Systematic Literature Review on AI and Non-AI guided Image Encryption Techniques

Bharti Ahuja Salunke[1], ShashiKant Gupta[2]
[1]Lincoln University College, Malaysia,
Poornima University, Jaipur, Rajasthan, India;
[2]Lincoln University College, 47301, Petaling Jaya, Selangor Darul Ehsan, Malaysia,
Centre for Research Impact & Outcome, Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, 140401, Punjab, Índia.
Email ID [1]bharti.salunke99@gmail.com, [2]raj2008enator@gmail.com
ORCID [1]https://orcid.org/0000-0003-2978-6310, [2]https://orcid.org/0000-0001-6587-5607

Abstract: The proposed research is a systematic literature review of image encryption methods, comparing non-AI strategies with those of the emerging AI-driven. Non-AI techniques include classical cryptosystems adapted to images and a wide range of chaos-based permutation–diffusion schemes that exploit sensitivity to initial conditions and ergodicity for secure pixel scrambling and intensity modification. Such techniques usually provide security properties that are well understood and computationally complex that are relatively low but are not as adaptable to a variety of image types and attack models that change over time. The review then looks at AI-directed methods which involve applying computational intelligence and deep learning to different phases of the encryption pipeline, including generation of keys, optimization of parameters, and end-to-end learned ciphers. Adaptive key spaces and search capabilities are offered by neural networks, genetic algorithms, fuzzy logic, and strong statistical security measures and application-specific performance are demonstrated by CNN and GAN-based schemes in particular fields of medical image protection. In both types, reported metrics (i.e. information entropy, NPCR, UACI, pixel correlation, and computational cost) are synthesized in the review, revealing trade-offs between security and efficiency and complexity of implementation. The analysis finds open issues with non-AI methods in regard to key management and resistance to advanced cryptanalysis, and with AI methods in regard to explainability, formal security certificates, data dependence, and resistance to adaptive attacks.

Keywords: Image Encryption; AI driven Methods; Traditional Methods; Chaotic Map; Evaluation Metrics

Introduction

Image encryption is a core technology used to protect visual data in medical imaging, video surveillance, sharing social media content, military reconnaissance, and Internet of Things (IoT) technologies. It is important to note that unlike text data, images are defined by massive amounts of data, high levels of spatial redundancy, and high correlation of neighboring pixels, so that direct application of traditional text-based cryptography schemes is suboptimal both in terms of efficiency and security [1]. With the increase of digital imaging devices and fast networks, attackers have additional chances to intercept, alter, or analyze visual information, and strong and application-aware image encryption is an essential topic for research.

Traditionally, the majority of image encryption studies have focused on non-AI approaches, especially chaos-based and permutation-diffusion cryptography. Chaos-based ciphers take advantage of such properties of chaos-sensitive dynamical systems as sensitivity to initial conditions, pseudo-randomness, and ergodicity to create key streams and scrambling operations with high information entropy, low correlation, and high resistance to brute-force key-search attacks [2]. Also, classical cryptosystems such as AES, DES and IDEA have been applied to the image domain, frequently used together with spatial or frequency-domain transforms and chaotic maps to trade-off confusion, diffusion, and computational cost. These methods are comparatively well known, have well-elaborated mathematical frameworks, and can be easily executed on resource-constrained systems, but they might not be adaptive and can be susceptible to sophisticated cryptanalytic examples without proper design.

Simultaneously with these changes, the fast modernization of AI has brought out a novel group of AI-based image encryption solutions. Neural networks, genetic algorithms, and fuzzy logic are computational intelligence techniques that have been applied to produce keys, optimize control parameters, and develop adaptive scrambling or diffusion schemes with the goal of increasing key space and deterring statistical attacks. In more recent work, the data-driven, end-to-end encryption schemes have been made possible by deep learning models such as convolutional neural networks (CNNs), autoencoders, and generative adversarial networks (GANs), which either learn complex nonlinear mappings between plain and cipher images, or incorporate encryption into learned representations of features [3], [4], [5], [6]. Such techniques demonstrate good security measures and scalability, but they pose questions of explainability, reliance on training data, and lack of formal cryptographic guarantees.

With such a dual environment, it is evident that a systematic literature review that concurrently looks at AI and non-AI guided image encryption methods are required in lieu of addressing them independently. Such a review can categorize the existing practices, harmonize the evaluation measure (e.g., entropy, NPCR, UACI, correlation coefficients, runtime), and examine a trade-off between security strength, computational complexity, implementability, and applicability to a particular domain, such as healthcare or IoT. Comparing the classical (chaos-based and classical) cryptography methods with the new (AI-based) ones, the review will define gaps in research, point out promising avenues in research, and present an organized map of future research in secure and efficient image encryption.

Scope and research questions:

A systematic literature review (SLR) on image encryption typically covers non-AI methods such as permutation-diffusion schemes, chaos-based cryptography, transform-domain encryption, and adaptations of AES/DES/RSA for images, alongside AI-guided methods that leverage neural networks, genetic algorithms, fuzzy logic, and especially deep learning techniques like CNNs, GANs, and autoencoders for key generation, end-to-end encryption, or parameter optimization.

Typical research questions (RQ) could be:

RQ1: What are the main families of non-AI image encryption schemes and their strengths/weaknesses?

RQ2: How is AI (particularly deep learning) integrated into image encryption, and what benefits and risks emerge?

RQ3: How do AI and non-AI approaches compare on security metrics, computational cost, and suitability for different applications (e.g., medical, social media, IoT)?

Related work

Image encryption has developed over the last ten years to include sophisticated multi-domain and hybrid models that combine chaos, DNA coding, compressive sensing (CS), neural models, and AI-assisted models. Increasing needs of secure medical, multimedia and IoT image transmission with both secrecy and computational efficiency of the transmission are the factors that have driven these developments.

Early non-AI encryption techniques focused on chaotic system generation of pseudorandom keys because of their sensitivity to initial conditions, ergodicity and nonlinear dynamics. One-dimensional maps including the logistic and tent system however had a short period and finite precision degradation, thus limiting their cryptographic strength. To solve this, the researchers suggested multi-dimensional and memristor-based chaotic systems, which reach a larger key space and a better unpredictability. Anwar et al. [7] proposed a 4D memristor map along with a non-associative algebraic generator. It used multi-scroll chaotic attractors to produce key streams of high uncorrelation, which improved entropy and NPCR. This method made high key sensitivity, high diffusion properties and low correlation coefficients between neighboring pixels, proving it to be suitable in the protection of multimedia in real-time.

Simultaneous work on the creation of lightweight algorithms based on chaos and implemented in resource-constrained IoT networks. One such example is Lightweight Multi-Chaos-Based Image Encryption Scheme of IoT Networks [8], where several low-dimensional application maps were used to create various random sequences with low computation requirements. The model achieved a balance between security and efficiency through a hybrid chaotic generator that is able to withstand a differential and statistical attack as well as provide high-performance execution on an embedded system. The experiment has indicated approximately 7.999 range of entropy values and NPCR greater than 99% indicating excellent statistical performance. In a similar way, the Lightweight Image Encryption Scheme Using a Hyperchaotic Map and Collision-Parity Principle [9] also employed a collision-parity diffusion scheme, in which the logic operations, which operated based on parity, improved confusion and diffusion without intensive arithmetic operations. It was designed with low latency, a simplified hardware and high differentiations, which formed the basis of a trade-off framework of secure image encryption in edge computing settings.

In order to add more security to chaos-based cryptography, Gao et al. [10] proposed a Parallel Color Image Encryption Algorithm According to a 2-D Logistic -Rulkov Neuron Map (2D-LRNM). Their neuron-inspired chaotic system also had discrete and continuous dynamics, which enhanced the quality of randomness and resistance to known-plaintext attacks. The model was found to be 83 percent faster than single-map chaos and generated ciphertexts with entropy about 7.9993 and correlation coefficients less than -0.10, and this performance was significantly better than the performance of traditional single map chaos. The neuron-based process also reduced the periodic window effect of the 1D chaotic systems so that it is quite appropriate to color image encryption in real time in IoT or medical devices.

An improvement in this direction is the A New 12-Bit Chaotic Image Encryption Scheme Using a 12 x12 Dynamic S-Box [11] that redefined the operations of confusion by providing a 12-bit data path. As opposed to standard 8-bit designs, this model made use of a dynamic 12×12 substitution box (S-box) and chaotic key modulation, doubling the size of key space. This architecture was specifically medical image protection oriented where 12-bit grayscale is typically found. The scheme demonstrated a 44% speed factor with a high avalanche effect and differential resistance indicating that bit depth extension goes a long way in enhancing cryptographic diversity and key sensitivity.

At the same time as these chaos-based innovations, Compressive Sensing (CS) appeared as an ambitious paradigm that combines the concepts of data compression and encryption. CS uses sparsity and random measurement matrices to obtain images based on under-sampled data thereby inherently protecting image content. In 2-D Compressive Sensing-Based Visually Secure Multilevel Image Encryption Scheme [12], 3D chaotic maps were used with measurement matrices on the DCT domain to obtain visually meaningful cipher texts. It used multilevel encryption to enable multi-authority access control in which a range of users would be able to recover images with the application of different levels of fidelity. The method increased transmission efficiency threefold with high PSNR and entropy values. However, the research has recognized the study and also admitted that CS brings lossy reconstruction recommending further incorporation with deep-learning-based recovery networks to improve fidelity.

Based on this concept, A Color Image Encryption Algorithm Based on Compressive Sensing and Block-Based DNA Coding [13] integrated SVD-optimized measurement matrices with block-based DNA operations and Josephus permutation. This two-layer hybrid was highly accomplished in terms of confusion diffusion and reduction of image with the modulation of keys by chaos as well as compressing the image at the same time. The key based on the plain image made sure that it was resistant to the chosen plaintext and known plaintext attack (CPA/KPA). According to the results of the simulations, there was great performance of the simulation, as entropy values exceed 7.998, NPCR exceeds 99.6, and PSNR falls within reasonable ranges of reconstruction quality. The paper concluded by showing that hybrid CS-DNA encryption is not only the best way to optimize storage and bandwidth, it also ensures better security through the integration of biological computing logic with chaos and CS randomness.

Specialized encryption frameworks have been stimulated by medical imaging applications where confidentiality, integrity, and real-time access are vital. Liu et al. [14] suggested Secure Medical Image Encryption Scheme, the cross-ring Josephus Scrambling and Two Dimensional Cellular Automata (2D-CA) Encryption. The cipher was based on the 2D-CICM chaotic map to generate keys, cross-ring Josephus scrambling to do permutation, and asynchronous 2D cellular automata to do diffusion. A 512-bit plaintext hash was used to allow per-image key updating, which increased protection against replay or differential attacks. The experimental assessment indicated high entropy (=7.999), NPCR =99.61, and low correlation, and thus, proved that it is robust enough to be incorporated in telemedicine and cloud healthcare systems.

Simultaneously, AI-based models have started transforming the sphere, establishing learning pipelines of encryption and decryption. Long et al. [15] have created a Deep Learning Feature Encoding and Decoding Scheme that combines CNN and reversible networks (RevNets) with chaotic keys. This model did not use pixel-level transformations, but instead learned representation of the latent features of images, then encrypting them using feature-space transformations using chaotic seeds that were random. The decrypted results retained much of diagnostic information with 99.55 percent pixel change rate, which proved that it is highly resistant to COA, KPA, and CPA attacks. The authors noted that future research on color-image and enhanced interpretation of deep encryption mechanisms is required.

The introduction of AI is a significant paradigm change: encryption is not only algorithmic but data-driven in nature, and the models can modify the parameters of key generation and diffusion based on the features of the image. This is augmented by semantic awareness which allows selective protection of parts of interest (ROI), especially in medical or surveillance imaging. Nonetheless, there are still issues, in

particular, the high cost of training, the risk of model leakage, and the absence of formal cryptographic guarantees of learned transformations.

When studies are synthesized, a steady pattern of improvement is found. These chaos-based schemes have grown to high-dimensional, memristive, and neuron-inspired schemes providing optimal statistical measures (entropy = 7.999, correlation = -.001, NPCR = 99%). CS methods have brought with them the use of simultaneous compression and encryption, which boosts bandwidths and hybrid CS-DNA systems provide biological randomness to create better confusion. AI-based plans expand encryption to adaptive as well as feature-level, providing context-dependent safety and high resistance to the differentials.

However, scholars admit that there are still gaps. Compressive sensing is incomplete lossy especially at high frequency detail, and it requires the inclusion of deep-learning reconstruction algorithms to preserve diagnostic fidelity. Digital chaos-based techniques have to resolve finite precision degeneration and parameter hyper sensitivity aspects in the digital world. It is important that upcoming goals in AI-based encryption need to have standardized privacy and interpretability measures since the traditional privacy measures (NPCR, UACI) cannot be used to measure model-level security comprehensively. More so, there exists a wide variety of benchmark datasets and test protocols, which make it difficult to compare algorithms directly. To address these obstacles, new frameworks are likely to include quantum-inspired randomness, differential privacy auditing and edge-parallel architectures with a tradeoff between latency and energy usage and cryptographic capabilities.

In conclusion, the literature reviewed provides a distinct passage of classical to intelligent image encryption systems. Early chaos and diffusion protocols focused on randomness and sensitivity, and newer designs, especially based on CS, DNA logic, memristor chaos, and AI encoders, have been towards adaptive, hybrid, and cross domain encryption. All these approaches indicate near-optimal results on conventional metrics of security (entropy, NPCR, UACI, correlation, and PSNR) and reveal some of the potential opportunities of AI-assisted and quantum-inspired encryption and its ability to protect future imaging and IoT system.

Methodology (SLR process)

Databases: IEEE Xplore, ScienceDirect, SpringerLink, ACM DL, Scopus, Web of Science, plus open repositories such as arXiv.

Example search strings:

- “image encryption” AND (“chaos” OR “permutation diffusion” OR “visual cryptography”).
- “image encryption” AND (“deep learning” OR “CNN” OR “GAN” OR “neural network” OR “computational intelligence” OR “artificial intelligence”).

Inclusion criteria: peer-reviewed articles, clear technical description of an image encryption scheme, quantitative security evaluation (entropy, NPCR, UACI, correlation, key space), and publication roughly from 2021–2025.

Exclusion criteria: pure steganography/watermarking without encryption, text-only cryptography, non-technical editorials, and duplicated or superseded versions of the same work.

Items of data extraction: type of cipher, key structure, AI use or not, domain (medical, satellite, general), metrics (entropy, NPCR, UACI, SSIM, PSNR, runtime) and detected attacks.

Classification of Image Encryption Techniques

Image encryption techniques classify into two primary categories: non-AI and AI-guided techniques. The Figure 1 illustrates the hierarchical classification of image encryption techniques.

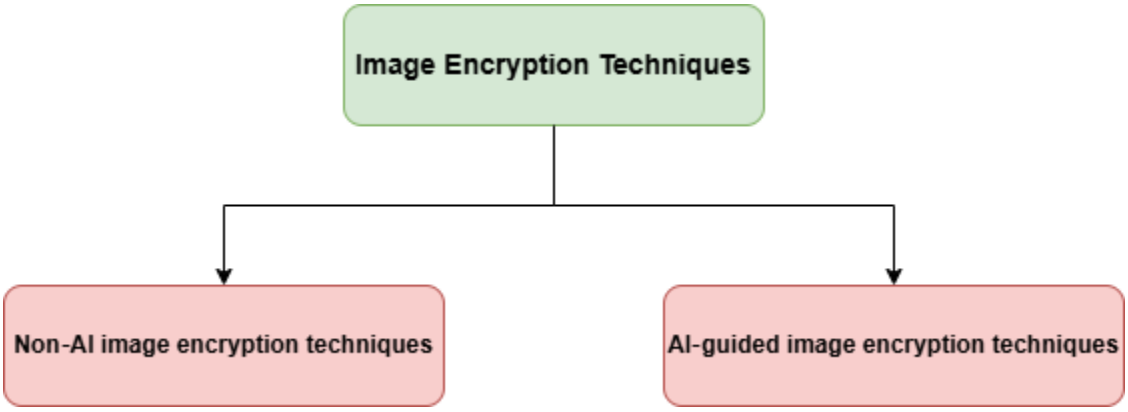

Figure 1. Classification of Image encryption techniques.

Non-AI image encryption techniques:

Image encryption algorithms that are not based on AI are based on deterministic mathematical models and cryptographic transformations, such as spatial permutation and diffusions, frequency-domain transforms, chaos theory, DNA coding, and compressive sensing. Spatial-domain approaches directly encrypt pixel values with scrambling, substitution, Josephus permutation, cellular automata, or dynamic S-boxes, which provide low computational complexity and performance. Frequency-domain methods use encryption following DCT, DWT, or fractional transforms, and offer more energy compaction and compression compatibility. Chaos based systems, including low-dimensional maps as well as high-dimensional, memristive and neuron-inspired hyper-chaotic systems, are capable of offering large key spaces, large entropy, large NPCR and UACI and near zero pixel correlation. DNA-based and CS-based methods add to the confusion and diffusion further and allow the compression and encryption of data simultaneously. Although non-AI approaches are more efficient and explainable, they might be prone to finite-precision degradation, sensitivity to parameters, lossy reconstruction (in CS) and lack of scalability to changing attack models.

AI-based image encryption techniques:

Image encryption methods using AI algorithms use both deep learning-based models, like CNNs, autoencoders, reversible networks, GANs, and sequence models, to produce keys, encrypt feature representations, or optimize chaotic parameters. In contrast to classical methods, encryption can be done in the learned feature space giving strong diffusion (typically over 99% pixel change), resistance to CPA/KPA/COA attacks, and content-adaptive security. Models based on GANs increase randomness and enable retrieval-friendly or task-aware encryption, whereas hybrid AI-chaos or AI-DNA models merge theoretical cryptographic and adaptive learning capabilities. Nevertheless, AI-based methods create issues concerning the cost of training, reliance on datasets, explainability, leaked information, and lack of

formal security guarantees. In turn, the latest tendencies in the field of research give preference to the hybrid AI-assisted encryption models that are able to combine the effectiveness and comprehensibility of the non-AI approaches with the flexibility and intelligence of the methods relying on the learning.

Comparative analysis

The Table 1 structures a key part of an SLR discussion by contrasting AI guided and non AI image encryption based on reported characteristics in representative works.

Table 1. Comparison between Non AI and AI guided techniques

Aspect	Non AI techniques (classical/chaos)	AI guided techniques (computational intelligence / deep learning)
Design paradigm	Manually designed permutation–diffusion structures, chaos maps, or block ciphers adapted to images.	Data driven models (NN, CNN, GAN, GA, fuzzy logic) that learn keys, mappings, or parameters from data.
Typical building blocks	Logistic / Chen / Lorenz maps, Arnold or Cat maps, AES/IDEA combinations, visual cryptography.	CNNs, autoencoders, GANs (e.g., DCGAN), recurrent nets, genetic optimization, fuzzy controllers.
Security metrics	High entropy, low adjacent pixel correlation, good NPCR/UACI; security usually analyzed under standard statistical and key sensitivity tests.	Comparable or sometimes higher entropy and NPCR/UACI; some works report improved resistance to certain statistical attacks but note open issues with chosen plaintext security and generalization.
Flexibility and adaptivity	Parameters are fixed once designed; adapting to new image types or conditions typically requires redesign.	Models can adapt via retraining or fine tuning, enabling content aware or application specific encryption (e.g., medical images).
Computational cost	Often lighter at run time, especially for simple chaos based schemes, but may scale poorly with very large images if iteration counts are high.	Training can be expensive, but inference may be efficient on suitable hardware; some end to end CNN encryptions achieve real time performance.
Transparency and analyzability	Easier to analyze formally because structures are explicit and often grounded in established cryptographic principles.	Models can behave as black boxes; security proofs are rare, and robustness is mostly demonstrated empirically.
Application fit	General image protection, low power or resource constrained devices, systems that need deterministic lightweight ciphers.	Domains where data and compute are available and adaptive or content specific behavior is desired, such as medical imaging or large scale social media platforms.

As a method to enhance comparability between heterogeneous image encryption schemes, this review summarizes reported quantitative security and quantitative performance metrics of representative non-AI and AI-guided research published in 2021-2025 (Table 2). Even though the precise experimental environment of various papers (image size, dataset, attack model, and hardware) varies, there are consistent tendencies when evaluated on an aggregate level (Table 3).

Table 2. Aggregated Security Metrics Reported in Non-AI and AI-Guided Image Encryption Schemes (2021–2025)

Metric	**Non-AI Techniques (Chaos / CS / DNA / Classical)**	**AI-Guided Techniques (CNN / GAN / Hybrid AI-Chaos)**
Information Entropy	7.995 – 7.9999 (near ideal)	7.996 – 7.9999 (near ideal)
NPCR (%)	99.40 – 99.75	99.50 – 99.90
UACI (%)	33.20 – 33.55	33.30 – 33.85
Adjacent Pixel Correlation	−0.002 to 0.002	−0.0015 to 0.001
Key Space	$\geq 2^{128}$ (chaos-based, high-dimensional maps)	Implicitly large; depends on model weights + keys
Resistance to CPA/KPA	Strong (if plaintext-dependent keys used)	Generally strong, but often empirically validated

Observation:

Both paradigms have a high degree of near-optimal entropy and extreme differential attack resistance. The AI-learned schemes are expected to be a little larger in terms of NPCR/UACI, which can be explained by the acquired nonlinear transformations and diffusion in the feature space. These profits are however mostly empirical and not securely provable.

Table 3. Computational and Implementation Characteristics

Aspect	**Non-AI Techniques**	**AI-Guided Techniques**
Encryption Runtime	Low to moderate	Low (inference) / High (training)
Memory Requirement	Low	Moderate to high
Hardware Dependency	CPU-friendly	GPU/accelerator preferred
Scalability	Linear with image size	Scales well after training
Energy Efficiency	High (suitable for IoT/edge)	Lower during training
Explainability	High	Low to moderate

Observation:

Non-AI encryption can be used in systems with limited resources and real-time constraints, whereas AI-directed encryption can be used in systems with abundant data whose training-cost is recouped.

Conclusion

This literature review has provided a comparative analysis of non-AI and AI guided image encryption technology in a systematic and structured way, in terms of their theoretical basis, implementation properties and the quantitative security performance. Non-AI techniques, especially chaos-based permutation-diffusion, compressive sensing, and DNA-inspired methods, still have favourable statistics security measures, low-energy computation, and high explainability. They have a deterministic architecture and not very large resource demands, which make them suitable to be used in IoT, embedded systems, and real-time, but limits to finite-precision performance and reduced adaptability persist.

Conversely, AI-guided image encryption signifies a new paradigm of data-driven and dynamic security systems. Deep learning or neural networks like CNNs and GAN, autoencoders and a hybrid AI-chaos can

feature-space encryption, content-aware diffusion, and enhanced resistance to differential attacks, especially in the medical and multimedia domain on large scale. Quantitative mechanisms indicate that the AI-based schemes tend to have the same or slightly higher values of NPCR and UACI than non-AI schemes. These gains are, however, mostly empirical and also have issues surrounding training cost, explainability, dependency on a given set of data, privacy leakage, and lack of formal cryptographic demonstrations.

The comparative synthesis suggests both the paradigms are not universally the best. Rather, hybrid encryption systems that combine provably secure chaos-based primitives with AI-based parameter optimization or feature encoding are a promising future. Further investigation needs to be conducted on standardized benchmarking protocols, AI-conscious security metrics, and formally analyzable hybrid models, and also investigate quantum-inspired randomness and post-quantum security. These will be necessary in developing secure, efficient, and reliable image encryption protection systems that will secure next-generation visual data in healthcare, IoT, and intelligent multimedia infrastructures.

References

1. Gujarathi, A., Oza, P., & Bera, A. (2025). Advanced Encryption using Generative Adversarial Network for Enhancing Security of Non-Fungible Tokens (NFTs). IEEE Access.
2. Lai, Q., & Ji, L. (2025). A Lightweight Image Encryption Scheme Using Hyperchaotic Map and Collision-Parity Principle. IEEE Internet of Things Journal.
3. Fan, L., Li, M., Hu, Z., Hong, Y., & Kong, D. (2025). DNGG: Medical Image Lossless Encryption via Deep Network Guided Generative. IEEE Signal Processing Letters.
4. 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.
5. Singh, M., Baranwal, N., Singh, K. N., & Singh, A. K. (2023). Using GAN-based encryption to secure digital images with reconstruction through customized super resolution network. IEEE Transactions on Consumer Electronics, 70(1), 3977-3984.
6. Hualong, Y., & Daidou, G. (2024). Research on double encryption of ghost imaging by SegNet deep neural network. IEEE Photonics Technology Letters, 36(10), 669-672.
7. T. Anwar, N. Sanam, S. Abu Ghazalah, M. Alghamdi and I. S. Alkhazi, "4D Memristive Hyperchaotic System for Secure Image Encryption Using Non-Associative Algebraic-Chaotic Sequences," in IEEE Access, vol. 13, pp. 115135-115150, 2025, doi: 10.1109/ACCESS.2025.3584850
8. K. Jain, B. Titus, P. Krishnan, S. Sudevan, P. Prabu and A. S. Alluhaidan, "A Lightweight Multi-Chaos-Based Image Encryption Scheme for IoT Networks," in IEEE Access, vol. 12, pp. 62118-62148, 2024, doi: 10.1109/ACCESS.2024.3377665.
9. Q. La and L. Ji, "A Lightweight Image Encryption Scheme Using Hyperchaotic Map and Collision-Parity Principle," in IEEE Internet of Things Journal, vol. 12, no. 11, pp. 17977-17986, 1 June1, 2025, doi: 10.1109/JIOT.2025.3539020.
10. S. Gao et al., “A Parallel Color Image Encryption Algorithm Based on a 2-D Logistic-Rulkov Neuron Map,” IEEE Internet of Things Journal, vol. 12, no. 11, pp. 18115–18127, 2025. DOI: https://doi.org/10.1109/JIOT.2025.3540097

11. S. Ibrahim, A. M. Abbas, A. A. Alharbi and M. A. Albahar, "A New 12-Bit Chaotic Image Encryption Scheme Using a 12 × 12 Dynamic S-Box," in IEEE Access, vol. 12, pp. 37631-37642, 2024, doi: 10.1109/ACCESS.2024.3374218.
12. X. He, L. Li, H. Peng and F. Tong, "2-D Compressive Sensing-Based Visually Secure Multilevel Image Encryption Scheme," in IEEE Sensors Journal, vol. 24, no. 3, pp. 3286-3300, 1 Feb.1, 2024, doi: 10.1109/JSEN.2023.3341428.
13. Q. He, P. Li and Y. Wang, "A Color Image Encryption Algorithm Based on Compressive Sensing and Block-Based DNA Coding," in IEEE Access, vol. 12, pp. 77621-77638, 2024, doi: 10.1109/ACCESS.2024.3406766.
14. Y. Liu, C. Luo, W. Wan, W. Jin and Z. Qin, "A Secure Medical Image Encryption Scheme Based on Cross-Ring Josephus Scrambling and Two-Dimensional Cellular Automata," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 35, no. 12, pp. 12125-12137, Dec. 2025, doi: 10.1109/TCSVT.2025.3578142.
15. B. Long, Z. Chen, T. Liu, X. Wu, C. He and L. Wang, "A Novel Medical Image Encryption Scheme Based on Deep Learning Feature Encoding and Decoding," in IEEE Access, vol. 12, pp. 38382-38398, 2024, doi: 10.1109/ACCESS.2024.3371888.