy and pixel correlation. To address these challenges, this project presents a novel image encryption and decryption method based on chaotic maps and scan patterns**.** By using Zeta and Spiral Scan Patterns**,** the pixel positions are rearranged to break the spatial correlation. Further, the Arnold Cat Map is applied for confusion, and the Logistic Map introduces diffusion by modifying pixel values through chaotic sequences. This hybrid approach ensures enhanced image security, making it highly effective against common cryptographic attacks while preserving image integrity during transmission or storage.

II. Existing System Overview

Traditional image encryption techniques often rely on standard cryptographic algorithms such as AES, DES, or RSA. While these methods are highly secure for text-based data, they are not well-suited for image encryption due to the inherent characteristics of images, such as large data size, high redundancy, and strong pixel correlation. Additionally, many existing systems use only a single chaotic map, like the Logistic Map or Arnold Cat Map, to introduce confusion or diffusion. However, using a single transformation limits the complexity of the encryption and can leave the system vulnerable to brute-force, statistical, or differential attacks.

III. Proposed Enhancement

To overcome the limitations of existing methods, the proposed system introduces a hybrid image encryption and decryption approach that combines scan patterns and multiple chaotic maps.

- Initially, the image pixels are rearranged using Zeta and Spiral Scan Patterns, effectively breaking the spatial relationships and reducing pixel correlation.
- This is followed by the application of the Arnold Cat Map, which enhances confusion by further scrambling the pixel positions.
- Finally, the Logistic Map is used for diffusion, where pixel values are altered based on chaotic sequences, providing high sensitivity to initial conditions and improving unpredictability.
-This multi-stage encryption method significantly increases security by combining structural and value-based transformations.
- As a result, the proposed system offers strong resistance to common cryptographic attacks while remaining

computationally efficient and suitable for secure image storage and transmission.

IV. System Working Principle

The proposed image encryption and decryption system operates through a sequence of transformation stages that combine scan patterns and chaotic maps to ensure high levels of security. The working principle is divided into two main phases: encryption and decryption. Encryption Process

- The user selects the input image to be encrypted using a file browser interface.

-The image pixels are rearranged using Zeta and Spiral Scan Patterns, which distort the original structure by altering the sequence in which the pixels are accessed. This process disrupts spatial correlations and increases randomness in pixel positions.

- The scrambled image is then passed through the Arnold Cat Map, a chaotic transformation that further confuses the image by reshuffling pixel positions in a complex and reversible manner. This step increases the difficulty of identifying any patterns or correlations.

-Finally, the pixel values are modified using the Logistic Map, a one-dimensional chaotic function known for its high sensitivity to initial conditions. This step changes the actual pixel intensities based on a chaotic sequence, thereby spreading out small changes throughout the image, ensuring strong diffusion.

The result is a highly scrambled and unrecognizable cipher image, which is then ready for secure storage or transmission.

Decryption Process

The decryption phase takes the encrypted image (cipher image) and performs the exact reverse of the encryption steps, using the same keys and parameters.

V. Implementation Details

The proposed image encryption and decryption system is implemented using Python, leveraging OpenCV (cv2) for image processing tasks and Pillow (PIL) for image manipulation. The implementation is structured in modular steps to perform pixel rearrangement, chaotic confusion, and pixel value diffusion.

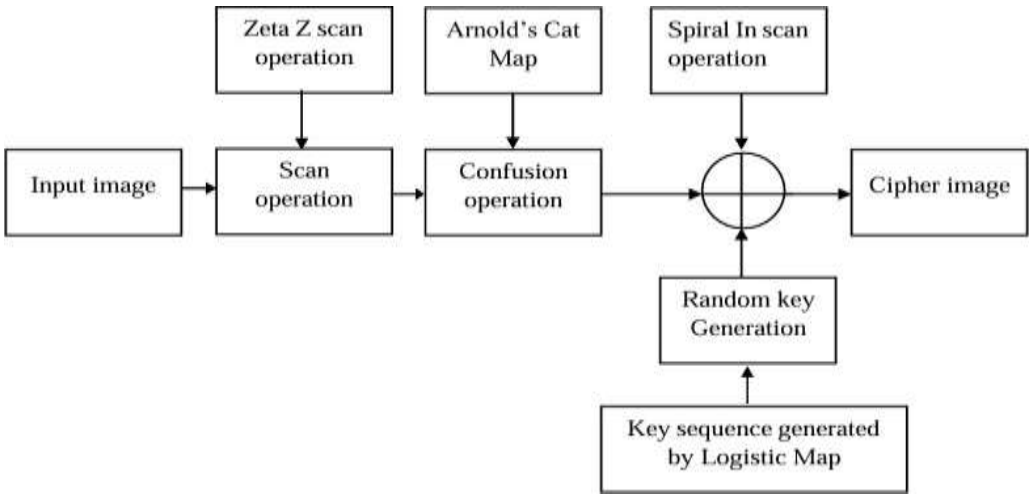

Fig 1 : Block diagram for the proposed encryption algorithm

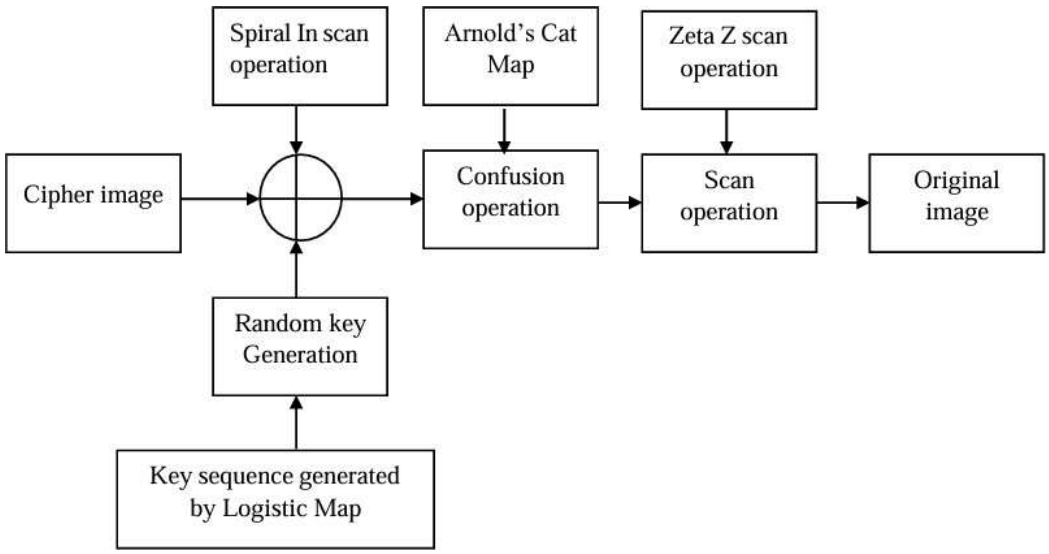

Fig 2 : Block diagram for the proposed decryption algorithm

VI. Results and Discussion

The implementation of the proposed image encryption and decryption system was carried out using Python, with OpenCV for image processing and Pillow for image manipulation.

The system was tested on various grayscale images, and the results demonstrate the effectiveness of combining scan patterns with chaotic maps. Visually, the encrypted images appear completely distorted and bear no resemblance to the original image, confirming that the applied transformations—Zeta and Spiral Scan Patterns, Arnold Cat Map, and Logistic Map—successfully conceal the original content. Upon decryption, using the correct keys and reversing the process in the exact order, the original image is perfectly restored without any loss or degradation, proving the accuracy and reversibility of the algorithm.

VII. Conclusion

This paper presents a practical and innovative upgrade to traditional laser-LDR-based In this project, a secure and efficient image encryption and decryption system was successfully implemented using a combination of Zeta and Spiral Scan Patterns, Arnold Cat Map, and Logistic Map, with Python as the development language and OpenCV and Pillow for image processing. The hybrid approach effectively applies both confusion and diffusion principles to ensure high levels of image security. Experimental results showed that the encrypted images are highly randomized, resistant to statistical analysis, and sensitive to encryption keys. Moreover, the system demonstrated reliable decryption with accurate reconstruction of the original image, proving its robustness and reversibility. The layered encryption method enhances security without significantly increasing computational complexity, making it practical for real-world applications such as secure image transmission and storage.

To further improve the system, several enhancements can be considered. First, extending the algorithm to support color images and video encryption would broaden its applicability in multimedia security. Second, dynamic key generation mechanisms using biometric inputs or timestamps could increase unpredictability and security. Third, integrating machine learning models to analyze encryption strength and optimize scan pattern selection could lead to more adaptive and intelligent encryption systems.

References

[1] A. K. Singh, K. Chatterjee and A. Singh, "An Image Security Model Based on Chaos and DNA Cryptography for IIoT Images," in IEEE Transactions on Industrial Informatics, vol. 19, no. 2, pp. 1957-1964, Feb. 2023, doi: 10.1109/TII.2022.3176054.

[2] P. Mao, X. Zhang and W. Jiang, "Image Encryption Algorithm Based on Combination Chaotic System and DNA Coding" 2022 4th International Conference on Natural Language Processing (ICNLP), Xi'an,China, 2022, pp.133-140, doi: 10.1109/ICNLP55136.2022.00029.

[3] D. Yang, X. Liu and Y. Gao, "Image Encryption and Decryption Algorithm Based on Fractional Order Simplified Lorenz Chaotic System and DNA Coding," 2022 3rd International Conference on Electronics, Communications and Information Technology (CECIT), Sanya, China, 2022, pp. 25-34, doi: 10.1109/CECIT58139.2022.00013.

[4] H. Chen and J. Zheng, "An image encryption algorithm using two dimensional chaotic map and DNA coding," 2021 IEEE 2nd Inter national Conference on Information Technology, Big Data and Artifi -cial Intelligence (ICIBA), Chongqing, China, 2021, pp. 966- 972, doi: 10.1109/ICIBA52610.2021.9687885.