Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

AI-Driven Chaotic System for Secure Image Encryption and Decryption using Simulink

Dr L Rangaiah
Dean-Academics,
RajaRajeswari College of Engineering, Bengaluru
academicdean@rrce.org

Apoorva S
Student, Department of ECE,
RajaRajeswari College of Engineering, Bengaluru
siddarajuapoorva@gmail.com

Harshitha V M
Student, Department of ECE,
RajaRajeswari College of Engineering, Bengaluru
harshithavm2@gmail.com

Kavyashree D R
Student, Department of ECE,
RajaRajeswari College of Engineering, Bengaluru
kavyashreedr123@gmail.com

Maithry S Rao
Student, Department of ECE,
RajaRajeswari College of Engineering, Bengaluru
manyasistermy3@gmail.com

Abstract: ***This research proposes an AI-driven chaotic system for a secure image encryption and decryption using the Simulink. This proposed system leverages the unpredictability of the chaotic maps and the intelligence of the Artificial neural networks (ANN) to generate secure encryption keys. The chaotic system is designed to provide high sensitivity to initial conditions, ensuring the confidentiality and the integrity of image data. The AI-driven approach ensures adaptive encryption and decryption, making the system resilient to cyber threats. Simulation results demonstrate the productiveness of the proposed system in securing image data, showcasing its potential for applications in the data protection and also in the cybersecurity. An efficient ANN-based chaotic system for the image encryption and decryption is implemented in Simulink and MATLAB using the Xilinx System Generator (XSG)l. The generated Verilog code from the XSG is executed in Vivado for pixel distribution, enabling hardware-level optimization. Security tests, including histogram analysis, MSE, PSNR, SNR, SSIM, and confirmed successful encryption. The system's analysis and visualization, conducted within the Simulink, MATLAB, and Vivado, confirm its effectiveness***

Keywords— Artificial Neural Networks (ANN), Chaotic Systems, Simulink, Vivado, Xilinx System Generator (XSG).

I. INTRODUCTION

In recent years, image encryption, being a significant area of information security, has attracted a large number of researchers and scientists. Numerous studies using various methodologies have been implemented, and novel and useful algorithms have been proposed to improve safe image encryption schemes. Digital images encryption approaches based on chaotic systems are novel techniques. This technology encrypts images using random chaos sequences and is a very secure and fast method of image encryption. The usage of chaotic systems in cryptography to get encrypt images has been proposed as a possible solution to a variety of security problems due to their numerous advantages over random characteristics such as sensitive dependency on the basic conditions and the parameter are settings, simplicity of design, and aperiodic signal, which makes them an ideal option for cryptography. The method used, which is artificial neural network (ANN)-based Chua chaotic system (CCS), was simpler, more effective, and produced good results as compared to other complex methods of image hiding, such as chaotic block image permutation and XOR operations are performed to achieve image encryption [1] The reliable storage and transmission of digital images are paramount in various applications, including multimedia systems, medical imaging, and military imaging systems.

Encryption methods, such as DES (Data Encryption Standard) or AES (Advanced Encryption Standard), are commonly utilized for securing textual data. However, when applied to image data, traditional encryption techniques face particular hurdles due to the unique characteristics inherent in visual content. Therefore, image encryption techniques need to consider these characteristics specifically to achieve effective encryption of image data [4].

As an important cryptographic technology, chaotic cryptography combines chaotic theory and cryptography and constantly improves its theoretical system. This technique has been widely studied due to the chaotic characteristics of such systems. A typical chaos-based algorithm of the image encryption was proposed. The algorithm combines confusion and diffusion in traditional cryptography, which firstly utilizes Arnold's cat map to mix up the positions of plain-image pixels to introduce diffusion [2].

This project explores the usage of chaotic systems for image encryption and decryption. By leveraging the unpredictability of chaotic systems, a secure and efficient encryption model is developed. This approach offers a modern solution to improve the security and also the reliability of image data protection. Traditional algorithms of encryption are often not optimized for image processing, specifically those related to real-time applications. On addressing this, chaotic systems, which are vastly used for its sensitivity to inceptive conditions and randomness are combined with Artificial Intelligence (AI) using ANN model to develop robust, real-time image encryption techniques. Simulink, a graphical programming environment integrated with MATLAB, offers a powerful platform for modeling such systems. This structure was efficiently designed on a field-programmable gate array (FPGA) chip utilizing the Xilinx system generator (XSG) tool present in the MATLAB. Security tests, including histogram analysis, MSE, PSNR, SNR, SSIM, and confirmed successful

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

encryption. The system's analysis and visualization, conducted within Simulink, MATLAB, and Vivado, confirm its effectiveness.

II. CHAOS SYSTEMS

A chaotic system is a **nonlinear dynamical system** that is governed by deterministic mathematical rules, also exhibits behavior that is so complex and sensitive to its starting point that it appears to be completely random.

Let us understand the core properties of chaos systems:

1. Sensitivity to Initial Conditions –

This is a famous characteristic. It says that an infinitesimally minute change in the inceptive conditions (initial values) of the system will lead to an exponentially broader divergence in the system output over time. This characteristic is directly utilized to produce highly sensitive encryption keys. If an attacker attempts a brute-force attack by slightly varying the key's basic parameters, the output sequence will be completely different, making it impossible for decrypting the data. The basic parameters of chaotic map are typically used as the secret key.

2. Deterministic and Reproducible –

Although the output appears random, the system is fundamentally deterministic. Given the exact same inceptive conditions and the parameters, the system will always generate the exact same sequence. This is the property that makes decryption possible. The sender (encryptor) and receiver (decryptor) must agree on the exact same secret key (initial conditions and parameters). The decryption process simply runs the chaotic map forward from the same key to regenerate the identical chaotic sequence that was used for the encryption. Using this identical sequence, the inverse operations (e.g., inverse permutation, and repeated XOR) are executed to retrieve original image perfectly.

Numerous chaos systems have been proposed, including some with simple structures and chaotic orbits, such as 1 dimensional chaos systems like logistic maps, and others with the higher dimensions, exhibiting complex chaotic behaviors and orbits. Considering the maximization of encryption efficiency, the proposed scheme of encryption employs two efficient chaotic mappings.

Two Major phases involved in Chaotic systems are:

- Permutation (Scrambling Phase):

Permutation is the first phase of chaotic image encryption, and its purpose is to shuffle the positions of pixels in the image so that visual information is completely disrupted. A chaotic map such as the Arnold's cat map and Baker's map is carried out to prompt a sequence of random-like values that determine the new ordering of pixel positions. This chaotic sequence is then sorted or indexed to form a permutation pattern, which is applied to the image either row-wise or column-wise, or by first converting the image into a one-dimensional array. As a result, the structure, patterns, and neighboring pixel relationships of original image are destroyed. This step significantly increases the security by preventing attackers from exploiting spatial correlations in the image.

- Diffusion (Confusion Phase):

Diffusion is the second phase of chaotic image encryption and focuses on altering the **intensity values** of permuted pixels. In this phase, another chaotic sequence is prompted, which is transformed into a key stream with values typically ranging 0 to 255 to equal the pixel range. This key stream is then mixed with the permuted image through operations such as bitwise XOR or addition modulo 256. In some designs, a feedback mechanism is used where each encrypted pixel also rely upon the previously encrypted pixel, ensuring that minute modification in the original image produce large variations in the encrypted output—an effect known as the avalanche effect. By modifying pixel values in this highly sensitive manner, the diffusion step ensures that statistical data of the original image is fully concealed, making the encryption non-compliant to differential and statistical attacks.

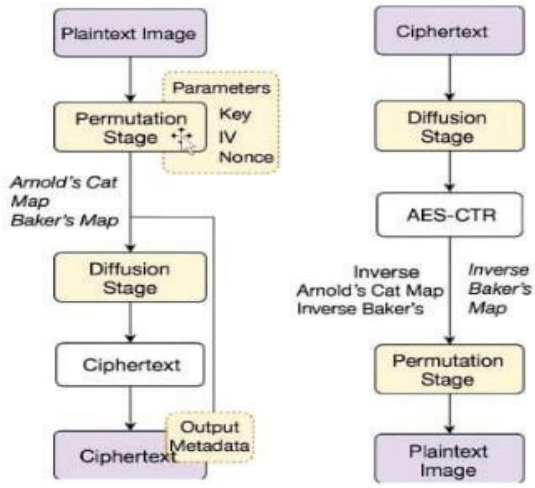


Fig 1. Encryption and Decryption flow diagram

A. Arnold's cat Map :

Arnold's cat map is a chaotic mapping method for the repeated folding and enlargening transformation in a finite region. Assume that we have an original grayscale image P of size N × N with pixel coordinates S = {(x, y) | x, y =0,⋯ ,N−1}. In image encryption, the Arnold map works by taking each pixel location (x ,y) of N×N image and computing new coordinates (x′ ,y′) using a special transformation matrix. This operation destroys the pixel relationships and produces a scrambled output.

The Arnold's cat map can be expressed as,

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (\text{Mod } n)$$

B. Baker's Map :

The Baker's Map, also known as the Baker's Transformation, is a classical chaotic map used for scrambling data such as images. It gets its name from the process a baker uses to knead dough stretching, folding, and flattening it similar to how the given image is stretched and rearranged for the production of a chaotic output. The map operates on unit square and transforms input coordinates (x, y) into new coordinates through a series of stretching, cutting, and stacking operations. By repeatedly applying the baker's map, image becomes more and more scrambled, it will be difficult for an attacker to retrieve any meaningful information without correct parameters.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

III. RELATED WORK

The usage of chaotic systems in cryptography to encrypt images has been proposed as a possible solution to a variety of security problems due to their numerous advantages over random characteristics as sensitive dependency on initial conditions and parameter settings, simplicity of design, and aperiodic signal, which makes them an ideal option for cryptography systems. Artificial intelligence techniques have significant importance in modeling because of its ability to reason and learn in an environment of uncertainty, approximation, and imprecision. These techniques comprise a collection of new technologies that offer an alternate approach to mathematical modeling for nonlinear dynamics, an issue that permeates all fields of science. One of the most efficient and general modeling methods is ANN.

Fig 2. Simulink blocks for ANN based encryption

Select chaotic maps or systems, such as Arnold's cat Map and Baker's Map that is used to produce a key stream for encryption. The chaotic map's output can be used for key generation in encryption process. Then we have utilized AI techniques like Artificial Neural Networks (ANNs) to enhance key generation, improve encryption algorithms, and make the system adaptive to various conditions.

For instance, a neural network could predict potential key values or adapt the chaotic system's parameters for dynamic encryption based on image features. Before encryption, an image (usually in formats like JPEG, or PNG) is converted into a matrix format of pixel values. These pixel values are transformed to grayscale for simplicity, although color images can also be processed using RGB channels separate.

After that we applied permutation techniques (such as pixel shuffling) using chaotic sequences to further secure the image. The pixel positions are shuffled based on the chaotic sequence which we have used to generate the keys. During decryption, the chaotic map is reset to the same initial conditions and parameters (seed value) as used during encryption. The ANN based model may be used to ensure that the chaotic sequence is correctly synchronized with the encryption process.

Finally, we implemented the chaotic map, key generation, then the encryption, and the decryption processes within Simulink.

IV. METHODOLOGY

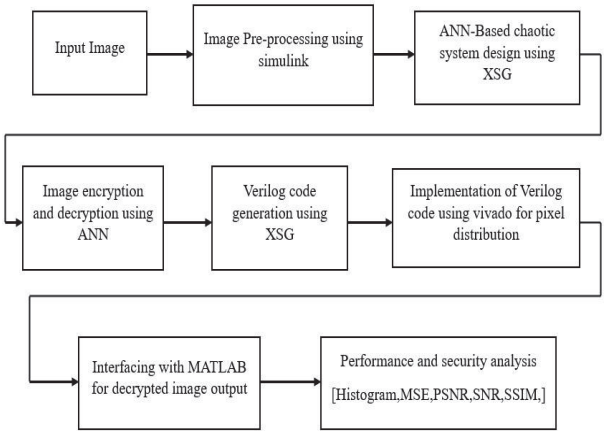


Fig 3. Methodology used in ANN encryption using Simulink

The process starts with an input image, which will undergo encryption and decryption. The input image should be in the format .jpg or .png. And the next step is preprocessing the image in Simulink. In Simulink (MATLAB-based tool) there are many blocks such as resizing, filtering, or converting the image into a suitable format. We can also used 2D to 1D convertor and buffer to store the pixels of the image.

Then we designed an ANN model which is carried out to start a chaotic sequence for encryption. XSG is a tool within MATLAB that allows FPGA-based hardware implementation of the ANN model. The chaotic sequence which is generated by the ANN will be applied to the image for the encryption. The decryption process inverses the encryption using ANN. The inverse operations of diffusion and permutation reconstruct the original image utilizing the same chaotic keys.

The production of chaotic key streams is one of the most critical components of the system. In this work, chaotic maps are controlled and optimized using AI-driven techniques that automatically tune initial values and map parameters based on randomness assessment metrics. The AI ensures that the generated chaotic sequences exhibit strong unpredictability, high entropy, and also sensitivity to even minimal changes in initial values. This optimization improves the strength of both permutation and diffusion phases, issuing an extra layer of security beyond conventional chaotic systems.

Once the Simulink model is validated, XSG is used to generate Verilog code for hardware synthesis. The generated HDL code is imported into Vivado, where simulations verify correct pixel manipulation and encryption patterns. This hardware validation ensures that the system is not limited to software environments but can be implemented on FPGA boards for real-time encryption applications. The hardware design focuses on maximizing speed, reducing latency, and optimizing FPGA resource consumption.

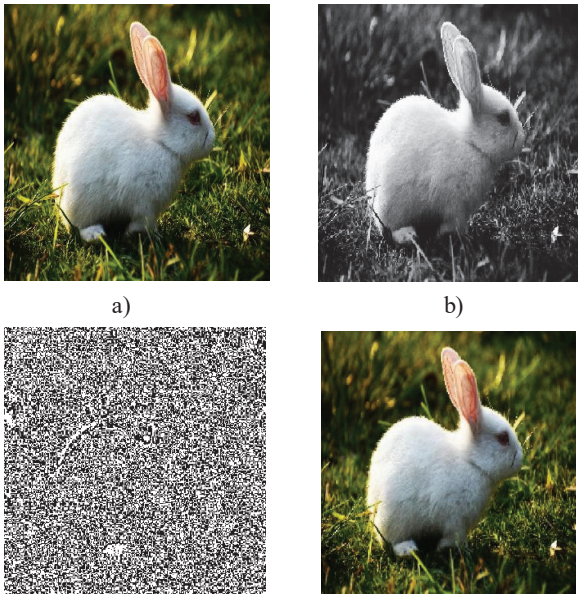
The decrypted image is retrieved and displayed in MATLAB for verification. Various performance metrices are calculated between decrypted image and the original image these includes the mean square error, histogram analysis, peak signal to noise ratio, entropy, the structural similarity index measure and correlation coefficient all these security analysis are carried out to ensure a secure and reliable system for encryption.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

V. RESULTS AND DISCUSSION

A. Simulink Outputs :

The output from the Simulink blocks are processed as below



a) b) c) d)

Fig 4. a) Original Image, b) Greyscale Image, c) Encrypted Image, d) Decrypted Image

B. Performance and Security Analysis :

Numerous analysis are presented to evaluate the proposed algorithms' efficiency and security, including the histograms, the correlation coefficients, the information entropy, the key space, and the differential attack analysis. This section applies the study to an image of 256*256 size. Experiments are conducted and data analysis is performed using a MATLAB environment.

1. Histogram analysis:

The histogram is a useful statistical function that illustrates the distribution of pixel values by graphing the number of pixels at each color intensity level. It is commonly used to test image encryption algorithms' accuracy. A successful encryption algorithm has to produce the encrypted images with uniformly distributed histograms [1].

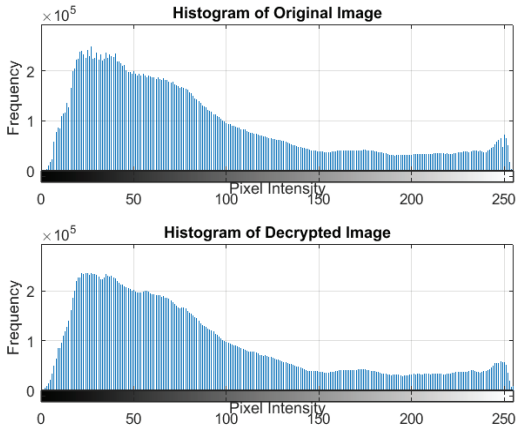


Fig 5. Histogram of Original image and decrypted image

2. Mean Square Error (MSE):

In the image encryption process, Mean Square Error (MSE) is used for measuring how different the encrypted image is from the original image. In image decryption, MSE is used to measure how similar the decrypted image is to the original image.

Low MSE suggests that there are not much difference between both original image and encrypted image.

Our suggested model has given MSE = 0.582

3. Peak Signal to Noise Ratio (PSNR):

Peak Signal-to-Noise Ratio (PSNR) is the vastly used quality-measurement metric which tells how similar two images are. PSNR measures the ratio between the maximum possible pixel value and the distortion (error) between two images. Higher PSNR means better quality, meaning the images are very similar.

PSNR for our model is 50.479 dB

4. Structural Similarity Index Measure (SSIM):

SSIM is an advanced image quality metric that calculates similarity between the two images based on their structure, luminance, and contrast. It is considered more accurate than PSNR and MSE because it focuses on how humans perceive images. SSIM values range from 0 to 1, where values close to 1 indicate high similarity (useful for assessing decrypted images). We need to get high SSIM, close to 1, meaning the decrypted image matches the original structurally.

Our SSIM = 0.8289 which indicates that good similarity is there between the images.

5. Entropy:

Entropy is a statistical measure that indicates the degree of randomness or unpredictability in an image. In image encryption, entropy is used for evaluating the security of encrypted image.

We calculated entropy for both original image and decrypted image and the results are as below

Entropy (Original Image) = 7.6102

Entropy (Decrypted image) = 7.6078

As we can see that both the values are almost equal.

6. Number of Pixel Change Rate (NPCR):

The Number of Pixel Change Rate (NPCR) evaluates the sensitivity of image encryption algorithm by measuring how many pixels change in encrypted image when a single pixel in original image is modified. A high NPCR value (typically above 99.6%) indicates strong diffusion capability, meaning the encryption algorithm effectively spreads small changes across the entire image, making it highly resistant to differential attacks.

NPCR = 99.79% This implies that our encryption is highly sensitive and secure.

7. Correlation Coefficient:

The correlation coefficient is a statistical measure used to examine the relationship between the neighboring pixels in an image. Natural images have high correlation because adjacent pixels are often similar in intensity. However, a safe encrypted image must eliminate this similarity entirely. Therefore, the correlation of adjacent pixels in an encrypted image should be close to zero or negative. This shows that the encryption algorithm produces a highly random output, making it difficult for the hackers to identify patterns.

Correlation coefficient of our model is 0.0017 this suggests that the neighboring pixels in encryption are not related.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

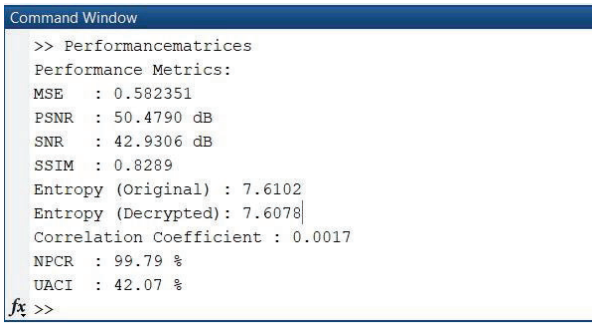


Fig 6. Values of all performance metrices

VI. CONCLUSION

The proposed AI-driven chaotic image encryption and decryption system successfully demonstrates a powerful integration of chaos theory, artificial intelligence, and hardware-oriented design tools such as Simulink and Xilinx System Generator. By combining permutation and diffusion mechanisms with AI-optimized chaotic key generation, the system achieves strong security, high sensitivity to initial conditions, and excellent resistance to statistical, differential attacks. The Simulation results in MATLAB and hardware validation using Vivado confirms that this model not only maintains the high encryption quality but is also suitable for real-time FPGA implementation. Overall, the work provides a robust, efficient, and scalable encryption framework which can also be applied to the secure communication in critical fields such as healthcare, defense, and financial data transmission.

The integration of AI with chaotic systems presents a promising direction for secure image encryption. By utilizing the randomness and high sensitivity of the chaotic maps alongside the adaptive learning capability of AI, a more strong and intelligent encryption system can be achieved. Implementing this within the Simulink environment adds further value by allowing real-time simulation, visualization, and performance analysis of the encryption and the decryption processes. Such system not only strengthens image security through better entropy and key sensitivity but also opens avenues for scalable and application-specific customization, such as in IoT, medical imaging, and defense systems. In conclusion, the AI-driven chaotic encryption framework stands as a significant advancement over traditional approaches, addressing their key shortcomings and setting a new benchmark in intelligent multimedia security.

VII. FUTURE SCOPE

The proposed system opens several promising avenues for future development. One of the most significant enhancements would be extending the model to support real-time video encryption, enabling secure multimedia communication in surveillance and telemedicine applications. Additionally, integrating more advanced AI techniques such as deep learning or reinforcement learning could further optimize chaotic parameters and improve the adaptability of the encryption process under dynamic conditions. Future work may also explore hybrid multi-chaotic systems to strengthen security and reduce predictability. Implementing the design on physical FPGA boards will allow real-world benchmarking of latency, power consumption, and throughput.

Finally, expanding the system to support color images, medical imaging standards such as DICOM, and IoT-based secure transmission platforms would broaden its applicability across modern digital communication environments.

VIII. REFERENCES

[1]. Wisal Adnan Al-Musawi, Mohammed Abd Ali Al-Ibadi, Wasan A. Wali Y, “Artificial intelligence techniques for encrypt images based on the chaotic system implemented on field- programmable gate array.” Vol. 12, No. 1, March 2023, pp. 347~356

[2]. F. S. Hasan and M. A. Saffo, “FPGA hardware co-simulation of image encryption using stream cipher based on chaotic maps,” Sensing and Imaging, vol. 21, no. 1, p. 35, Dec. 2020, doi: 10.1007/s11220-020-00301.

[3]. R. A. Aboughalia and O. A. S. Alkishriwo, “Color image encryption based on chaotic block permutation and XOR operation,” arXiv preprint arXiv:1808.10198, Aug. 2018,

[4]. S. Čelikovský and V. Lynnyk, “Message embedded chaotic masking synchronization scheme based on the generalized Lorenz system and its security analysis,” International Journal of Bifurcation and Chaos, vol. 26, no. 8, p. 1650140, Jul. 2016, doi: 10.1142/S0218127416501406.

[5]. Li, Q., Ma, B., Wang, X., Wang, C. & Gao, S. Image steganography in color conversion. IEEE Trans. Circuits Syst. II Express Briefs (2023).

[6]. S. Saudagar et al., "Image Encryption based on Advanced Encryption Standard (AES)," 2023 International Conference for Advancement in Technology (ICONAT), Goa, India, 2023, pp. 1-4

[7]. D. M. Alsaffar et al., "Image Encryption Based on AES and RSA Algorithms," 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 2020, pp. 1-5

[8]. Mimetic: Mobile encrypted traffic classification using multimodal deep learning. Computer Networks, G.Aceto, D.Ciuonzo, A.Montieri, and A.Pescape. Mimetic 165:106944,2019.

[9]. K. Tajik, A. Gunasekaran, R. Dutta, B. Ellis, R. B. Bobba, M. Rosulek, C. Wright, V, and W.-c. Feng, “Balancing image privacy and usability with thumbnail-preserving encryption,” in the 26th Annual Network and Distributed System Security Symposium (NDSS 2019), 2019.

[10]. M. Gong, X. Chai, Y. Lu, and Y. Zhang, “Exploiting four-dimensional chaotic systems with dissipation and optimized logical operations for secure image compression and encryption,” for Video Technology, 2024.

[11]. R. Lin, S. Liu, J. Jiang, S. Li, C. Li, and C.-C. J. Kuo, “Recovering sign bits of DCT coefficients in digital images as an optimization problem,” Journal of Visual Communication and Image Representation, vol. 99, p. 104045, 2024.

[12]. M. Gong, X. Chai, Y. Lu, and Y. Zhang, “Exploiting four-dimensional chaotic systems with dissipation and optimized logical operations for secure image compression and encryption,” for Video Technology, 2024.

[13]. P. Kong, A. Li, D. Guo, L. Zhou, and C. Qin, “Joint lossless compression and encryption for medical images,” for Video Technology, pp. 1–1, 2023.