Journal of Science, Computing and Engineering Research (JSCER)
Volume-9, Issue- 4, April 2026.
DOI: *https://doi.org/10.46379/jscer.2023.060503*
ISSN: 2708-1079

IMAGE ENCRYPTION DECRYPTION USING DEEP LEARNING & A CHAOTIC MAP

[1]Pradeep Kumar,[2]Dhananjay Saini,[3]Aditya,[4]Hardik Jain,[5]Kunal Yadav

[1]Professor, Department of AI&DS, Modern Institute of Technology and Research Centre, Rajasthan, India.

[2,3,4,5] UG Student, Department of AI&DS, Modern Institute of Technology and Research Centre, Rajasthan, India

Article Information

Received: Mar 30 2026
Revised : Mar 30 2026
Accepted: Mar 31 2026
Published: April 02, 2026

Corresponding Author:

Dhananjay Saini

Abstract— The rapid growth of digital image sharing has increased the need for secure and efficient image protection techniques. Traditional encryption methods are not well-suited for images due to their large size, high redundancy, and strong pixel correlation. To overcome these limitations, modern approaches using Deep Learning and Chaotic Maps provide enhanced security and performance .This project presents an Image Encryption and Decryption System using Deep Learning and a Chaotic Map, designed to ensure secure transmission of image data. The system uses chaotic maps to generate highly sensitive and random sequences for pixel permutation and diffusion, while deep learning techniques improve encryption strength and assist in accurate decryption .The system enables users to encrypt images into secure formats and decrypt them back to their original form using appropriate keys. It integrates key components such as image preprocessing, chaotic sequence generation, neural network-based transformation, and encryption-decryption modules.The proposed solution improves data security, resists common cryptographic attacks, and provides an efficient framework for secure image communication in various applications.

Keywords: Image Encryption, Image Decryption, Deep Learning, Chaotic Map, Image Security, Cryptography, Neural Networks

Citation: Pradeep Kumar, Dhananjay Saini, Aditya, Hardik Jain, Kunal Yadav, "IMAGE ENCRYPTION DECRYPTION USING DEEP LEARNING & A CHAOTIC MAP", Journal of Science, Computing and Engineering Research, 9(04), April 2026.

I. INTRODUCTION

The rapid expansion of digital communication and multimedia technologies has significantly increased the exchange of image data across various domains such as social media, healthcare, surveillance, and defense systems. As images often contain sensitive and confidential information, ensuring their security during storage and transmission has become a major concern. Unauthorized access, data breaches, and cyber-attacks pose serious threats to image data, making robust encryption techniques essential for protecting privacy and maintaining data integrity.

Traditional encryption methods such as AES and DES are primarily designed for text-based data and may not perform efficiently when applied to images due to their large size, high redundancy, and strong correlation between adjacent pixels. These limitations reduce their effectiveness in real-time image security applications. Therefore, there is a need for more advanced and efficient techniques specifically designed for image encryption and decryption.

With the advancement of Artificial Intelligence, particularly Deep Learning, along with the application of Chaos Theory, new possibilities have emerged for enhancing image security. Chaotic maps are highly sensitive to initial conditions and generate pseudo-random sequences, making them suitable for encryption tasks such as pixel permutation and diffusion. At the same time, deep learning models can learn complex patterns and transformations, improving encryption strength and enabling accurate reconstruction during decryption.

This project, Image Encryption and Decryption using Deep Learning and a Chaotic Map, aims to develop a secure and efficient framework for protecting image data. The system combines chaotic sequence generation with neural network-based transformations to perform robust encryption and reliable decryption. Users can input images, encrypt them into secure formats, and later decrypt them using appropriate keys and learned patterns.

The proposed system includes key components such as image preprocessing, chaotic map-based key generation, deep learning-based transformation, encryption and decryption modules. This integrated approach enhances security,

improves resistance against common cryptographic attacks, and provides a scalable solution for secure image communication in real-world applications.

II. PROBLEM STATEMENT

The rapid growth of digital image sharing across platforms such as social media, healthcare systems, surveillance networks, and cloud storage has created serious concerns regarding data security and privacy. Images often contain sensitive and confidential information, and unauthorized access, tampering, or data leakage can lead to significant risks. Although digital communication has become faster and more accessible, ensuring secure transmission and storage of image data remains a major challenge.

Existing image encryption methods often lack robustness against advanced attacks such as brute-force, statistical, and differential attacks. Many approaches also fail to maintain a balance between security, computational efficiency, and reconstruction accuracy during decryption. Additionally, some systems are complex, require high computational resources, or do not ensure complete randomness in encrypted outputs, making them vulnerable to potential threats.

Another major challenge is generating secure and unpredictable encryption keys. Without strong key generation mechanisms, encrypted images can be easily compromised. Furthermore, ensuring accurate and lossless decryption of images is equally important, especially in critical applications such as medical imaging and defense, where even minor distortions can lead to incorrect interpretations.

Therefore, there is a need for a robust, efficient, and intelligent image encryption and decryption system that can overcome the limitations of traditional methods. By leveraging the strengths of chaotic maps for randomness and deep learning for adaptive transformations, a more secure and reliable solution can be developed to protect image data in modern digital environments.

III. PROPOSED METHOD

The proposed system is designed to provide secure and efficient image encryption and decryption by combining chaotic map-based randomness with deep learning techniques. It ensures high security, accurate reconstruction, and resistance against various cryptographic attacks.

A. Image Input and Preprocessing

The process begins with users providing an input image for encryption. The system reads the image using image processing libraries such as OpenCV and converts it into a suitable format (grayscale or RGB matrix). Preprocessing steps such as resizing, normalization, and noise handling are applied to ensure uniformity and improve the efficiency of further operations.

B. Chaotic Map-Based Key Generation

A chaotic map (such as the Tent Map or Logistic Map) is used to generate highly sensitive and pseudo-random sequences. These sequences act as encryption keys and are extremely dependent on initial parameters. Even a slight change in initial conditions produces entirely different outputs, ensuring strong security and unpredictability.

C. Pixel Permutation (Confusion Stage)

Using the generated chaotic sequences, the pixels of the image are rearranged (permuted). This step breaks the strong correlation between adjacent pixels, making the image visually unrecognizable. The permutation process ensures that the original structure of the image is completely altered.

D. Pixel Diffusion (Encryption Stage)

After permutation, pixel values are modified using chaotic sequences and mathematical operations such as XOR. This diffusion process spreads the influence of each pixel across the image, enhancing security and making it resistant to statistical and differential attacks.

E. Deep Learning-Based Transformation

A deep learning model (such as a CNN or autoencoder) is integrated to further strengthen encryption. The model learns complex patterns and transformations, enhancing randomness and improving decryption accuracy. It also assists in reconstructing the original image with minimal loss.

F. Decryption Process

The decryption process applies the inverse operations in reverse order. Using the same chaotic keys , the system performs reverse diffusion and inverse permutation to reconstruct the original image. Accurate key matching ensures lossless or near-lossless recovery of the image.

G. System Architecture and Implementation

The system is implemented using Python with libraries such as OpenCV, NumPy, and TensorFlow/PyTorch for deep learning. The architecture includes modules for preprocessing, chaotic key generation, encryption, decryption, and result visualization.

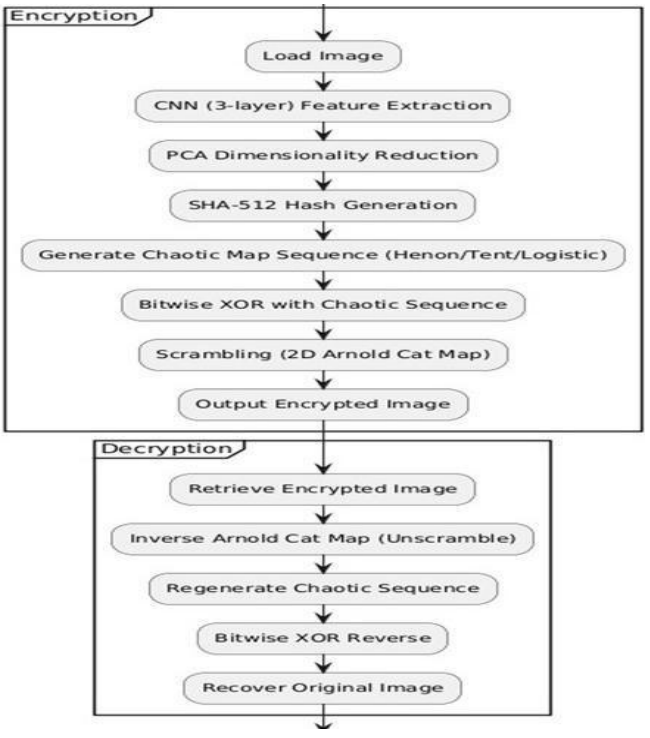

Fig.1.Proposed work Model

IV. TECH STACK

A. Frontend Technologies

The frontend of the system can be developed using Flask, providing a simple and interactive user interface. It allows users to upload images, perform encryption and decryption, and visualize results. The interface displays the original, encrypted, and decrypted images for easy comparison and analysis.

B. Backend Technologies

The backend is implemented using Python, which handles the core logic of image encryption and decryption. It manages image processing, chaotic key generation, deep learning model execution, and system workflow. The backend integrates all modules to ensure smooth and efficient processing.

C. Artificial Intelligence and Deep Learning

The system utilizes deep learning frameworks such as TensorFlow/Keras or PyTorch to build models like CNNs or autoencoders. These models help in enhancing encryption strength and improving decryption accuracy by learning complex image transformations and patterns.

D. Image Processing Libraries

For handling image-related operations, OpenCV is used for reading, processing, and transforming images. NumPy is used for efficient matrix operations and numerical computations, which are essential for pixel manipulation during encryption and decryption.

E. Chaotic Map Implementation

Chaotic maps such as the Tent Map are implemented using Python to generate pseudo-random sequences. These sequences are used as encryption keys for pixel permutation and diffusion, ensuring high sensitivity and strong security.

F. Encryption and Decryption Mechanism

The system applies a combination of pixel permutation (confusion) and pixel diffusion (XOR operations) using chaotic sequences. During decryption, inverse operations are performed using the same keys to accurately reconstruct the original image.

G. Security and Key Management

The system ensures high security through sensitive key generation using chaotic maps. Even a slight variation in initial parameters results in completely different encrypted outputs. Secure handling of keys is essential to prevent unauthorized access and ensure reliable decryption.

H. Development Tools and Environment

The project is developed using Visual Studio Code . Libraries and dependencies are handled using Python's package ecosystem. The system is modular and can be extended or deployed for real-world secure communication applications.

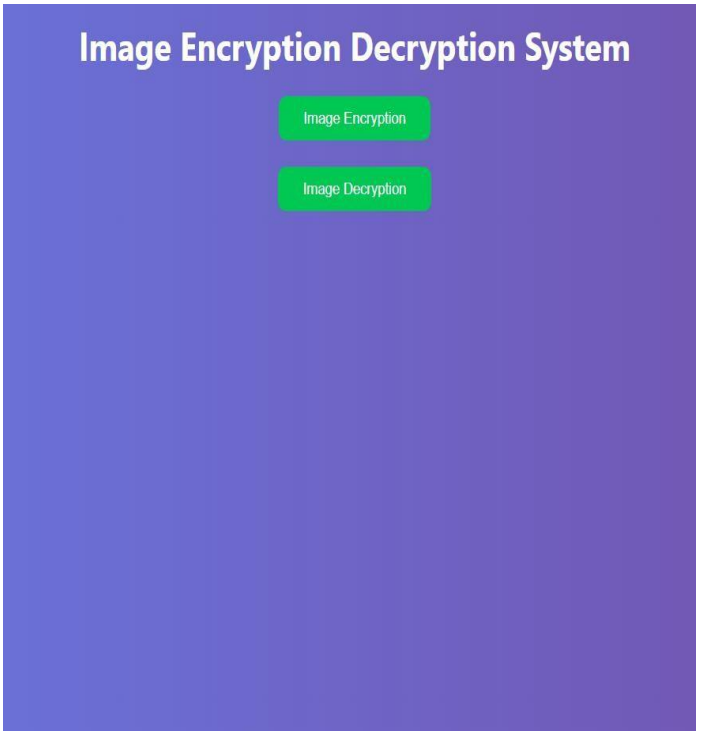

Fig. 2. Home Page

V. RESULTS

The developed Image Encryption and Decryption System using Deep Learning and Chaotic Map successfully demonstrates the practical application of advanced security techniques in digital image protection. The system is capable of providing secure, efficient, and reliable encryption of image data by combining chaotic map-based randomness with deep learning models.

The results show that the system effectively transforms original images into highly secure encrypted formats, making them visually unrecognizable and resistant to various attacks. At the same time, the decryption process accurately reconstructs the original image with minimal or no loss of information when correct keys are applied.

Overall, the proposed system proves to be a robust solution for secure image transmission and storage. It enhances data privacy, improves resistance against common cryptographic attacks, and ensures efficient performance. The project demonstrates that integrating chaotic maps with deep learning techniques can provide a powerful and practical approach for modern image security applications.

VI. CONCLUSION

The proposed Image Encryption and Decryption System using Deep Learning and Chaotic Map demonstrates how combining chaos theory with deep learning techniques can provide a highly secure, efficient, and adaptive solution for image protection. By integrating chaotic key generation, pixel permutation, diffusion processes, and neural network-based transformations, the system ensures strong encryption while maintaining accurate decryption.

The workflow ensures that each stage of encryption introduces high randomness and sensitivity, making the encrypted image resistant to statistical, brute-force, and differential attacks. The use of chaotic maps strengthens key unpredictability, while deep learning enhances transformation complexity and improves reconstruction accuracy.

This combination results in a system that is both secure and reliable.

The layered design of permutation, diffusion, and learning-based transformation creates a robust encryption pipeline rather than a single static approach. This makes the system more dynamic and difficult to break compared to traditional methods. Additionally, the ability to accurately reconstruct the original image highlights the effectiveness of the proposed model.

Overall, the system provides a scalable and practical framework for modern image security applications. It can be extended to secure video data, integrated with cloud-based storage systems, or enhanced with more advanced deep learning architectures. The project establishes a strong foundation for future developments in intelligent and adaptive multimedia security systems and demonstrates the potential of combining chaotic systems with AI for advanced cryptographic solutions.

REFERENCES

1. Ahmed, F., et al. Image Cryptography with Autoencoders using Chaotic Maps. GitHub Repository, 2023.
2. Zhang, L., et al. Image Encryption Algorithm Combining Chaotic Image Encryption and CNN. MDPI Electronics, 2022.
3. Kumar, S., et al. Efficient Image Encryption Using Deep Neural Networks and Chaotic Maps. ScienceDirect, 2020.
4. Wang, Y., et al. Deep Learning for Image Encryption: Enhancing Security and Efficiency. ScienceDirect, 2023.
5. Chen, X., et al. Image Encryption using Chaotic Logistic Mapping and DNA Encoding. arXiv, 2020