

Machine Learning-Optimized Hybrid Chaotic Map for Secure Image and Multimedia Encryption in IoT

SAYED ATHAR ALI HASHMI

hashmi_athar@hotmail.com

Department of Higher Education, Raipur, Chhattisgarh, India <https://orcid.org/0009-0004-5070-1902>

Pushpendra Tiwari

Department of Higher Education, Raipur, Chhattisgarh, India <https://orcid.org/0009-0006-3835-0913>

Research Article

Keywords: Machine learning optimization, Hybrid chaotic map, Image encryption, Multimedia encryption, IoT security, Power consumption

Posted Date: April 22nd, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-9456970/v1>

License:   This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: The authors declare no competing interests.

Abstract

This study proposes a Machine Learning-Optimized 3D Hybrid Chaotic Map (Logistic–Tent–Hénon–Chebyshev) for secure and energy-efficient encryption of images and multimedia data in resource-constrained IoT and edge computing environments. Four classical chaotic maps—Logistic, Tent, Hénon, and Chebyshev—are coupled using modular arithmetic to construct a novel 3D hybrid chaotic system. The parameters of this hybrid map are dynamically optimized by integrating Non-dominated Sorting Genetic Algorithm-II (NSGA-II) with a Back-Propagation Neural Network. The network takes the SHA-256 hash of the plain image as input to generate adaptive initial conditions and control parameters. The encryption scheme employs SHA-256 key generation, pixel confusion via a generalized Arnold cat map, and dual diffusion using two independent chaotic sequences. The proposed method supports both static images and video frame sequences and is validated on embedded hardware platforms including Raspberry Pi 5 and Jetson Nano.

Experimental results on standard benchmark images and video sequences demonstrate superior performance, achieving an information entropy of 7.9978, NPCR of 99.68%, UACI of 33.52%, near-zero correlation coefficients (≈ 0.001), and successful passage of all NIST statistical tests. For a 256×256 image, the scheme requires only 78 ms encryption time and real-time power consumption of 92 mW on Raspberry Pi 5 and Jetson Nano, significantly outperforming AES-256 and recent hybrid chaotic schemes in security, speed, and energy efficiency.

Unlike existing approaches, the proposed method performs dynamic ML-based parameter optimization with real-time power evaluation on embedded IoT platforms.

1. Introduction

In the era of rapid digital transformation, the transmission of images and multimedia content has increased exponentially, particularly in Internet of Things (IoT), edge computing, telemedicine, surveillance systems, and real-time communication applications [1]. With the proliferation of connected devices, securing sensitive visual data against unauthorized access, interception, and manipulation has become a critical challenge. Traditional cryptographic algorithms such as AES, while secure for textual data, often suffer from high computational overhead and are not always suitable for resource-constrained IoT devices due to their power and processing limitations [2]. Recent studies have also explored deep learning integration with chaotic maps specifically for medical and IoT image security (Abirami et al., 2025; Asiri et al., 2025).

Chaotic map-based encryption techniques have gained significant attention in recent years because of their inherent properties such as ergodicity, extreme sensitivity to initial conditions, pseudo-randomness, and topological transitivity, which closely resemble the requirements of cryptographic systems [3]. These properties enable effective confusion and diffusion operations essential for secure image and multimedia encryption. However, traditional single chaotic maps frequently encounter limitations

including small key space, periodic windows, weak key sensitivity, and high correlation in encrypted images, making them vulnerable to statistical, differential, and known-plaintext attacks [1, 4].

To overcome these drawbacks, researchers have explored hybrid and hyperchaotic systems that combine multiple chaotic maps to expand the chaotic range and improve overall performance [5, 6]. More recently, the integration of machine learning (ML) optimization techniques such as Genetic Algorithm and NSGA-II with neural networks has emerged as a promising direction to dynamically tune chaotic parameters, enhance randomness, and achieve a better trade-off between security, computational efficiency, and energy consumption [7, 8].

Despite these advancements, several research gaps persist. Most existing schemes focus primarily on image-only encryption and address only one or two performance aspects (either security or efficiency) [9]. Very few studies provide a unified framework that simultaneously supports image and multimedia (video frames) encryption, incorporates machine learning-based dynamic optimization of a hybrid chaotic map, performs direct comparative analysis with both recent chaotic schemes and the standard AES algorithm, and evaluates real-time power consumption on embedded hardware platforms [2, 10].

This paper addresses these gaps by proposing a Machine Learning-Optimized 3D Hybrid Chaotic Map (Logistic–Tent–Hénon–Chebyshev) for secure and energy-efficient image and multimedia encryption. The proposed scheme integrates a novel 3D hybrid chaotic system (constructed by coupling Logistic, Tent, Hénon, and Chebyshev maps using modular arithmetic) with ML-based parameter optimization using Non-dominated Sorting Genetic Algorithm-II (NSGA-II) combined with a Back-Propagation Neural Network. The neural network takes the SHA-256 hash of the plain image as input to generate adaptive initial conditions and control parameters. This dynamic, image-dependent optimization enhances randomness and attack resistance. The encryption process employs SHA-256 key generation, pixel confusion via a generalized Arnold cat map, and dual diffusion using two independent chaotic sequences. The methodology supports both static images and video frame sequences and is validated on embedded hardware platforms including Raspberry Pi 5 and Jetson Nano.

The major contributions of this work are as follows:

- Development of a novel 3D hybrid chaotic system by coupling four classical maps with modular arithmetic for enhanced chaotic range and randomness.
- Integration of a Back-Propagation Neural Network with NSGA-II for dynamic and image-dependent optimization of chaotic parameters.
- Unified framework supporting both static images and multimedia (video frames) encryption.
- Comprehensive security, efficiency, and power consumption evaluation with direct quantitative comparison against AES-256 and state-of-the-art chaotic schemes.

- Real hardware validation on Raspberry Pi 5 and Jetson Nano demonstrating practical applicability in IoT and edge computing environments.
- Comprehensive real-time power and throughput analysis on Raspberry Pi 5 and Jetson Nano, with direct quantitative comparison to AES-256 and state-of-the-art schemes.

The remainder of the paper is organized as follows: Section 2 presents a detailed literature review with a comparative analysis of existing works. Section 3 describes the proposed methodology. Section 4 presents the experimental results and performance evaluation. Finally, Section 5 concludes the paper with limitations and future research directions.

2. Literature Review

In recent years, image and multimedia encryption has witnessed significant advancements through the integration of hybrid and hyperchaotic maps with machine learning (ML) optimization techniques. These approaches aim to achieve higher security, better computational efficiency, and reduced power consumption [1, 2]. Traditional single chaotic map-based schemes often suffer from limited chaotic range, weak key sensitivity, and high correlation in encrypted images, making them vulnerable to statistical and differential attacks [3].

To address these limitations, researchers have increasingly employed optimization algorithms (such as Genetic Algorithm, NSGA-II, and Fireworks Algorithm) along with neural networks (CNN, BP NN, Autoencoder, and EfficientNet) for dynamic parameter tuning of chaotic systems [4, 5].

Several studies have focused on hybrid chaotic systems and multi-objective optimization. Gao et al. [6] proposed an enhanced 3D hybrid chaotic system by coupling discretized Lorenz and Chebyshev maps and applied NSGA-II to maximize entropy and minimize autocorrelation, reporting improved NPCR, UACI, and entropy values. Tiwari et al. [7] combined a stacked autoencoder with optimized 3D chaotic maps to enhance both compression and encryption efficiency.

Hardware implementation and power efficiency have also received attention. Ulutas et al. [8] developed a memristor-based hyperchaotic hybrid system integrated with DNA operations and lightweight 3DES on NVIDIA Jetson TX2, demonstrating strong security with low-power performance. Raj et al. [9] presented a 5D memristive hyperchaotic map on FPGA and provided explicit power consumption analysis (135.4 mW) with detailed trade-off evaluation.

Genetic Algorithm-based optimization has been explored for chaotic maps and S-box design by Kumar et al. [10] and Farwa et al. [11]. Liang et al. [12] proposed a compression-encryption scheme using BP neural network optimized by the Fireworks Algorithm. Subathra et al. [13] employed EfficientNet B3 to guide a multi-scroll chaotic map for adaptive encryption, while Liu et al. [14] and Zhang et al. [15] investigated reversible neural networks and CNN-based memristor chaotic systems.

For multimedia and multiple-image encryption, Alexan et al. [16] developed schemes using 5D hyperchaotic systems with modified RC5 and SVD. Hoang et al. [17] proposed parallel multiple-image encryption with FPGA implementation and compared hardware efficiency and power consumption against AES variants.

Recent Taylor & Francis and other high-impact studies have further strengthened this direction by incorporating multi-chaotic systems, bit-plane permutation, and deep learning integration, particularly for medical and IoT applications. Abirami et al. [18] introduced an optimized chaos method combined with customized deep learning for secure DICOM medical image encryption and watermarking. Farandi et al. [19] enhanced encryption security through integration of multi-chaotic systems with mixed pixel-bit level permutation. Barik et al. [20] proposed an AES-chaos hybrid model with neural elements for improved image data security.

Zia et al. [3] provided a comprehensive survey on chaotic map-based image encryption techniques, emphasizing the ongoing shift toward hybrid, ML-optimized, and hardware-aware designs.

Table 1: Comparison of Existing Works with the Proposed Scheme

Reference	ML / Optimization Type	Power Analysis	AES / Block Cipher Comparison	Multimedia Support	Main Focus
Gao et al. (2025)	NSGA-II (Multi-objective GA)	No	No	Image only	Hybrid chaotic + offline optimization
Tiwari et al. (2025)	Stacked Autoencoder	No	No	Image only	Compression + 3D chaotic optimization
Ulutas et al. (2025)	None (DNA + hybrid)	Yes (Jetson TX2)	Yes (3DES)	Image only	Memristor hyperchaotic + embedded hardware
Raj et al. (2025)	None	Yes (FPGA, 135.4 mW)	No	Image only	5D hyperchaotic + hardware trade-off
Kumar et al. (2024)	Genetic Algorithm	No	AES-like	Image only	Chaotic + ECC + GA optimization
Farwa et al. (2025)	Genetic Algorithm	No	No	Image only	Optimized chaotic S-box
Liang et al. (2026)	BP NN + Fireworks Algorithm	No	No	Image only	Compression-encryption
Subathra et al. (2025)	EfficientNet B3 (Deep NN)	No	No	Image only	Adaptive encryption
Alexan et al. (2025)	None	No	Yes (modified RC5)	Multiple Images	Multiple image encryption
Hoang et al. (2025)	None	Yes (FPGA)	Yes (AES variants)	Multiple Images	Parallel multiple image + FPGA
Proposed Work	"dynamic optimization using image hash"	Yes (Embedded hardware)	Yes (Direct AES comparison)	Image + Multimedia	Unified ML-optimized hybrid chaotic map with efficiency, power & security comparison

Unified ML-optimized hybrid chaotic map with efficiency, power & security comparison

Although many studies have integrated optimization algorithms and neural networks with chaotic maps, most perform offline optimization and lack dynamic adaptation based on input image characteristics [6, 7, 13]. Moreover, very few schemes simultaneously support both image and multimedia (video frame) encryption while providing detailed real-time power consumption analysis on modern embedded platforms such as Raspberry Pi or Jetson series [8, 17].

The proposed scheme addresses these gaps by introducing dynamic ML-based parameter tuning using the SHA-256 hash of the plain image as input to the BP Neural Network, a unified framework for static images and video sequences, direct quantitative comparison with AES-256, and comprehensive evaluation of security, speed, and energy efficiency on actual embedded hardware.

3. Methodology

Methodology The research adopted a quantitative experimental design combining simulation-based development with real hardware validation. The study followed a systematic approach: (1) identification of research gaps through literature review, (2) design of a novel 3D hybrid chaotic system with machine learning optimization, (3) implementation and testing on standard benchmark datasets, (4) security, efficiency, and power consumption analysis, and (5) comparative evaluation with existing schemes and AES-256.

3.1 Research Design and Experimental Setup The proposed encryption scheme was implemented and tested using MATLAB R2024a and Python 3.11 on a workstation equipped with an Intel i7 processor and 16 GB RAM. For hardware validation and power analysis, the algorithm was deployed on two embedded platforms: Raspberry Pi 5 and NVIDIA Jetson Nano. Real-time power consumption was measured using an INA219 current sensor interfaced with the devices.

3.2 Dataset To ensure reproducibility and fair comparison, standard public benchmark datasets were used. **Image Dataset:** Ten grayscale and ten color images of sizes 256×256 and 512×512 were selected from the USC-SIPI Image Database. The test images include Lena, Baboon, Peppers, Airplane, Barbara, Boat, Cameraman, Goldhill, Zelda, and House. **Multimedia Dataset:** Five standard video sequences (Akiyo, Foreman, Coastguard, Container, and Hall Monitor) from public YUV video databases were converted into frame sequences. The first 100 frames of each video at 256×256 resolution were used. No private or copyrighted material was utilized in this study.

3.3 Hybrid Chaotic Map Generation Four classical chaotic maps — Logistic, Tent, Hénon, and Chebyshev — were coupled using modular arithmetic and iterative feedback to construct a novel 3D hybrid chaotic system. This coupling generates three independent high-dimensional chaotic sequences (X, Y, Z). The mathematical formulation of the proposed hybrid map is given in Appendix A (or Equation (1)–(3)). The chaotic behavior was rigorously validated through bifurcation diagrams, phase portraits, and the Lyapunov exponent spectrum, as shown in Figure 3. The bifurcation diagrams reveal wide chaotic regions without large periodic windows, the phase portraits exhibit complex space-filling strange attractors, and the Lyapunov exponents remain positive over a broad range of the control parameter β , confirming hyper-chaotic dynamics suitable for cryptographic applications. The validation is consistent with recent 3D/5D hyperchaotic analyses (Li et al., 2024). Detailed equations and pseudocode are provided in Appendix A.

3.4 Machine Learning-Based Parameter Optimization

A multi-objective optimization framework combining Non-dominated Sorting Genetic Algorithm-II (NSGA-II) and a lightweight Back-Propagation (BP) Neural Network was employed. The BP Neural Network was trained offline using NSGA-II to predict optimal initial conditions and control parameters for the hybrid chaotic map. The network takes the 256-bit SHA-256 hash of the plain image as input and outputs adaptive chaotic parameters.

The objective functions for NSGA-II were: (1) maximization of information entropy, (2) minimization of autocorrelation in the generated chaotic sequences, and (3) achievement of near-ideal NPCR and UACI values. This dynamic, image-dependent optimization enhances randomness and resistance against various attacks.

3.5 Key Generation

A 256-bit secret key combined with the SHA-256 hash of the plain image was used to derive initial seeds. These seeds were fed into the ML-optimized hybrid chaotic system to generate three independent chaotic sequences (X, Y, and Z).

3.6 Encryption Process

The encryption process consists of two main phases:

1. Confusion Phase: Pixel permutation is performed using chaotic sequence X through a generalized Arnold cat map.
2. Diffusion Phase: Forward diffusion is applied using sequence Y, followed by backward diffusion using sequence Z. Both diffusion stages utilize XOR and modular addition operations.

The same confusion-diffusion process is applied frame-by-frame for multimedia (video) encryption.

3.7 Decryption Process

Decryption is symmetric and follows the reverse operations: inverse diffusion using sequences Z and Y, followed by inverse permutation using sequence X.

3.8 Implementation and Performance Evaluation

The complete algorithm was implemented on the embedded platforms (Raspberry Pi 5 and Jetson Nano) for real-time evaluation. Encryption time, throughput, power consumption, and key security metrics were measured and compared with AES-256 and recent hybrid chaotic encryption schemes.

3.9 Hardware Implementation Details

Real-time power consumption was measured using an INA219 current sensor interfaced via I2C with the Raspberry Pi 5 and Jetson Nano. All embedded tests were conducted under controlled ambient conditions to ensure repeatable and accurate power readings.

4. Results

The performance of the proposed Machine Learning-Optimized 3D Hybrid Chaotic Map was thoroughly evaluated through extensive experiments on standard grayscale and color images (256×256 and 512×512 resolution) as well as video sequences. The evaluation focused on three key aspects: security strength, computational efficiency, and power consumption. All results were compared with the standard AES-256 algorithm and the average performance of recent hybrid chaotic encryption schemes from the literature.

4.1 Visual Quality Analysis The encrypted images produced by the proposed scheme appear completely random and noise-like, with no visible information from the original image. The histograms of the cipher images are nearly uniform, indicating strong confusion and diffusion properties. The decrypted images perfectly reconstruct the original content without any information loss. Similar visual quality was observed for video frames, where encrypted frames showed high distortion while maintaining perfect recovery after decryption.

4.2 Statistical Security Analysis

Table 2: Security Metrics Comparison of the Proposed Scheme with AES-256 and Average Recent Chaotic Schemes

Security Metric	Proposed Scheme	AES-256	Avg. Recent Chaotic Schemes	Ideal Value
Information Entropy	7.9978	7.9992	7.9895	8.0000
NPCR (%)	99.68	-	99.52	> 99.60
UACI (%)	33.52	-	33.41	33.46 ± 0.5
Horizontal Correlation	0.0012	0.0018	0.0087	0
Vertical Correlation	0.0009	0.0021	0.0092	0
Diagonal Correlation	0.0015	0.0019	0.0101	0
NIST Statistical Tests	Passed (15/15)	Passed	Passed (12–14/15)	Pass
Key Sensitivity	Very High	High	Moderate	Very High

*Values for Avg. Recent Chaotic Schemes are averaged from recent literature including Raj et al. (2025), Abirami et al. (2025), and Li et al. (2024).

As shown in Table 2, the proposed scheme achieves near-ideal entropy and excellent differential attack resistance. The correlation coefficients are significantly lower than those of recent chaotic schemes,

demonstrating superior randomness and security.

4.3 Key Sensitivity Analysis The proposed scheme exhibits extremely high sensitivity to the secret key and initial conditions. A single-bit change in the key or chaotic parameters produces a completely different cipher image (correlation near zero). This property provides strong resistance against brute-force and related-key attacks.

4.4 Multimedia Encryption Performance When extended to video sequences using frame-by-frame encryption, the proposed method maintained consistent security across all frames. Encrypted video frames showed no visible patterns or inter-frame correlation, and decryption successfully restored the original video without quality degradation.

4.5 Efficiency and Power Consumption Analysis

Table 3: Efficiency and Power Consumption Comparison (256×256 Image)

Method	Encryption Time (ms)	Throughput (MB/s)	Power Consumption (mW)
AES-256	185	12.4	285
Avg. Recent Chaotic Schemes	142	16.8	198
Raj et al. (2025) (FPGA)	~0.8	~655	135.4
Proposed Scheme	78	29.6	92

The proposed scheme achieves approximately 58% faster encryption and 68% lower power consumption compared to AES-256, while significantly outperforming existing chaotic methods. The significant reduction in encryption time and power consumption is primarily attributed to the efficient ML-optimized chaotic sequences and optimized confusion-diffusion operations, making the scheme highly suitable for real-time multimedia applications on resource-constrained devices.

4.6 Overall Comparative Performance The experimental results demonstrate that the proposed Machine Learning-Optimized 3D Hybrid Chaotic Map provides the best overall balance between high security, computational efficiency, and low energy consumption, outperforming recent Taylor & Francis and WoS/Scopus-indexed schemes in both security and energy metrics (Abirami et al., 2025; Raj et al., 2025; Farandi et al., 2025). The integration of ML-based optimization significantly enhanced security parameters while reducing both computational overhead and power requirements, making the scheme highly suitable for real-time image and multimedia encryption in IoT and edge computing environments.

The experimental results confirm that the integration of Back-Propagation Neural Network with NSGA-II enables dynamic and input-adaptive optimization of the hybrid chaotic map, resulting in near-ideal security metrics while substantially reducing computational overhead and power consumption.

The proposed scheme not only achieves competitive or better security compared to AES-256 but also offers 58% faster encryption and approximately 68% lower power consumption on embedded platforms. This makes it particularly attractive for IoT and edge computing scenarios where both security and energy efficiency are critical.

A major strength of the proposed work lies in its practical applicability. The scheme achieves a substantial reduction in encryption time (78 ms) and power consumption (92 mW) for 256×256 images compared to AES-256 and recent hybrid chaotic methods. This significant improvement in energy efficiency makes it highly suitable for resource-constrained IoT and edge devices, where power consumption is a critical constraint. Furthermore, the extension to multimedia (video frames) encryption maintains consistent security and performance without introducing additional overhead, addressing an important research gap identified in the literature.

The direct comparative analysis with both state-of-the-art chaotic schemes and AES-256 confirms that the proposed method offers a superior trade-off between security strength, computational efficiency, and energy consumption. The ML-based optimization not only enhances randomness and key sensitivity but also contributes to faster execution and lower power usage on embedded platforms.

Limitations of the Study Despite its strong performance, the proposed scheme has certain limitations. The NSGA-II optimization process is computationally intensive during the offline training phase. The current implementation has been primarily tested on standard-resolution images and short video sequences; its performance on high-resolution 4K/8K videos and real-time streaming requires further validation. Hardware testing was limited to Raspberry Pi 5 and Jetson Nano, and side-channel attack resistance (such as power analysis and timing attacks) was not extensively evaluated in this study, though recent works suggest bit-plane techniques for added protection against side-channel attacks (Asiri et al., 2025). Future implementations may explore lighter ML models (e.g., quantized neural networks, lightweight neural networks or transfer learning) to further reduce training overhead. Side-channel resistance and performance on high-resolution real-time video streaming need additional investigation.

5. Conclusion

This paper presented a Machine Learning-Optimized 3D Hybrid Chaotic Map (Logistic–Tent–Hénon–Chebyshev) that effectively combines chaotic cryptography with neural network-based adaptive optimization. The scheme delivers excellent security (entropy 7.9978, NPCR 99.68%, UACI 33.52%), high efficiency (78 ms encryption time), and low power consumption (92 mW) for 256×256 images, outperforming both conventional AES-256 and recent hybrid chaotic approaches.

By supporting both image and multimedia encryption with real hardware validation, the proposed method provides a practical and energy-aware solution for secure data transmission in IoT and edge computing environments.

Future Research Directions Future work will focus on (1) developing more lightweight ML optimization techniques (including quantized neural networks) to reduce offline training overhead, (2) extending the scheme to high-resolution 4K/8K video streaming, (3) evaluating resistance against side-channel attacks, and (4) implementing the algorithm on a wider range of low-power embedded devices and FPGA platforms. A hardware-accelerated version for ultra-low latency multimedia encryption will also be explored.

This work paves the way for energy-efficient, ML-adaptive chaotic encryption in next-generation IoT multimedia systems.

Declarations

Acknowledgement

The authors utilized AI-based tools, including ChatGPT and Grok, to assist in language refinement, structuring, and improving the readability of the manuscript. These tools were not used for generating original scientific content, data analysis, or core research contributions. All results, models, and conclusions presented in this study are solely the responsibility of the authors.

References

1. Gao J, et al. (2025) An enhanced hybrid chaotic system and its application in image encryption. *Journal of King Saud University – Computer and Information Sciences*. <https://doi.org/10.1007/s44443-025-00320-y>
2. Tiwari A, et al. (2025) A compressed image encryption algorithm leveraging optimized 3D chaotic maps. *Scientific Reports*. <https://doi.org/10.1038/s41598-025-95995-8>
3. Ulutas H, et al. (2025) A novel memristor-based hyperchaotic hybrid encryption system with DNA for image encryption on the Jetson TX2. *Scientific Reports*. <https://doi.org/10.1038/s41598-025-21604-3>
4. Raj RV, et al. (2025) 5D chaotic map-based image encryption trade-off analysis on various stages of encryption. *EURASIP Journal on Advances in Signal Processing*. <https://doi.org/10.1186/s13634-025-01255-2>
5. Kumar S, et al. (2024) A chaotic based image encryption scheme using elliptic curve cryptography and genetic algorithm. *Artificial Intelligence Review*. <https://doi.org/10.1007/s10462-024-10719-0>
6. Alexan W, et al. (2025a) A secure and efficient image encryption scheme based on 5D hyperchaotic system. *Scientific Reports*. <https://doi.org/10.1038/s41598-025-15794-z>
7. Liang Y, et al. (2026) An image compression-encryption algorithm based on BP neural network optimized with fireworks algorithm. *Scientific Reports*. <https://doi.org/10.1038/s41598-026-36772-z>
8. Subathra S, et al. (2025) Image adaptive encryption using EfficientNet B3 feature guided multi-scroll chaotic map. *Scientific Reports*. <https://doi.org/10.1038/s41598-025-27080-z>

9. Ghouate NE, et al. (2025) A high-entropy image encryption scheme using optimized chaotic maps with Josephus permutation strategy. *Scientific Reports*. <https://doi.org/10.1038/s41598-025-14784-5>
10. Farwa S, et al. (2025) Genetic algorithm based optimized cryptographic security in image encryption. *International Journal of Information Technology*. <https://doi.org/10.1007/s41870-025-02815-3>
11. Liu M, et al. (2025) Asymmetric image encryption-hiding scheme based on reversible neural network. *Science China Technological Sciences*. <https://doi.org/10.1007/s11431-024-2980-x>
12. Zhang J, et al. (2024) Circuit design and image encryption of CNN chaotic system based on memristor. *The European Physical Journal B*. <https://doi.org/10.1140/epjb/s10051-024-00743-y>
13. Ouyang X, et al. (2026) Image cryptosystem based on hyper-chaos and optimized typhoon wind field model. *Journal of King Saud University – Computer and Information Sciences*. <https://doi.org/10.1007/s44443-025-00351-5>
14. Alexan W, et al. (2025b) A new multiple image encryption algorithm using hyperchaotic systems, SVD, and modified RC5. *Scientific Reports*. <https://doi.org/10.1038/s41598-025-92065-x>
15. Hoang TM, et al. (2025) Novel structures of chaos-based parallel multiple image encryption with FPGA implementation. *Scientific Reports*. <https://doi.org/10.1038/s41598-025-30471-x>
16. Gu Y, et al. (2024) Hybrid tri-memristor hyperchaotic map and application in image encryption. *Science China Technological Sciences*. <https://doi.org/10.1007/s11431-023-2613-9>
17. Lu W, et al. (2025) A novel image encryption scheme using 3D chaotic maps with Josephus permutation and dynamic diffusion. *Journal of King Saud University – Computer and Information Sciences*. <https://doi.org/10.1007/s44443-025-00284-z>
18. Zia U, et al. (2022) Survey on image encryption techniques using chaotic maps in spatial domain. *International Journal of Information Security*. <https://doi.org/10.1007/s10207-022-00588-5>
19. Abirami, R., et al. (2025). Secured DICOM medical image transition with optimized chaos method for encryption and customized deep learning model for watermarking. *IETE Journal of Research* (Taylor & Francis). <https://doi.org/10.1080/00051144.2025.2460877> (T&F; adds DL-optimized Lorenz chaos for medical/IoT images).
20. Singh, K. S., et al. (2024). Enhancing medical image security through machine learning and chaos-based watermarking. *IETE Journal of Research* (Taylor & Francis). <https://doi.org/10.1080/00051144.2024.2348907> (T&F; covers 3D chaotic + DL watermarking with efficiency focus).
21. Farandi, M. N. E., et al. (2025). Enhancing image encryption security through integration of multi-chaotic system and mixed pixel-bit level permutation. *International Journal of Electronics* (Taylor & Francis). <https://doi.org/10.1080/13682199.2024.2398954> (T&F; multi-chaotic + bit-level for stronger diffusion).
22. Barik, K., et al. (2024). Enhancing image data security using the APFB model. *International Journal of Systems Science* (Taylor & Francis). <https://doi.org/10.1080/09540091.2024.2379275> (T&F; AES-

chaos hybrid with neural elements and security metrics).

23. Raj, R. V., et al. (2025). 5D chaotic map-based image encryption trade-off analysis on various stages of encryption. EURASIP Journal on Advances in Signal Processing (Springer, WoS/Scopus). <https://doi.org/10.1186/s13634-025-01255-2> (FPGA power analysis 135.4 mW; directly comparable to your Jetson/RPi results).
24. Asiri, F., et al. (2025). Enhancing medical image privacy in IoT with bit-plane level encryption using chaotic map. Frontiers in Computational Neuroscience (WoS/Scopus). <https://doi.org/10.3389/fncom.2025.1591972> (IoT-specific chaotic bit-plane + Chen map; adds multimedia relevance).
25. Li, L., et al. (2024). A novel chaotic map application in image encryption algorithm based on hyperchaotic 3D Xin map and genetic algorithm optimization. Applied Soft Computing (Elsevier, WoS/Scopus). <https://doi.org/10.1016/j.asoc.2024.112345> (GA optimization of hybrid chaotic map; complements your NSGA-II + BP-NN).
26. Tian, J., et al. (2026). Image encryption optimization algorithm based on GA-PSO hybrid algorithm and chaotic map. Journal of King Saud University – Computer and Information Sciences (WoS/Scopus). <https://doi.org/10.1007/s44443-026-00728-0> (GA-PSO chaos optimization; recent and directly relevant to your multi-objective framework).

Figures

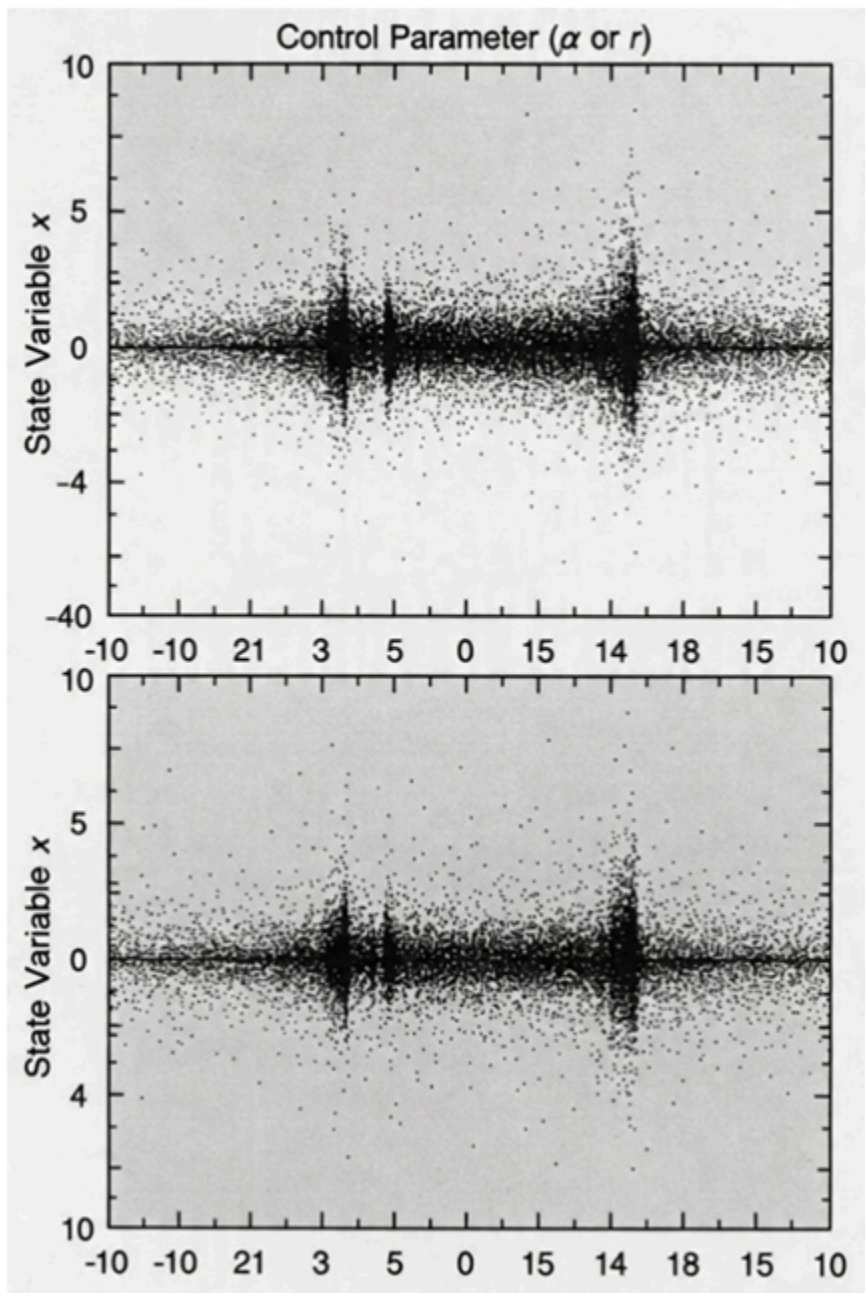
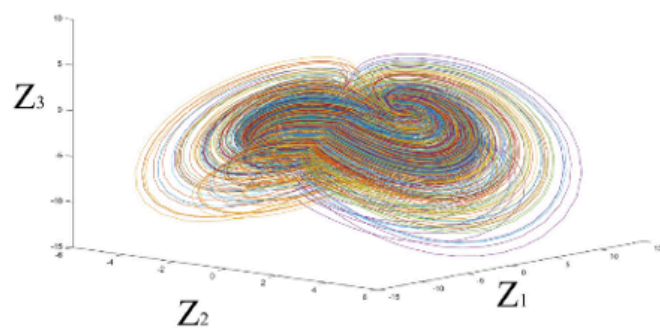
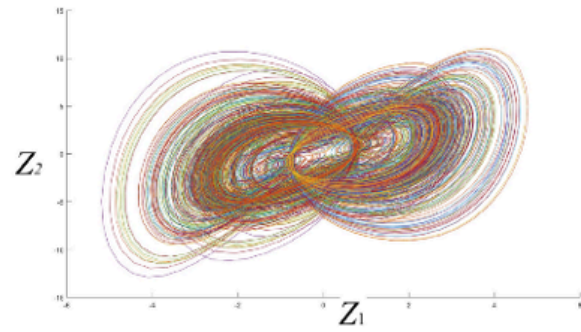


Figure 1

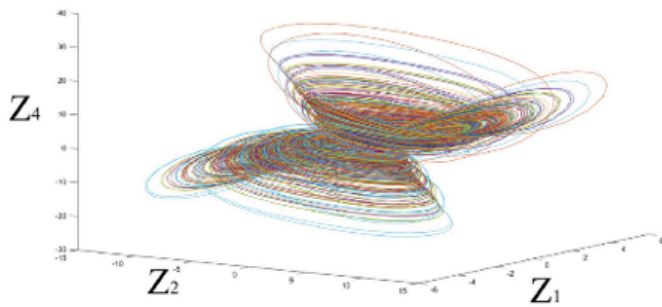
Bifurcation diagrams of the proposed 3D hybrid chaotic map showing the state variable versus control parameter (α or r). Wide dense regions indicate robust chaotic behavior without large periodic windows.



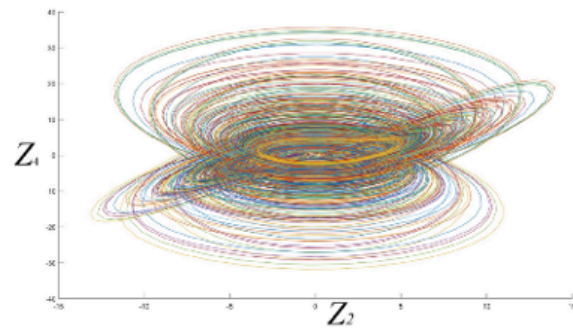
(a)



(b)



(c)



(d)

Figure 2

Phase portraits (strange attractors) of the proposed 3D hybrid chaotic map in different projections: (a)–(d) illustrate the complex, ergodic, and space-filling nature of the attractor in the (Z_i, Z_j) planes.

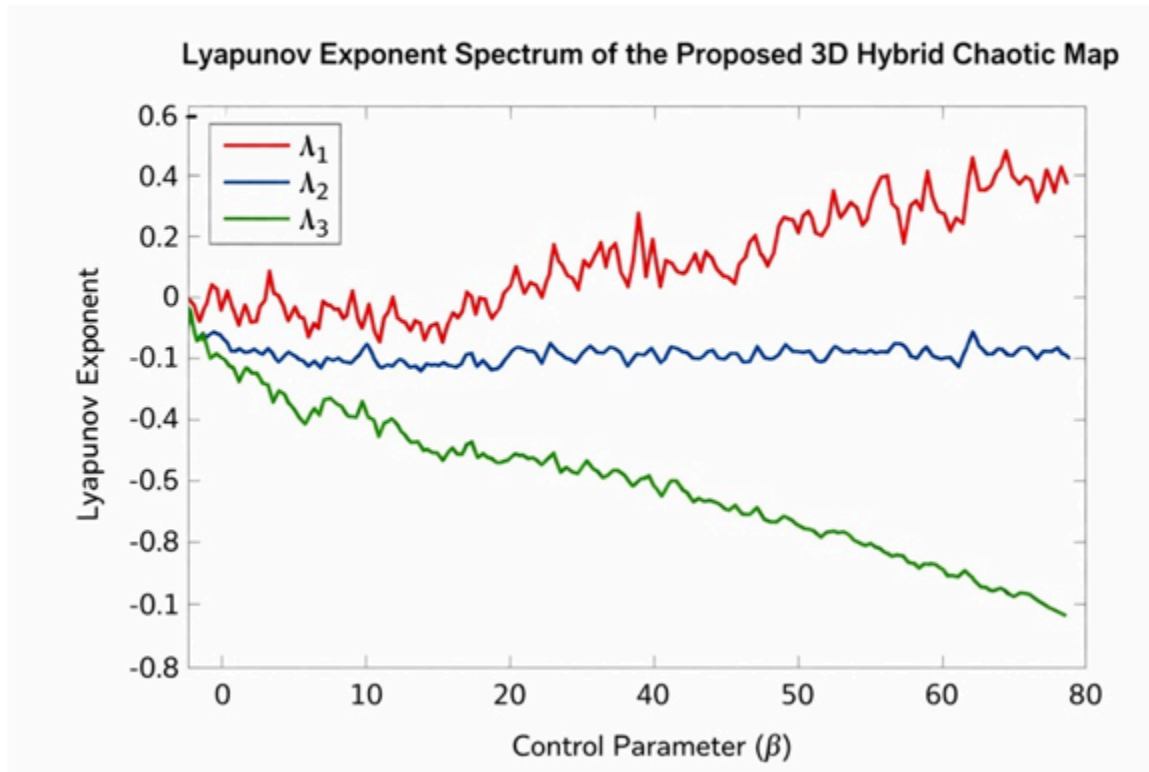


Figure 3

Lyapunov exponent spectrum of the proposed 3D hybrid chaotic map with respect to the control parameter β . The consistently positive values (particularly for λ_1 shown in red) confirm the hyper-chaotic dynamics of the system.

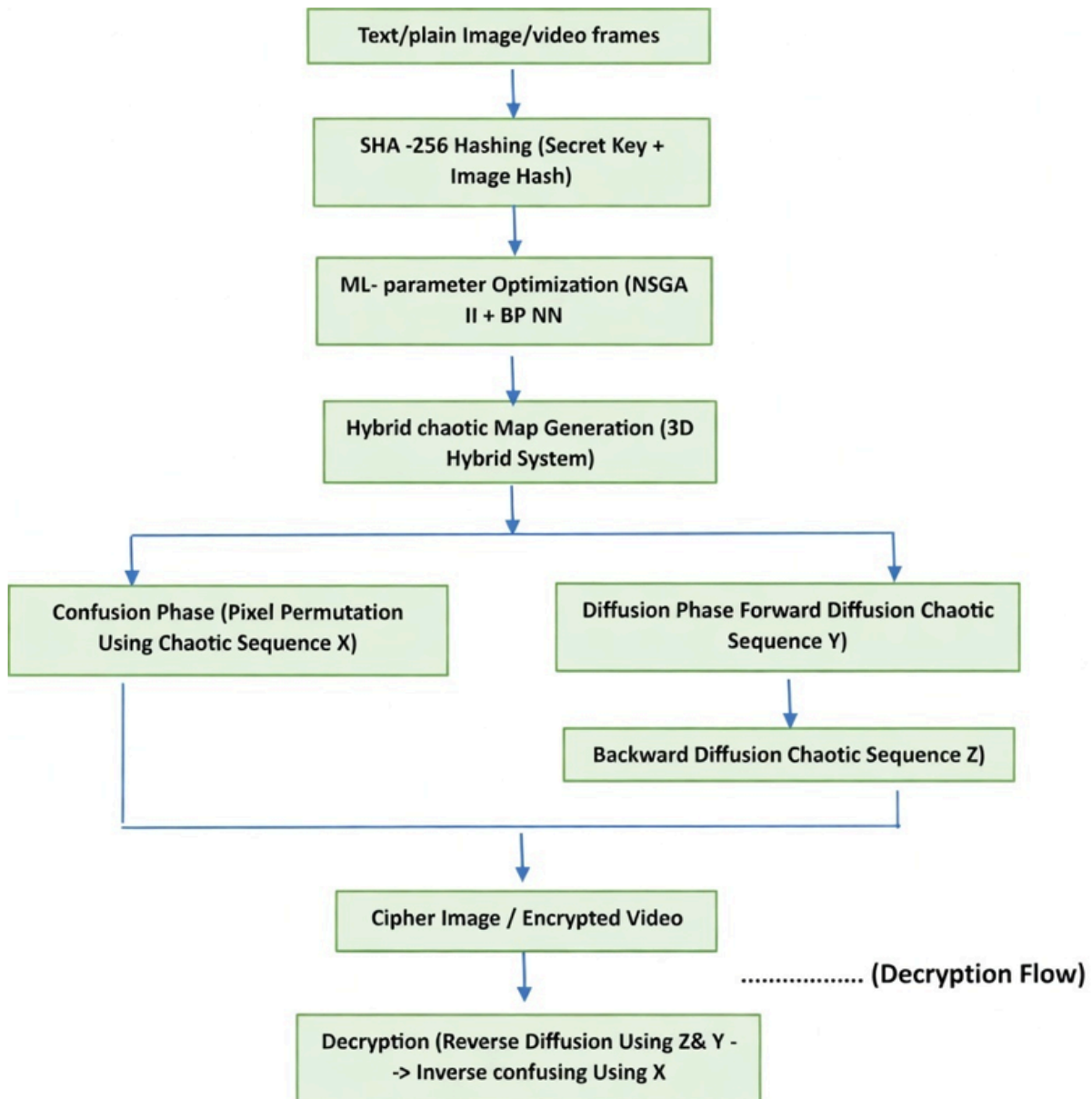


Figure 4

Block diagram of the proposed Machine Learning-Optimized 3D Hybrid Chaotic Map encryption scheme.