

SURVEY OF DEEP LEARNING-BASED CHAOTIC CRYPTOGRAPHIC FRAMEWORKS FOR MEDICAL IMAGE TRANSMISSION

A. Josekin¹, Dr. M. Nandhini², Dr. I. Paulina Vasanthi³

¹Research Scholar, Department of Computer Science, Pondicherry University

Email: josebellar258@gmail.com

²Professor, Department of Computer Science, Pondicherry University

Email: mnandhini2005@pondiuni.ac.in

³Vice Principal & Dean of Academics, Bishop Ambrose College

Email: paulinavasanthi17@gmail.com

Received: 5th January, 2026; Revised: 18th January 2026; Accepted: 25th January, 2026; Available Online: 28th January, 2026

ABSTRACT

The secure transmission of medical images is critical in modern healthcare systems, especially with the expansion of telemedicine, cloud diagnostics, and IoMT-based platforms. Conventional encryption methods often fall short in addressing the unique demands of medical imaging, such as format sensitivity, real-time constraints, and evolving cyber threats. This survey explores the integration of deep learning and chaos theory in cryptographic frameworks to overcome these limitations. By systematically reviewing and categorizing recent advancements into chaos-based, deep learning-based, and hybrid encryption approaches, the paper highlights how hybrid models offer enhanced adaptability, security, and efficiency. These models leverage the unpredictability of chaotic systems and the feature-learning capacity of neural networks to enable context-aware encryption, intelligent key generation, and support for region-specific protection. The review also identifies emerging trends like blockchain integration, compressive sensing, and bio-inspired mechanisms, which further strengthen data confidentiality and resilience. Despite these advancements, challenges such as standardization, computational overhead, and deployment in resource-constrained environments persist. This work concludes by emphasizing the need for lightweight, scalable, and regulation-compliant encryption frameworks that can meet the dynamic needs of intelligent healthcare systems and ensure the reliable protection of sensitive medical data.

Keywords: Medical image encryption, Chaotic systems, Deep learning, GAN, Blockchain, IoT security, DNA coding, Homomorphic encryption, Compressive sensing, Secure transmission, NPCR, UACI.

How to cite this article: Josekin A, Nandhini M, Vasanthi IP., Survey of Deep Learning-Based Chaotic Cryptographic Frameworks for Medical Image Transmission. Int J Drug Deliv Technol. 2026;16(81s): 1614-1627; DOI: 10.25258/ijddt.16.81s.195

Source of support: Nil.

Conflict of interest: None

1. Introduction

The digitization of healthcare, propelled by advancements in telemedicine, cloud-based platforms, and the Internet of Medical Things (IoMT), has transformed the storage, processing, and transmission of patient data. Among these, medical imaging modalities such as MRI, CT, X-ray, and digital pathology play a critical role in diagnosis, treatment planning, and clinical

research. However, the transmission of such sensitive data across heterogeneous and often unsecured networks makes it vulnerable to unauthorized access, tampering, and privacy breaches. These threats raise significant clinical, ethical, and legal concerns, emphasizing the need for robust and domain-specific encryption frameworks tailored to the unique requirements of medical imaging.

Conventional cryptographic methods like AES and RSA offer strong generic security but struggle with the computational and structural complexities posed by medical images such as high dimensionality, format heterogeneity, and real-time transmission needs. Additionally, the rise of adversarial threats, including deep learning-based attacks and future quantum computing risks, exposes the limitations of traditional approaches in modern healthcare environments. Chaos theory, with its properties of deterministic randomness, sensitivity to initial conditions, and topological mixing, offers promising capabilities for lightweight and highly secure image encryption. Meanwhile, deep learning (DL) models—such as Convolutional Neural Networks (CNNs), Autoencoders, and Generative Adversarial Networks (GANs)—excel in learning complex patterns, enabling intelligent encryption mechanisms such as adaptive key generation, format-aware transformation, and Region of Interest (ROI) encryption. However, each paradigm in isolation has limitations in scalability, adaptability, or cryptographic strength.

To overcome these challenges, recent research has explored hybrid encryption systems that integrate chaotic systems with deep learning models. These hybrid approaches have demonstrated enhanced security metrics, increased resistance to statistical and AI-driven attacks, and better adaptability to the dynamic needs of IoMT and cloud infrastructures. Moreover, advancements such as DNA-based encoding, blockchain integration, and homomorphic encryption further enrich the design of next-generation encryption frameworks. The key contributions of this survey are as follows:

- It systematically reviews and classifies over 60 recent methods (2020–2025) for medical image encryption that combine chaotic systems and deep learning models.
- It provides a critical performance analysis using standardized metrics such as entropy, NPCR, UACI, PSNR, and computational complexity.
- It identifies the advantages, trade-offs, and limitations of chaos-based, deep learning-based, and hybrid frameworks in the context of medical data security.

- It highlights emerging innovations and trends including ROI encryption, compressive sensing, quantum resistance, and edge-friendly implementations.
- It outlines future directions for research, focusing on lightweight architecture design, benchmark standardization, and regulatory compliance for clinical deployment.



Fig.1. Fundamental Process of Image Encryption and Decryption

The above image illustrates a fundamental image encryption and decryption procedure. An original image is converted into an encrypted image through an encryption method and a key. The encrypted image can be restored to its original form utilising the identical key and a decryption method.

This paper is structured as follows: Section 2 explores chaos-based encryption techniques; Section 3 discusses deep learning-based methods; Section 4 presents hybrid DL-chaotic encryption systems; Section 5 details the proposed methodology; and Section 6 concludes with insights and recommendations for future research.

2. Chaos Based Encryption

Recent developments in image encryption have increasingly focused on integrating chaotic systems, intelligent optimization, and hybrid cryptographic techniques to enhance security, randomness, and computational efficiency. Traditional methods such as the Arnold Cat Map (ACM) and AES have shown limitations in key space and computational cost, respectively, while hybrid approaches offer improved performance. For instance, Chaudhary et al. [1] demonstrated that combining ACM with a Logistic Map achieved better differential attack resistance (NPCR = 99.61%, UACI = 33.52%) than AES. Similarly, Kumar and Saini [2] employed the Henon map with Termite Alate Optimization to improve key generation and confusion, achieving

high entropy (7.9992) and low correlation (0.0008), although restricted to grayscale images. Lightweight methods like those proposed by Kiran et al. [3] and Gilmolk and Aref [6] used SCAN patterns and fuzzy logic-based operations, respectively, offering fast encryption suitable for IoT systems but lacking color image support and dynamic key updates. More advanced models integrating convolutional autoencoders, chaotic maps, DNA encoding, and dynamic S-boxes (Ahmed et al. [4]; Ali et al. [5]) achieved high entropy (7.9992) and NPCR (99.6%), ensuring secure encryption with minimal distortion, though the computational burden remains a concern for real-time applications.

In parallel, recent works have explored deep learning, blockchain integration, and compressive sensing for enhanced encryption robustness and application-specific security. Archana et al. [8] proposed a blockchain-enabled image encryption framework using chaotic maps and Honey Badger Optimization, achieving strong tamper resistance and suitability for medical IoT (entropy = 7.9993, NACI = 0.996). Deep learning-based approaches, such as the CNN-chaotic hybrid by Feng et al. [11] and the GAN-based model by Singh et al. [30], demonstrated improvements in speed and encryption strength, though computational intensity limits embedded system deployment. Quantum-resilient and high-dimensional encryption methods were presented by Zhou et al. [13] and Ahuja et al. [27], incorporating 5D chaos and lattice cryptography, providing enhanced unpredictability yet requiring optimization for low-resource environments. Compressive sensing integrated with wavelet transforms and chaotic systems (Huang et al. [9]; Zhang et al. [20]) achieved high imperceptibility (PSNR > 40 dB), while ROI-based encryption by Wang and Wang [18] focused on protecting sensitive regions in medical images. Reviews by Eltoukhy et al. [31] emphasized the need for lightweight, quantum-resistant schemes, and practical frameworks like those of Meng et al. [28] and Kumar and Revathi [32] demonstrated promising results for real-time medical security, though broader validation across diverse modalities and devices remains necessary.

Table.1. Overview of Chaos-Based Image Encryption Methods

Authors	Technique/Model	Key Metrics	Strengths	Limitations
Chaudhary et al. (2022)	ACM, ACM+LM, AES	NPCR: 99.61%, UACI: 33.52%	Strong differential resistance	AES has high cost; ACM lacks key space
Kumar & Saini (2024)	Henon Map + TAOA	Entropy: 7.9992, Corr: 0.0008	High randomness	Grayscale only
Kiran et al. (2022)	Bit-plane + SCAN + Tent Map	NPCR: 99.63%, UACI: 33.21%	Lightweight & fast	No dynamic keys, grayscale only
Ahmed et al. (2023)	CAE + DNA + Chaos + S-box	Entropy: 7.9993	Hybrid, color images	Needs more dataset validation
Ali et al. (2024)	Modified AES + 3D Chaos	NPCR: 99.94%, Time: 0.96 ms	Real-time use, strong metrics	Needs large-scale testing
Gilmolk & Aref (2024)	Chaos + Fuzzy Logic	PSNR: 38.7 dB	IoT friendly, low-power	Limited image compatibility
Mfundo et al. (2023)	Logistic-Sine + Fuzzy Henon	Entropy: 7.9994	Strong stats, robust	None specified

Archana et al. (2025)	Chaos + Blockchain + HBO	NAC I: 0.996	Decentralized, secure	Complex design
Huang et al. (2023)	CS + IWT + Chaos + RSA	PSNR > 40 dB	High imperceptibility	Computationally intensive
Erkan et al. (2023)	2D Hyperchaotic Map	Entropy: 7.9991	High security	Not lightweight
Feng et al. (2023)	CNN + Chaos	Entropy: 7.9986, PSNR: 38.2	Secure, fast	High resource demand
Lai et al. (2023)	Salomon Map + Diffusion	NPC R: 99.67 %	Efficient scheme	No color/high-res test
Zhou et al. (2023)	5D Chaos + Lattice Crypto	Entropy > 7.9989	Post-quantum secure	Heavy computation
Kocak et al. (2024)	MILE Map + PSO	Entropy: 7.9994	Localized tuning	Limited dataset validation
Wen et al. (2024)	Block Perm. + Bit-plane Diff.	Avalanche: 50.16 %	High diffusion	High processing load
Wang & Su (2021)	CS + 4W Chaos + DNA	PSNR: 41.02 dB	High security	DNA logic overhead
Hua et al. (2018)	Logistic-Sine Chaos	Entropy: 7.9992	Fast, secure	No cloud/quantum support
Wang & Wang (2023)	ROI + Logistic-Tent Map	PSNR: 38.67 dB	Privacy-focused	Not multimodal

Chai et al. (2024)	RDHEI + HBP-RMC	ER: 3.02 bpp	High capacity	Format-specific
Zhang et al. (2023)	2DCS + Henon + DRPE + DNPT	NPC R: 99.61 %, PSNR: 38.24	Strong security	Reconstruction overhead
Mansouri & Wang (2021)	SP-CMG	NPC R: 99.61 %, Entropy: 7.9993	Large key space	Not memory-efficient
Ghazvini et al. (2020)	Chen + LS Map + GA	PSNR: 41.02 dB	Robust encryption	GA adds cost
Talhaoui & Wang (2021)	1D Chaos + Substitution	Time: 0.45s	Efficient, secure	Not tested on large data
Wang et al. (2021)	LDCML + DNA	NPC R: 99.61 %, Entropy: 7.9992	Secure diffusion	DNA logic complexity
Raghuvanshi et al. (2024)	CNN + DNA + Chaos	PSNR > 58 dB	High-quality encryption	None specified
Du et al. (2022)	Fast Permutation + Shift	NPC R: 99.60 %, Time: Fast	Real-time encryption	Chaos use minimal
Ahuja et al. (2023)	5D + 4D Chaos + HDIEA	Entropy: 7.9996	High randomness	High computation

Meng et al. (2024)	AES-GCM + DWT+DCT	PSNR: 53.45 dB	Secure, medical-grade	Needs multimodal test
Hazzazi et al. (2024)	Fibonacci + Tribonacci + DWT	Entropy: 7.999	Real-time capable	Grayscale only
Singh et al. (2024)	GAN + Chaos + CSRNet	SSIM: 0.9456, 75% faster	Secure & efficient	None specified
Eltoukhy et al. (2025)	Survey on MIE	NPC R > 99.62 %, PSNR > 37	Comprehensive review	Highlights gaps
Kumar & Revathi (2024)	Memristor + DNN	NPC R: 99.95 %, UACI: 35.9 %	Strong diffusion	Needs platform validation
Wen et al. (2023)	Chaotic Bit-plane Diffusion	Entropy: 7.9993	Strong resistance	Needs IoT adaptation
Feng et al. (2021)	DNA + Feistel + Logistic	NPC R > 99.6 %	Improved security	Initial flaws exposed
Li et al. (2021)	IES-NP-DDT + Chaos	PSNR: 37.15 dB	Efficient, secure	Real-time scope unknown

Chaos-based image encryption leverages the unique properties of chaotic systems—such as sensitivity to initial conditions, pseudo-randomness, and nonlinearity—to secure images by disrupting pixel patterns and spatial correlations. These systems, classified into

discrete maps (e.g., Logistic, Tent) and continuous attractors (e.g., Lorenz, Chen), are validated using indicators like Lyapunov exponents, fractal dimensions, and entropy. Encryption approaches include symmetric methods (stream/block ciphers in spatial or frequency domains like DWT/DCT) and asymmetric methods (chaotic synchronization, elliptic curve integration). Hybrid models combining chaos with DNA computing, neural networks, or cellular automata further strengthen security. Applications span medical imaging, IoT, and satellite systems, though challenges like cryptanalysis resistance, encrypted-domain processing, and selective encryption persist.

Table.2. Essential Components of Chaos-Based Image Encryption

Aspect	Details
Chaotic Models	Discrete (Logistic, Tent, Henon), Continuous (Lorenz, Chen, Rössler)
Key Properties	Sensitivity to initial conditions, nonlinearity, fractal behavior
Indicators Used	Lyapunov Exponent, Bifurcation, Fractal Dimension, ApEn, NIST tests
Symmetric Techniques	Spatial (stream/block ciphers), Frequency (DWT, DCT), Hybrid approaches
Asymmetric Techniques	Chaotic Synchronization, Elliptic Curve + Chaos, Phase Space Analysis
Hybrid Technologies	DNA coding, Neural Networks, Cellular Automata, Quantum-safe integrations
Evaluation Metrics	Key Space, Entropy, Histogram Analysis, Correlation, NPCR, UACI
Applications	Medical image security, IoT encryption, satellite image protection
Key Challenges	Cryptanalysis resistance, encrypted-domain processing, selective encryption

3. Deep Learning Based Encryption

Recent studies have utilized various deep learning models to enhance image encryption. Patel [36] introduced EB-TDLM, a Transformer-based encryption framework integrated with blockchain for dynamic key generation, achieving outstanding performance (entropy 16.99, NPCR 99.99%, UACI 39.49%, SSIM 1.0), though limited in IoT settings. Inam et al. [38] proposed a CycleGAN-based encryption approach for unstructured medical data, reporting high visual fidelity (PSNR 37.6 dB, SSIM 0.995). Subramanian et al. [37] leveraged convolutional autoencoders for steganography, offering good imperceptibility (PSNR ~36.4 dB) but lacking true encryption. Tsai et al. [43] developed GMEI-GAN for reversible data hiding, with PSNR 45.09 dB and SSIM 0.9936, while Mhawi et al. [45] reviewed GAN-based methods and advocated for lightweight chaotic hybrid models due to strong metrics (entropy ≈ 7.999 , NPCR $> 99.62\%$). Zhang et al. [50] introduced MATDH using deep hashing and lightweight frequency-domain encryption (mAP 92.4%, accuracy 93.1%), showing promise for secure image retrieval. Conversely, MaungMaung et al. [39] and Maung Maung & Kiya [41] exposed vulnerabilities in learnable encryption through Stable Diffusion and StyleGAN attacks, highlighting potential risks in DL-based methods.

Ahmad and Shin [40] presented a perceptual encryption (PE) method using EfficientNetV2 for secure TB diagnosis with reduced transmission overhead (12%) and improved diagnostic accuracy (10%). Wang et al. [42] proposed a secure Capsule CNN (CCNN)-based framework with adaptive LSB embedding, achieving good entropy (7.9973), though susceptible to structural attacks. Alamgeer et al. [46] developed BPPIE-ODL, combining Dragonfly Algorithm, blockchain, and DL for lightweight healthcare encryption (accuracy 98.13%). Jia et al. [47] introduced chunk-based CNN inference using Fully Homomorphic Encryption (FHE), achieving 94.76% accuracy and 40% storage reduction. Pulido Gaytan et al. [48] reviewed FHE-enabled neural networks (e.g., BFV, CKKS), noting high accuracy (up to 95%) but high latency. Yu et al. [44] proposed a CRT-based RDHEI technique supporting share-based

recovery with PSNR 52.13 dB and capacity 3.42 bpp. S.G. and S.G. [49] presented PPDD using Gaussian noise and denoising DL networks for secure IoT image transmission (SNR 33.85 dB, SI 0.98). Finally, İhsan and Doğan [51] introduced PanAAVA, combining biometric key generation and LSB steganography (NPCR 99.74%, SSIM 0.9977), although limited by reliance on biometric signals.

Table.3. DL-Based Image Encryption Techniques

Authors	Technique/Model	Key Metrics	Strengths	Limitations
Patel (2025)	Transformer + Blockchain (EB-TDLM)	Entropy: 16.99, NPCR: 99.99%, UACI: 39.49%, SSIM: 1.0	Multi-layer encryption, tamper resistance	Not ideal for constrained IoT environments
Subramanian et al. (2021)	Autoencoder-based Steganography	PSNR (Stego): 36.4 dB, PSNR (Extracted): 34.7 dB	High imperceptibility and generalization	No encryption; limited standalone security
Inam et al. (2024)	CycleGAN-based Encryption	PSNR: 37.6 dB, SSIM: 0.995, NPCR: 99.59%, UACI: 33.38%	Paired data not needed, good on unstructured data	Requires optimization for IoMT
MaungMaung et al. (2024)	Stable Diffusion Attack on DL Encryption	SSIM: 0.41, LPIPS: 0.24–0.36	Revealed vulnerabilities in learnable	Critical leakage risks

			encryption	
Ahmad & Shin (2022)	Perceptual Encryption + Efficient NetV2	Bitrate overhead: 12%, Accuracy ↑ by 10%	Efficient diagnosis, minimal bandwidth impact	May lack support for multi-modal data
Maung Maung & Kiya (2023)	StyleGAN + Latent Diffusion Attack	SSIM: 0.42, LPIPS: 0.23–0.38	Demonstrated reconstruction of encrypted data	Security breach in block-scrambled DL systems
Wang et al. (2022)	Capsule CNN + PCS + Adaptive LSB	Entropy: 7.9973	Maintains visual quality, secure substitution	May be vulnerable to structural attacks
Tsai et al. (2021)	GMEI-GAN (Reversible Data Hiding)	PSNR: 45.09 dB, SSIM: 0.9936	Full data recovery, high quality	High model complexity
Yu et al. (2023)	RDHEI + CRTSS + Hybrid Coding	PSNR: 52.13 dB, Capacity: 3.42 bpp	Block encryption, share-based recovery	No support for dynamic streaming
Mhaw i et al. (2024)	Review of GAN-Based Encryption	Entropy $\approx$ 7.999, NPCR > 99.62%, UACI $\approx$ 33.48%, PSNR	High resistance to attacks	Need for lightweight GAN-chaotic hybrids

		> 37 dB		
Alamgeer et al. (2022)	BPPIE-ODL + Dragonfly + Blockchain + DL	Accuracy: 0.9813, Precision: 0.9551, F1: 0.9506	IoT-friendly, secure access control	Needs real-time evaluation in diverse scenarios
Jia et al. (2023)	CNN + Fully Homomorphic Encryption (FHE)	Accuracy: 94.76%, >40% reduction in cost/storage	Efficient encrypted domain inference	Moderate complexity still exists
Pulido Gaytan et al. (2021)	Review: Neural Networks + FHE (BFV, CKKS)	Accuracy up to 95%	Enables encrypted inference	High latency; needs hardware acceleration
S.G. & S.G. (2023)	PPDD (Gaussian Noise + Denoising DL)	SNR: 33.85 dB, SI: 0.98, ER: 0.013, CNR: 6.75	Edge decryption, robust privacy	Edge-based processing may limit scalability
Zhang et al. (2025)	MATDH + Deep Hashing + Frequency Encryption	mAP: 92.4%, Precision@100: 91.6%, Accuracy: 93.1%	High privacy and retrieval accuracy	Validation needed across other medical modalities
İhsan & Doğan (2024)	PanAAVA (ECG Key + Cipher + Stego)	NPCR: 99.7442%, UACI: 33.40%	Biometric key generation, high	Dataset dependency; limited

		, SSIM: 0.9977	security	generalization
--	--	----------------	----------	----------------

4. Hybrid Based Encryption

Recent developments in hybrid and chaos-based encryption schemes have demonstrated the potential of combining traditional chaotic maps with deep learning for secure image encryption. Ramesh Maniyath and Thanikaiselvan [52] introduced a model that integrates chaotic maps with deep neural networks (DNNs) to dynamically control encryption parameters, achieving high entropy and strong statistical security. Li and Peng [54] further enhanced medical image encryption by combining ResNet, attention mechanisms, and logistic chaotic maps, offering resistance to statistical attacks. Similarly, Iqbal et al. [55] combined DCNN, DNA encoding, and logistic chaos to boost randomness and diffusion but noted high computational costs. Tiwari et al. [61] proposed OptiSecure-3D, fusing optimized 3D chaotic maps with stacked autoencoders to enhance robustness against noise. Meanwhile, Dai et al. [59] and Man et al. [60] incorporated GANs and chaotic systems into encryption frameworks, while Panwar et al. [62] developed Encipher GAN using SSIM-driven loss and XOR operations to preserve visual quality and strengthen resistance to known plaintext attacks.

On the other hand, researchers have explored lightweight, compressive sensing, and classical cryptographic schemes to improve image encryption performance. Raghuvanshi et al. [53] introduced the FSR-SPD method using Flip-Shift-Rotate operations and piecewise chaotic maps for efficient diffusion, while Feng et al. [56] presented IEA-IF-DLT, integrating discrete logarithmic transformation for enhanced nonlinearity. Chai et al. [57] proposed an STP-based compressive sensing method with adaptive cyclic diffusion, and Chai et al. [67] earlier developed VMICE using dynamic LSB embedding and 3D Cat maps. Chen and Ye [58] merged SHA-3, RSA, and compressive sensing in an asymmetric scheme suited for secure transmission, though with latency trade-offs. Liu et al. [64] used salient object

detection for selective ROI-based encryption, and Ye et al. [66] proposed thumbnail-preserving encryption for JPEG images. Sirisha and Chandana [65] introduced a dual-function framework combining multi-key homomorphic encryption with Lion Swarm Optimization, while Darari et al. [63] combined Vigenère and RSA for dual-layer encryption. Collectively, these studies [52–67] reflect the growing shift toward algorithmic fusion, statistical robustness, and efficient, application-specific encryption strategies in image security.

Table.4. A Comparative Review on DL-Chaos Image Encryption

Authors	Technique/Model	Key Metrics	Strengths	Limitations
Ramesh Maniyath & Thanikaiselvan (2020)	Chaotic Map + DNN	Entropy: 7.9991, NPCR : 99.62 %, UACI : 33.46 %, PSNR : 35.27 dB	High adaptability, DNN-tuned parameters	Needs optimization for embedded devices [52]
Raghuvanshi et al. (2024)	FSR-SPD + PWLCM	Histogram ↓ 6.22%, Pixel Correlation ↓ 77.78 %	Efficient confusion-diffusion, lightweight	Needs improved randomness [53]
Li & Peng (2023)	AT-ResNet-CM (Attention + ResNet +	Entropy: 0.9965, Corr. Coef.:	Region-sensitive encryption,	Low entropy suggests randomness

	Chaotic Map)	0.0010	statistical resistance	mnness gap [54]
Iqbal et al. (2022)	DCNN + DNA + 2D Logistic Map	Entropy: 7.9992, NPCR : 99.62 %, UACI : 33.42 %	Strong robustness, DNA encoding	High computational overhead [55]
Feng et al. (2022)	IEA-IF-DLT	Entropy: 7.9991, NPCR : 99.63 %, UACI : 33.49 %	Fast, strong nonlinearity	Lacks dynamic streaming support [56]
Chai et al. (2023)	STP + Compressive Sensing + Adaptive Diffusion	PSNR : 41.37 dB, SSIM: 0.985, Bitrate ↓ 30.25 %	Compression with encryption, tamper resistant	Cloud-dependency limits offline use [57]
Chen & Ye (2022)	SHA-3 + RSA + Compressive Sensing	Entropy: 7.9985, NPCR : 99.60 %	Asymmetric security, no key sharing	Latency in real-time scenarios [58]
Dai et al. (2024)	GAN + Hyperchaos + Fibonacc	Entropy: 7.9994,	Dual-layer strengt	Complex; slow in time-

	i Q-Matrix	NPCR : 99.62 %, UACI : 33.46 %, PSNR : 37.09 dB	h, secure	critical apps [59]
Man et al. (2021)	LSGAN + Chaotic Inputs	Entropy: 7.9995, NPCR : 99.62 %, UACI : 33.47 %	High randomness, efficient	Resource-demanding training [60]
Tiwari et al. (2025)	OptiSecure-3D (3D Chaos + SAE)	Entropy: ~7.9, NPCR : 99.8%, UACI : 33.46 %	Excellent robustness, noise-resilient	Training time overhead [61]
Panwar et al. (2023)	Encipher GAN + XOR + SSIM Loss	PSNR : 36.24 dB, SSIM: 0.996, NPCR : 99.62 %	Good image fidelity, resistant to known-plaintext attacks	Optimization for edge/IoT needed [62]
Darari et al. (2020)	Vigenère + RSA	—	Simple dual-layer design	Static key; lacks metric

				validation [63]
Liu et al. (2025)	ROI + SOD + RGB Parallel Encryption	Throughput: 42.7 MB/s, Entropy: 7.9989, NPCR : 99.62 %	Efficient, ROI privacy preserved	Limited to visual ROI detection [64]
Sirisha & Chandana (2023)	MKHE + LSO	NPCR : 99.63 %, UACI : 33.42 %, PSNR : 57.68 dB, Acc: 96.84 %	Dual-functionality , secure + classify	May not scale in real-time [65]
Ye et al. (2023)	Thumbnail-Preserving Encryption (TPE)	PSNR : 38.27 dB, Bitrate ↑ 1.48%	JPEG compatible, reversible	Not suitable for non-JPEG formats [66]
Chai et al. (2020)	VMICE (Compressive Sensing + 3D Cat Map)	Entropy: 7.9976, PSNR : 37.89 dB	Good visual quality + encryption	Needs external carrier image [67]

5. Proposed Methodology

This section outlines the acquisition of medical image datasets and the implementation details of

the deep learning-based cryptographic framework, including model architectures and training procedures, facilitating the comprehensive evaluation of encryption efficiency and image quality preservation.

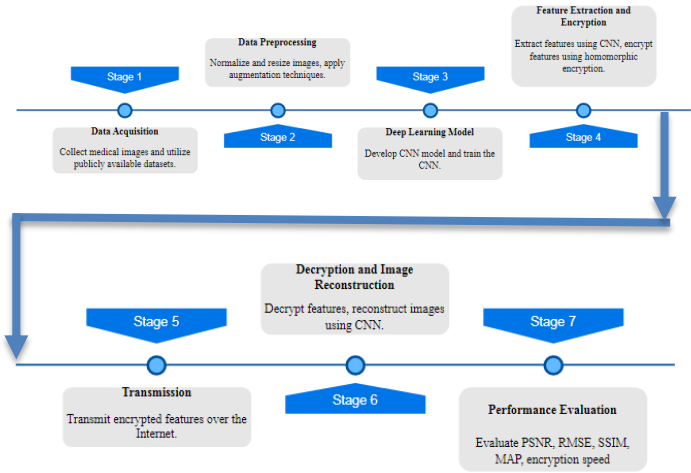


Fig.2. Efficient and Protected Medical Image Sharing Framework

This figure illustrates a seven-stage pipeline for secure and efficient medical image sharing using encryption:

- **Stage 1: Data Acquisition:** Collect medical images and/or use publicly available datasets.
- **Stage 2: Data Preprocessing:** Normalize and resize images, and apply data augmentation.
- **Stage 3: Deep Learning Model:** Develop and train a CNN for feature learning.
- **Stage 4: Feature Extraction and Encryption:** Extract features using CNN and encrypt them with homomorphic encryption.
- **Stage 5: Transmission:** Securely transmit encrypted features over the internet.
- **Stage 6: Decryption and Image Reconstruction:** Decrypt features and reconstruct medical images using CNN.
- **Stage 7: Performance Evaluation:** Assess system performance using metrics like PSNR, RMSE, SSIM, MAP, and encryption speed.

This framework ensures privacy-preserving, efficient, and high-quality medical image sharing in healthcare environments. A novel format-aware and lightweight hybrid model is developed to

address the constraints of current DL-based encryption frameworks, including their restricted adaptation to various medical image formats and resource-constrained IoMT contexts. This method combines intelligent key generation with chaotic encryption to markedly improve security, scalability, and transmission efficiency in medical imaging applications.

6. Conclusion

In conclusion, this review underscores the growing significance of hybrid image encryption approaches that integrate deep learning models with chaotic systems for securing medical images. These techniques consistently demonstrate high security performance achieving near-ideal values in entropy, NPCR, and UACI while supporting advanced features like ROI encryption, compressive sensing, and reversible data hiding. However, challenges such as computational overhead, limited real-time support for IoMT devices, and susceptibility to emerging AI-driven attacks persist. To ensure practical deployment in healthcare, future research must focus on lightweight, scalable, and quantum-resistant solutions aligned with regulatory standards, supported by standardized benchmarks for robust evaluation and clinical adoption.

References

1. Chaudhary, N.; Shahi, T.B.; Neupane, A. Secure Image Encryption Using Chaotic, Hybrid Chaotic and Block Cipher Approach. *J. Imaging* 2022, 8, 167.
2. Kumar, N. ., & Saini, S. . (2024). Image Encryption Model based on Chaotic Henon Map and Termite Alate Optimization Algorithm. *International Journal of Intelligent Systems and Applications in Engineering*, 12(18s), 428–436.
3. Kiran, Parameshachari, B.D., & Panduranga, H.T. (2022). Medical Image Encryption Using SCAN Technique and Chaotic Tent Map System. In: Shetty D.P., Shetty S. (eds) *Recent Advances in Artificial Intelligence and Data Engineering. Advances in Intelligent Systems and Computing*, vol 1386. Springer, Singapore.
4. Ahmed, F., Rehman, M. U., Ahmad, J., Khan, M. S., Boulila, W., Srivastava, G., Lin, J. C.-W., & Buchanan, W. J. (2023). A DNA based colour image encryption scheme using a convolutional autoencoder. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, 19(3s), Article 128, 1–21.
5. Ali, A., Gbashi, E., Hussein, Z., Alaskar, H., & Hussain, A. (2024). A Lightweight Image Encryption Algorithm Based on Secure Key Generation. *IEEE Access*, PP, 1–1.
6. Gilmolk, A.M.N., & Aref, M.R. (2024). Lightweight Image Encryption Using a Novel Chaotic Technique for the Safe Internet of Things. *International Journal of Computational Intelligence Systems*, 17, 146.
7. Mfungo, D.E., Fu, X., Xian, Y., & Wang, X. (2023). A Novel Image Encryption Scheme Using Chaotic Maps and Fuzzy Numbers for Secure Transmission of Information. *Applied Sciences*, 13(12), 7113.
8. Archana, G., Goyal, R., & Kumar, K.M.V.M. (2025). Blockchain-Driven Optimized Chaotic Encryption Scheme for Medical Image Transmission in IoT-Edge Environment. *International Journal of Computational Intelligence Systems*, 18, 11.
9. Huang, X., Dong, Y., Ye, G., et al. (2023). Meaningful image encryption algorithm based on compressive sensing and integer wavelet transform. *Frontiers of Computer Science*, 17, 173804.
10. Erkan, U., Toktaş, A., & Lai, Q. (2023). 2D hyperchaotic system based on Schaffer function for image encryption. *Expert Systems with Applications*, 213(B), 119076.
11. Feng, L., Du, J., Fu, C., & Song, W. (2023). Image Encryption Algorithm Combining Chaotic Image Encryption and Convolutional Neural Network. *Electronics*, 12(14), 3455.
12. Lai, Q., Hu, G., Erkan, U., & Toktas, A. (2023). A novel pixel-split image encryption scheme based on 2D Salomon map. *Expert Systems with Applications*, 213(Part A), 118845.
13. Zhou, S., Qiu, Y., Qi, G., & Zhang, Y. (2023). A new conservative chaotic system and its application in image encryption. *Chaos, Solitons & Fractals*, 175(Part 1), 113909.
14. Kocak, O., Erkan, U., Toktas, A., & Gao, S. (2024). PSO-based image encryption scheme

using modular integrated logistic exponential map. *Expert Systems with Applications*, 237(Part A), 121452.

15. Wen, H., Lin, Y., Kang, S., Zhang, X., & Zou, K. (2024). Secure image encryption algorithm using chaos based block permutation and weighted bit planes chain diffusion. *iScience*, 27, 108610.

16. Wang, X., & Su, Y. (2021). Image encryption based on compressed sensing and DNA encoding. *Signal Processing: Image Communication*, 95, 116246.

17. Hua, Z., Jin, F., Xu, B., & Huang, H. (2018). 2D Logistic-Sine-coupling map for image encryption. *Signal Processing*, 149, 148–161.

18. Wang, X., & Wang, Y. (2023). Multiple medical image encryption algorithm based on scrambling of region of interest and diffusion of odd even interleaved points. *Expert Systems with Applications*, 213(Part A), 118924.

19. Chai, X., Cao, G., Fu, Z., Gan, Z., Wang, B., & Zhang, Y. (2024). High-capacity reversible data hiding in encrypted medical images using adaptive pixel-modulation and HBP-RMC. *Biomedical Signal Processing and Control*, 95(B), 106424.

20. Zhang, C., Fan, H., Zhang, M., Lu, H., Li, M., & Liu, Y. (2023). Plaintext-related image encryption scheme without additional plaintext based on 2DCS. *Optik*, 272, 170312.

21. Mansouri, A., & Wang, X. (2021). A novel block-based image encryption scheme using a new Sine powered chaotic map generator. *Multimedia Tools and Applications*, 80, 21955–21978.

22. Ghazvini, M., Mirzadi, M., & Parvar, N. (2020). A modified method for image encryption based on chaotic map and genetic algorithm. *Multimedia Tools and Applications*, 79, 26927–26950.

23. Talhaoui, M. Z., & Wang, X. (2021). A new fractional one-dimensional chaotic map and its application in high-speed image encryption. *Information Sciences*, 550, 13–26.

24. Wang, X., Xue, W., & An, J. (2021). Image encryption algorithm based on LDCML and DNA coding sequence. *Multimedia Tools and Applications*, 80, 591–614.

25. Raghuvanshi, K. K., Kumar, S., Kumar, S., & Kumar, S. (2024). Image encryption algorithm

based on DNA encoding and CNN. *Expert Systems with Applications*, 252(B), 124287.

26. Du, K., Lyu, X., Zhang, C., Li, X., Zeng, T., & Zhao, L. (2022). A fast image encryption scheme based on simultaneous permutation-diffusion. *Proceedings of the 6th International Conference on Graphics and Signal Processing (ICGSP '22)*, 7–14.

27. Ahuja, B., Doriya, R., Salunke, S., Hashmi, M. F., Gupta, A., & Bokde, N. D. (2023). HDIEA: High dimensional color image encryption architecture using five-dimensional Gauss-logistic and Lorenz system. *Connection Science*, 35(1).

28. Bowen Meng, Xiaochen Yuan, Qiyuan Zhang, Chan-Tong Lam, Guoheng Huang, Encryption-then embedding-based hybrid data hiding scheme for medical images, *Journal of King Saud University - Computer and Information Sciences*, Volume 36, Issue 1, 2024, 101932, ISSN 1319-1578.

29. Hazzazi, M. M., Rehman, M. U., Shafique, A., et al. (2024). Enhancing image security via chaotic maps, Fibonacci, Tribonacci transformations, and DWT diffusion: a robust data encryption approach. *Scientific Reports*, 14, 12277.

30. Singh, M., Baranwal, N., Singh, K. N., & Singh, A. K. (2024). Using GAN Based Encryption to Secure Digital Images With Reconstruction Through Customized Super Resolution Network. *IEEE Transactions on Consumer Electronics*, 70(1), 3977–3984.

31. Eltoukhy, M. M., Alsubaei, F. S., Elnabawy, Y. M., & Hosny, K. M. (2025). Multiple image encryption techniques: Strategies, challenges, and potential future directions. *Alexandria Engineering Journal*, 125, 367–387.

32. Kumar, B.S., & Revathi, R. (2024). An efficient image encryption algorithm using a discrete memory based logistic map with deep neural network. *Journal of Engineering Applied Science*, 71, 41.

33. Wen, H., Lin, Y., Kang, S., Zhang, X., & Zou, K. (2023). Secure image encryption algorithm using chaos-based block permutation and weighted bit planes chain diffusion. *iScience*, 27(1), 108610.

34. Feng, W., Qin, Z., Zhang, J., & Ahmad, M. (2021). Cryptanalysis and Improvement of the Image Encryption Scheme Based on Feistel

Network and Dynamic DNA Encoding. *IEEE Access*, 9, 145459–145470.

35. Li, H., Li, T., Feng, W., Zhang, J., Zhang, J., Gan, L., & Li, C. (2021). A novel image encryption scheme based on non-adjacent parallelable permutation and dynamic DNA-level two-way diffusion. *Journal of Information Security and Applications*, 61, 102844.
36. Patel, Rucha. (2025). Novel Aspects of Secure Medical Image Encryption using Block-Chain and Transformer Based Deep Learning Model. *Journal of Information Systems Engineering and Management*. 10. 242-257. 10.52783/jisem.v10i33s.5474.
37. Subramanian, N., Elharrouss, O., Alma'adeed, S., & Bouridane, A. (2021). End-to-End Image Steganography Using Deep Convolutional Autoencoders. *IEEE Access*, PP, 1–1.
38. Inam, S., Kanwal, S., Anwar, A., Mirza, N. F., & Alfraihi, H. (2024). Security of End-to-End medical images encryption system using trained deep learning encryption and decryption network. *Egyptian Informatics Journal*, 28, 100541.
39. MaungMaung, A. P., Echizen, I., & Kiya, H. (2024). On the Security of Learnable Image Encryption for Privacy-Preserving Deep Learning. *IEEE Access*, PP, 1–1.
40. Ahmad, I., & Shin, S. (2022). A Perceptual Encryption-Based Image Communication System for Deep Learning-Based Tuberculosis Diagnosis Using Healthcare Cloud Services. *Electronics*, 11(16), 2514.
41. Maung Maung, A. P., & Kiya, H. (2023). Generative model-based attack on learnable image encryption for privacy preserving deep learning. *arXiv preprint arXiv:2303.05036*.
42. Wang, X., Liu, C., & Jiang, D. (2022). A novel visually meaningful image encryption algorithm based on parallel compressive sensing and adaptive embedding. *Expert Systems with Applications*, 209, 118426.
43. Tsai, C.-S., Wu, H.-C., Li, Y.-W., & Ying, J.J.-C. (2021). Applying GMEI-GAN to Generate Meaningful Encrypted Images in Reversible Data Hiding Techniques. *Symmetry*, 13(14), 2438.
44. Yu, C., Zhang, X., Qin, C., & Tang, Z. (2023). Reversible Data Hiding in Encrypted Images With Secret Sharing and Hybrid Coding. *IEEE Transactions on Circuits and Systems for Video Technology*, 33(11), 6443–6458.
45. Mhawi, M., Abdullah, H., & Sikora, A. (2024). GANs for Image Security Applications: A Literature Review. *Iraqi Journal of Information and Communication Technology*, 7(2), 89–102.
46. Alamgeer, M., Alotaibi, S., Alotaibi, S., Alturki, N., Hilal, A., Motwakel, A., Yaseen, I., & Eldesouki, M. (2022). Privacy Preserving Image Encryption with Deep Learning Based IoT Healthcare Applications. *Computers, Materials & Continua*, 73, 1159–1175.
47. Jia, H., Cai, D., Yang, J., et al. (2023). Efficient and privacy preserving image classification using homomorphic encryption and chunk-based convolutional neural network. *Journal of Cloud Computing*, 12, 175.
48. Pulido Gaytan, B., Tchernykh, A., Cortés-Mendoza, J.M., et al. (2021). Privacy-preserving neural networks with Homomorphic encryption: Challenges and opportunities. *Peer-to-Peer Networking and Applications*, 14, 1666–1691.
49. S. G., & S. G. (2023). Securing medical image privacy in cloud using deep learning network. *Journal of Cloud Computing*, 12, 40.
50. Zhang, S., Zhang, Q., Tang, J., & Xu, R. (2025). Secure Medical Image Retrieval Based on Multi-Attention Mechanism and Triplet Deep Hashing. *Computers, Materials & Continua*, 82, 2137–2158.
51. İhsan, A., & Doğan, N. (2024). An innovative image encryption algorithm enhanced with the Pan-Tompkins Algorithm for optimal security. *Multimedia Tools and Applications*, 83, 82589–82619.
52. Ramesh Maniyath, Shima & V, Thanikaiselvan. (2020). An Efficient Image encryption using Deep Neural Network and Chaotic Map. *Microprocessors and Microsystems*. 77. 103134. 10.1016/j.micpro.2020.103134.
53. Raghuvanshi, A., Budhia, M., Patro, K.A.K., et al. (2024). FSR-SPD: an efficient chaotic multi-image encryption system based on flip-shift-rotate synchronous-permutation-diffusion operation. *Multimedia Tools and Applications*, 83, 57011–57057.
54. Li, X., & Peng, H. (2023). Chaotic medical image encryption method using attention mechanism fusion ResNet model. *Frontiers in Neuroscience*, 17, 1226154.
55. Iqbal, N., Khan, M., Khurshid, K., & Hussain, I. (2022). An efficient hybrid encryption

model based on deep convolutional neural networks, deoxyribonucleic acid computing and chaotic system. *Multimedia Tools and Applications*, 82, 1–23.

56. Feng, W., Zhao, X., Zhang, J., Qin, Z., Zhang, J., & He, Y. (2022). Image Encryption Algorithm Based on Plane-Level Image Filtering and Discrete Logarithmic Transform. *Mathematics*, 10(17), 2751.

57. Chai, X., Fu, J., Gan, Z., Lu, Y., Zhang, Y., & Han, D. (2023). Exploiting Semi-Tensor Product Compressed Sensing and Hybrid Cloud for Secure Medical Image Transmission. *IEEE Internet of Things Journal*, 10(8), 7380–7392.

58. Chen, Z., & Ye, G. (2022). An asymmetric image encryption scheme based on hash SHA-3, RSA and compressive sensing. *Optik*, 267, 169676.

59. Dai, L., Hu, L., Chen, L., Wang, C., & Lin, F. (2024). An Image Double Encryption Based on Improved GAN and Hyper Chaotic System. *IEEE Access*, 12, 135779–135798.

60. Man, Z., Li, J., Di, X., et al. (2021). A novel image encryption algorithm based on least squares generative adversarial network random number generator. *Multimedia Tools and Applications*, 80, 27445–27469.

61. Tiwari, A., Diwan, P., Diwan, T. D., & et al. (2025). A compressed image encryption algorithm leveraging optimized 3D chaotic maps for secure image communication. *Scientific Reports*, 15, 14151.

62. Panwar, K.; Singh, A.; Kukreja, S.; Singh, K.K.; Shakhovska, N.; Boichuk, A. Encipher GAN: An End-to-End Color Image Encryption System Using a Deep Generative Model. *Systems* 2023, 11, 36.

63. Darari, R., Winarko, E., & Damayanti, A. (2020). Encryption and Decryption Application on Images with Hybrid Algorithm Vigenere and RSA. *Contemporary Mathematics and Applications (ConMathA)*, 2(2), 109.

64. Liu, B., Song, W., Zheng, M., Fu, C., Chen, J., & Wang, X. (2025). Semantically enhanced selective image encryption scheme with parallel computing. *Expert Systems with Applications*, 279, 127404.

65. Sirisha, U., & Chandana, B. S. (2023). Privacy Preserving Image Encryption with Optimal Deep Transfer Learning Based Accident

Severity Classification Model. *Sensors*, 23(1), 519.

66. Ye, X., Zhang, Y., Xiao, X., Yi, S., & Lan, R. (2023). Usability Enhanced Thumbnail-Preserving Encryption Based on Data Hiding for JPEG Images. *IEEE Signal Processing Letters*, 30, 793–797.

67. Chai, X., Wu, H., Gan, Z., Zhang, Y., Chen, Y., & Nixon, K. W. (2020). An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding. *Optics and Lasers in Engineering*, 124, 105837.