A Comprehensive Review of Key-Based Image Encryption Techniques: From Classical Ciphers to Intelligent Key Generation

Sharad Salunke[1], Arvind Kumar Tiwari [2]

[1] Post Doctoral Researcher, Lincoln University College, Malaysia;
Poornima University, Jaipur, Rajasthan, India;

[2] Department of Computer Science & Engineering, Kamla Nehru Institute of Technology, Sultanpur, 228118, Uttar Pradesh, India;

Email ID [1] shatad.sal@gmail.com, [2] arvind@knit.ac.in

Abstract: Due to the rapid increase in sharing of digital images over communication networks, confidentiality and integrity have become a major research concern. Image encryption system relies largely on the design and variety of encryption keys in order to achieve its strength. The present paper provides an extensive literature review of a wide range of key-generation schemes, including the static and pseudo-random ones, those based on chaos, DNA-coded and AI-based schemes. This paper critically examines more than 20 years of research and discovers the current areas of strengths, weaknesses, and gaps in the research on key-based image encryption. In addition, it suggests a classification scheme and brings into focus new tendencies like intelligent, adaptive and hybrid key generation to multimedia security next generation.

Keywords: Image encryption, encryption keys, chaos theory, DNA computing, AI-guided cryptography, key sensitivity, digital image protection

---

Introduction

The encrypted images have become a basic security requirement in the new camera-first communication ecosystem, such as telemedicine, smart surveillance, UAV/remote sensing, industrial inspection, social media sharing, and cloud storage, since images can be a significant semantic content and sensitive context that can be exploited despite a partial information leak. Unlike text, the natural images are very spatially redundant (inter-pixels correlation is exceedingly high) and are regularly structured in their statistics (histogram structures, texture periodicities, structural priors). These properties make naivete protection strategies vulnerable to statistical, differential, and chosen-plaintext/ciphertext attacks as well as make it difficult to develop an effective cipher because the images are large and might have to be provided protection in real-time. This has seen developments in the modern image encryption research to not only extend the concept of just applying the classical block ciphers directly, but also focus on implementing image-sensitive confusion diffusion pipelines, frequency/spatial hybrid designs, and more recently, adaptive and learning-directed designs to tune the security strength in accordance with the content and threat model.

The number of surveys that were made in the last 1-2 years indicates quite clearly that the quantifiable power of any image cipher lies not solely within a permutation/diffusion design, but within the quality of the key content underneath keysteam and control parameters which here is its randomness, unpredictability, sensitivity to initial conditions, resistance to reconstruction, and non-recycling across session/users [1]. In this case, the format of encryption key (and schedule) creation, more generally, is the decisive factor of security: such weak, short-period, biased, plaintext-correlated and reproducible keystream would be disastrous to any sophisticated diffusion. This observation has helped in the certain formation of the biggest generation methods in the image encryption.

Older and still widely used algorithms to produce keys using chaotic maps/hyperchaotic systems, and use sensitivity and ergodicity to produce pseudo-random sequences; recent are methods of refining chaotic key generators using higher dimensional dynamics, memristive/hardware friendly implementations, and improved statistical quality in order to avoid short periodicities and parameter degeneracy [2][3][4].

Simultaneously, there is also keying strategy diversification to :

(i) mathematical keys (chaotic/hyperchaotic sequences, DNA/mixed-radix transforms, elliptic-curve/number-theoretic constructs, cellular neural network-driven sequences),

(ii) content-dependent keys (hash-linked or feature-linked keys linking the ciphertext to the plaintext or ROI) and

(iii) biometric/device-anchored keys that attempt to facilitate improved uniqueness and utility in access-controlled deployments [5].

The other trend in the last 2-3 years was that key generation and key tuning became parameterized by the neural network or generative model: no longer parameterized by a fixed set of parameters, the hard-to-predict parameters are learned, the chaotic regime stabilized, or keys/keystreams with stronger statistical test resistance are produced. They include schemes that employ deep CNNs to generate or filter critical content in chaotic encryption pipelines and deep generative models (e.g., GAN variants) that are driven or encouraged to increase keystream unpredictability [6]. The other related direction is the time-varying coupling and learning-directed dynamics in which even though an attacker models part of the system, the coupling structure and the resulting keystream dynamism evolves in a less susceptible manner to adaptive attacks [7]. First attempts have as well been made on the borderline to investigate quantum-inspired or quantum aided key-generation schemes that are motivated by the potential of the more diverse range of randomness and more challenging to simulate distributions [8].

Despite this rapid innovation, key research gaps still remain: reproducibility and fair benchmarking across datasets and attack settings; insufficient reporting of key space key sensitivity and entropy with practical finite precision constraints; the insufficient analysis of threat models including chosen-plaintext, known-plaintext, and side-channel leakage and the model inversion of learning-based key generators; and insufficient analysis of threat models including chosen-plaintext, known-plaintext, and side-channel leakage and the model inversion in learning-based key generators. The latest surveys once more and once more brim with the necessity to move away as much as viable with designs that are passing the metric, and to regard key generation as a first-class item of study, rather than an implementation detail [1]. It is based on these observations that this review paper has been written, with the focus being on the development of encryption key generation in image encryption, in which the types of keys are first classified based on mathematical, chaotic/hyperchaotic, biometric/content-bound and AI-based paradigms, and the remaining open issues and future directions of the robust key generators are

summarized: robust key generators under finite precision, standardized randomness/cryptanalysis test suites, hybrid chaos-AI key schedulers to edge/IoT constraints, and security proofs/attack-driven.

Background and Motivation

The necessity to create key-generation algorithms in image encryption is predetermined by the growth of applying the visual information to the security-related fields, such as medical image diagnostics, military reconnaissance, smart transport, smart cities and multimedia services on clouds. Images are a very spatially redundent form of data, with high pixel correlations unlike textual data, and the classic cryptography primitives are very ineffective when used directly on images. As a result, the principle tenets of confusion and diffusion, which were initially postulated by Shannon, must be used image consciously and key centrically. In practice, the violation of the relationship between plaintext and ciphertext (confusion) and the distribution of the effect of a single pixel across the cipher image (diffusion) both are centrally determined by the quality of the encryption key. Weaknesses in entropy which lead to weak, predictable, or poorly-distributed keys inevitably result in vulnerability of encrypted images to statistical, differential and chosen-plaintext attacks despite its structure being complex-looking.

The earliest image coding algorithms worked with a static or user-selected key, which is typically applicable in many sessions. These were computationally efficient, but with poor key space, bad sensitivity to key variation, and were susceptible to brute-force and replay attacks. As the attack models evolved, scientists became aware that the application of the static key was not adequate in ensuring high level of visual information especially in open, open-ended and network circumstances. This knowledge led to the inclusion of randomized as well as chaos-based key generation by exploring the natural properties of nonlinear dynamical systems as sensitivity to initial conditions, ergodicity, and pseudo-randomness to enhance entropy and unpredictability. The chaotic key generators further increased the resistance to histogram and correlation attack by large but real-life implementation brought in new difficulties that encompassed finite-precision effects, parameter degeneracy, short cycle length, and reproducibility with partial information leakage.

The increased pace of the development of the deep learning and artificial intelligence has both refined the threat environment and introduced new opportunities to the adaptive security design. Modern attackers are employing learning based attacks capable of modelling chaotic systems and making predictions on parameters or utilise structure patterns over encryption pipelines. Recent research in turn has also been shifting to AI-based and adaptive key generation, in which neural networks, reinforcement learning or generative models naturally learn optimal key parameters based on data properties, threat-feedback or system constraints. Such mechanisms may be accommodated by the encryption system such that it is no longer possible to depend on a fixed or hand-written key schedule, but rather in some context-dependent and time-dependent fashion allow key evolution, much harder to predict or reverse-engineer. This adaptive paradigm can be heuristically driven on the basis of an analogy of maximum efficiency point detection (MEPD) on wireless power transfer systems. Maximum transfer of energy without constant feedback or explicit communication to minimize overheads and enhance robustness is deduced locally as MEPD has the best operating conditions. Similarly, good key selections in encrypting images are meant to maximize security- entropy, key sensitivity, NPCR/UACI, and learning attack resistance at the cost of the undesirable high computing costs, bandwidth, and complexity of key-exchange. The key should be

generated (intelligently) so that it is self-optimizing to maximize the confusion and diffusion of the image data, system accuracy and minimise the cost of computation with minimum overhead.

This incentive is particularly necessary when the resources at its disposal are limited such as edge devices, IoT cameras, UAVs, and real-time medical systems, where it is impossible to perform the heavy cryptography or high-frequency key exchange. This can be done by putting complexity in the places where it is most required, in this case in the key dynamics and not in the encryption structure and adaptive key generation can do this. Also, content-adaptive keys and AI-controlled keys allowed to selectively strengthen semantically sensitive keys can be used to protect semantically sensitive regions, which are as robust as security but as sensitive as the data itself.

Classification of Encryption Key Types

A crucial aspect of a sound image encryption is key generation, which directly determines how much an encryption scheme resists cryptanalysis and key-recovery attacks. Current studies look at a wide range of key types such as, but not limited to, static symmetric keys, chaotic keys, biometric keys, DNA keys, and multi-key designs that can be adaptive and support a higher level of degree of security against the challenges of lateral attacks as observed in the case of Figure 1 and summarized in Table 1.

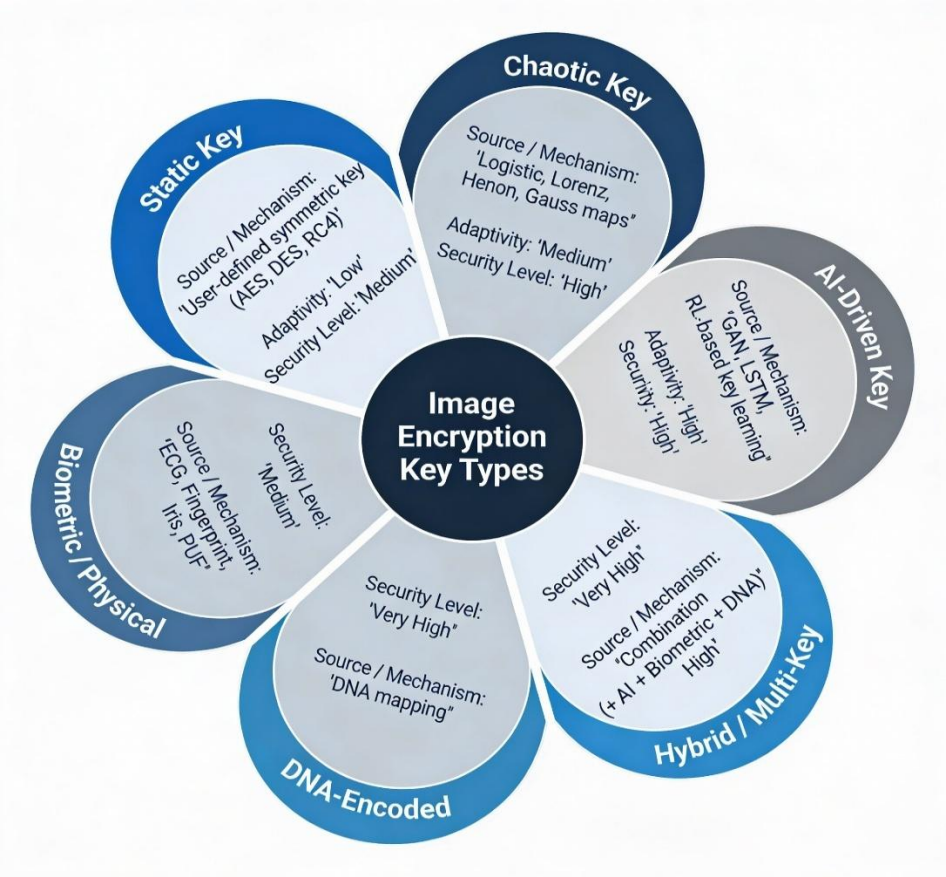

Figure 1. Image Encryption Key Types

Table 1. Classification based on encryption key types

Key Type	Source / Mechanism	Adaptivity	Security Level	Example Algorithms / References
Static Key	User-defined symmetric key (AES, DES, RC4)	Low	Medium	AES + Magic Cube [9], 3D Hyperchaotic Map [10], RSA and Arnold Map [11]
Chaotic Key	Logistic, Lorenz, Henon, Gauss maps	Medium	High	Multi-chaotic DNA [13], Logistic-Lorenz [12]
AI-Driven Key	GAN, LSTM, RL-based key learning	High	Very High	Deep Biometric [14], Dynamic AI-AES [15]
Biometric / Physical	ECG, Fingerprint, Iris, PUF	Medium	High	ECG-Crypto [16], Fingerprint [17]
DNA-Encoded	DNA mapping	Very High	Very High	DNA Tree [18], RNA–DNA [19]
Hybrid / Multi-Key	Combination (Chaos + AI + Biometric + DNA)	Very High	**Extremely High**	Hybrid AES + Chaos [11], Bio-Crypto [20]

Databases for conducting search

Table 2 below contains the database details.

Table 2. Database details

No.	Dataset Name	Domain / Type	No. of Images	Purpose / Justification	Access Link
1	**USC-SIPI Image Database**	Natural / Standard Benchmark	40+	Widely used in image encryption studies (Lena, Baboon, Peppers, Airplane). Ideal for baseline NPCR, UACI, and entropy evaluation.	https://sipi.usc.edu/database/
2	**Berkeley Segmentation Dataset (BSDS500)**	Natural / Texture-Rich	500	High-quality natural scenes with complex textures. Excellent for assessing diffusion and confusion under chaotic models.	https://www2.eecs.berkeley.edu/Research/Projects/CS/vision/grouping/resources.html
3	**Kodak Image Suite**	Natural Color / High-Resolution	24	High-resolution color images suitable for color encryption validation and PSNR/SSIM comparison.	http://r0k.us/graphics/kodak/
4	**Oxford Flowers 102**	Natural Objects / Texture Patterns	8,000+	High variety of color and structure; effective for evaluating key adaptability and encryption quality under diverse patterns.	https://www.robots.ox.ac.uk/~vgg/data/flowers/102/

Literature Review Framework

The following literature as depicted in Table 3 frameworks represent each considered research work with its key findings, methodology, and system representation style..

Table 3.Literature review based on Key Type used.

Category	Paper (short citation)	Year	Key Source / Type	Core Idea / Method	Eval Highlights (Entropy / NPCR / UACI, etc.)	Notes / Limitations
Deterministic (Static)	Bashir et al. [9], Magic Cube + AES	2012	Static AES + fixed rotation scheme	Blocks rotation (Magic Cube) + AES for image encryption	Typical AES metrics (not chaos-style); image testing implied	Static key per session; security mainly from AES; rotation adds structure
	Chowdhary et al. [21], Hybrid Techniques Survey	2020	Mixed (many static key sub-techniques)	Survey of hybrid image encryption methods (incl. ECC+Hill etc.)	Survey; reports broad metrics across works	Some covered methods use static keys; hybrid categorization overlaps
	Huo et al. [10], AES + 3D Hyperchaos	2025	Static AES + chaotic enhancement	Integrates hyperchaotic dynamics into AES process	Reports improved security/efficiency vs plain AES	Core is AES with session key; hybrid elements present
	Selvaraj et al. [11], IoMT Crypto	2023	RSA/Arnold for mgmt; fixed session key for data	Key mgmt + encryption pipeline for IoMT images	Applied metrics; focus on system integration	Fixed session keys
Chaotic	Feng et al. [12], Multi-Channel + Hyperchaos	2024	Two hyperchaotic maps	Pixel reorganization + hyperchaotic permutation/diffusion	Entropy≈7.99+, NPCR≈99% (typical claims)	Complexity increased; key sync needed
	Huang et al. [13], DNA Encoding + Chaos	2025	5D Hamiltonian chaotic system (init) + DNA	DNA rule encoding with chaotic keystream initialization	Entropy/NPCR/UACI reported; strong key space claimed	Security depends on DNA rule secrecy & chaos parameters

	Zhao et al. [22], Cryptanalysis of DNA+Chaos scheme	2025	Targets chaotic/DNA keys (attack)	Breaks a specific DNA+chaos algorithm via analysis	Shows weaknesses; recommends fixes	Demonstrates that not all chaos+DNA schemes are secure
AI-Driven	Jirjees et al. [23], Dynamic Image as Key	2023	Key derived from another image	Key depends on key-image; content-adaptive flavor	Good diffusion/NPCR typical	Security tied to secrecy of key-image
	Wang et al. [15], Deep Learning Biometric Key Generation	2021	Deep net-derived biometric keys	DL extracts stable keys from biometric images	Focus on reliability & stability of keys	Focused on key generation, not full image cipher.
	Manowska et al. [14], Crypto + Biometric Integration	2024	Biometric (AI processed) keys + crypto	Integration framework showing AI+crypto synergy	System-level outcomes; not image-only	Broader than image encryption
	Audhkhasi et al. [20], Dynamic Multichannel	2021	Dynamic/session keys (adaptive)	Secure image transmission with dynamic keying	Empirical robustness; transmission focus	Not a classic image cipher; transmission scheme
Biometric /Physical	Qin et al. [24], Biometric Images + 3D Arnold	2023	Biometric context-derived keys	Encrypts biometric images; nested 3D Arnold transform	Reports high Entropy/NPCR	Key generation may not stay stable every time.
	Hwang et al. [25], ECG Bio-Crypto Keys	2024	ECG-derived keys	Generates stable keys from ECG signals	Focus on stability/repeatability	Sensitive to noise; needs clean ECG signals.
	Castro et al. [16], Fingerprint-Authenticated Med Images	2023	Fingerprint-based authenticated keying	Auth + encryption for medical images	Applied NPCR/Entropy metrics typical	Focuses on medical use; less general encryption.

DNA	Huang et al. [13], DNA Encoding + Chaos	2025	DNA rules + chaotic init	DNA-encoded diffusion/perm + chaotic keystream	Entropy/NPCR/UACI strong (reported)	Sensitive to DNA rule mapping leakage
	Su et al. [17], 1D Chaos via DNA 3-Strand	2025	DNA-inspired chaotic system	New 1D chaotic system aligned to DNA structure	High entropy; large key space (claimed)	Novelty requires cryptanalysis depth
	Alawida et al. [18], DNA Tree Chaotic	2024	DNA tree + chaos	DNA tree structure for key/permutation	Strong diffusion metrics (reported)	Complex encoding; implementation cost
	Rahul et al. [26], Dynamic DNA Crypto + Chaos	2023	Dynamic DNA encoding + chaos	Dynamic DNA mapping rules during encryption	Entropy≈7.99+, NPCR≈99% (reported)	Rule management/ sync overhead
	Zhou et al. [19], Dynamic RNA/DNA Computing	2024	RNA+DNA computing-based keys	Bio-molecular computing paradigm for cryptosystem	High key space (claimed)	Hardware/complexity barriers
Hybrid / Multi-Key	Qin et al. [24], Biometric + Transform + Key	2023	Biometric + transform + crypto	Nested transforms with biometric-derived elements	High diffusion/confusion (reported)	Combines categories; sync & privacy considerations
	Feng et al. [12], Hyperchaos + Multi-Channel	2024	Hyperchaos + structural reorg	Multiple channels + hyperchaotic keys	Entropy/NPCR strong (reported)	Complex pipeline; parameter tuning
	Lin et al. [27], Dynamic Keys + AES	2021	Chaos/adaptive + AES static	Synchronised dynamic key schedule over AES	Improved NPCR/UACI vs plain AES	Key sync overhead; AES dependency

	Huo et al. [10], AES + Hyperchaos	2025	AES static + hyperchaos	Hybrid AES pipeline with chaotic dynamics	Better metrics than baseline AES	Still inherits AES mode considerations

Synthesis and Discussion

The history of key generation in the image encryption proves the obvious shift of the deterministic and deistic models towards the intelligent and adaptive ones to overcome the current security issues. Whereas older methods used fixed keys with little randomness and predictability, chaos-based systems have now taken over of the literature because of their high nonlinearity, ergodicity, and extreme sensitivity to initial conditions, which include large key spaces, and strong non-resistance to statistical and differential attacks. On this basis, DNA-based and AI-driven key generation models have been introduced as potentially attractive alternatives, which would add a higher level of adaptability, content awareness, and parameter optimization dynamism such that the encryption systems are more responsive to the different image properties and threat conditions. In this development, quantitative security measures remain very important in the assessment of cryptographic strength with the entropy of information values, and NPCR values of more than 7.9 bits and 99 percent respectively being generally considered by most as good indicators of high randomness, efficient diffusion, and overall robustness of cryptographic image encryption procedures.

Research Gaps and Future Directions

Table 4 demonstrates the research gap Vs future direction/recommendation based on discussed literature review.

Table 4. Research gap Vs Future direction/Recommendation.

Research Gap	**Future Direction / Recommendation**
Lack of standardized key evaluation metrics	Develop unified randomness and sensitivity metrics specific to image encryption.
Weak link between AI adaptability and cryptographic unpredictability	Design interpretable AI models for key evolution tracking.
High computational cost in chaotic and AI-based systems	Optimize with lightweight edge-AI and FPGA-based implementations.
Limited datasets for benchmarking image encryption performance	Create open benchmark repositories for key-type evaluation.

Conclusions

This review highlights the fact that, the design of encryption keys is the fundamental basis of secure image transmission because the ability of confusion and diffusion mechanisms to be strong ultimately depends on the quality, unpredictability and sensitivity of the key material used. Conventional fixed keys are becoming less secure against recent developments in cryptanalysis and learning-based attacks, but chaotic and hybrid key generation methods have proven to have definite benefits by vastly increasing the level of entropy and resistance against statistical and brute-force attacks. Specifically, adaptive image-

dependent keys enhance security through tying the encryption procedure to the intrinsic properties of the plaintext image, to provide high key uniqueness and effectively deterring key reuse between sessions. This kind of adaptability, in addition to enhancing the unpredictability, also integrates the security strength with the semantic and statistical features of the visual data, which is essential to the modern communication systems of multimedia and clouds.

Simultaneously, this review also points out that the implementation of image encryption schemes in real-life practice should be cautiously balanced in favor of both security and computational efficiency, particularly in real-time and resource-constrained settings. Exceptional randomness and sensitivity Chaotic and hyper-chaotic dynamic keys are computationally infeasible to exhaustive and differential attack; but they require that the choice of parameters and the implementation be stable, and they must be implemented within finite-precision limits. In future, the wisdom of artificial intelligence in guiding hybrid key creation can be seen as an opportunity since it combines the flexibility of intelligence-based optimization with the natural randomness of chaotic systems. Chaos, artificial intelligence, and new sources of quantum randomness are likely to be combined to provide next-generation adaptive key generation systems that are secure, scalable, and lightweight and thus, support effective real-time image protection at edge, IoT, and high-performance computing scales

References

1. Alghamdi, Y., & Munir, A. (2024). Image encryption algorithms: a survey of design and evaluation metrics. Journal of Cybersecurity and Privacy, 4(1), 126-152. https://doi.org/10.3390/jcp4010007
2. Dinu, A., & Frunzete, M. (2025). Image encryption using chaotic maps: development, application, and analysis. Mathematics, 13(16), 2588. https://doi.org/10.3390/math13162588
3. Murugan, R., & Yazhini, K. (2025). 5D chaotic map-based image encryption trade-off analysis on various stages of encryption. EURASIP Journal on Advances in Signal Processing, 2025(1), 60. https://doi.org/10.1186/s13634-025-01255-2
4. Su, Y., Xia, H., Chen, Z., Chen, H., & Huang, L. (2025). A Novel One-Dimensional Chaotic System for Image Encryption Through the Three-Strand Structure of DNA. Entropy, 27(8), 776. https://doi.org/10.3390/e27080776
5. Tao, L., Liang, X., Han, L., & Hu, B. (2025). Digital image encryption utilizing high-dimensional cellular neural networks and lower-upper triangular decomposition of matrix. Science Progress, 108(3), 00368504251375171. doi: 10.1177/00368504251375171
6. Almola, S. A., Khudeyer, R. S., & Younis, H. A. (2025). Biometric-Based Secure Encryption Key Generation Using Convolutional Neural Networks and Particle Swarm Optimization. Informatica, 49(16). https://doi.org/10.31449/inf.v49i16.7779
7. Zhang, H., Hu, H., & Ding, W. (2025). A time-varying image encryption algorithm driven by neural network. Optics & Laser Technology, 186, 112751. https://doi.org/10.1016/j.optlastec.2025.112751
8. Ahn, G., & Hong, S. (2025). QryptGen+: a quantum GAN-based high-security image encryption key generator with enhanced chaotic modeling. DOI:10.21203/rs.3.rs-6927959/v1.
9. Abugharsa, A. B., Basari, A. S. B. H., & Almangush, H. (2012). A Novel Image Encryption using an Integration Technique of Blocks Rotation based on the Magic cube and the AES Algorithm. arXiv preprint arXiv:1209.4777.

10. Huo, M., Zheng, Y., & Huang, J. (2025). Enhancing AES image encryption with a three-dimensional hyperchaotic system for increased security and efficiency. Plos one, 20(7), e0328297.
11. Selvaraj, J., Lai, W. C., Kavin, B. P., C, K., & Seng, G. H. (2023). Cryptographic encryption and optimization for internet of things based medical image security. Electronics, 12(7), 1636.
12. Feng, W., Yang, J., Zhao, X., Qin, Z., Zhang, J., Zhu, Z., & Qian, K. (2024). A novel multi-channel image encryption algorithm leveraging pixel reorganization and hyperchaotic maps. Mathematics, 12(24), 3917.
13. Huang, L., Ding, C., Bao, Z., Chen, H., & Wan, C. (2025). A DNA Encoding Image Encryption Algorithm Based on Chaos. Mathematics, 13(8), 1330.
14. Manowska, A., Boros, M., Hassan, M. W., Bluszcz, A., & Tobór-Osadnik, K. (2024). A Modern Approach to Securing Critical Infrastructure in Energy Transmission Networks: Integration of Cryptographic Mechanisms and Biometric Data. Electronics, 13(14), 2849.
15. Wang, Y., Li, B., Zhang, Y., Wu, J., & Ma, Q. (2021). A secure biometric key generation mechanism via deep learning and its application. Applied Sciences, 11(18), 8497.
16. Castro, F., Impedovo, D., & Pirlo, G. (2023). A medical image encryption scheme for secure fingerprint-based authenticated transmission. Applied Sciences, 13(10), 6099.
17. Su, Y., Xia, H., Chen, Z., Chen, H., & Huang, L. (2025). A Novel One-Dimensional Chaotic System for Image Encryption Through the Three-Strand Structure of DNA. Entropy, 27(8), 776.
18. Alawida, M. (2024). A novel DNA tree-based chaotic image encryption algorithm. Journal of Information Security and Applications, 83, 103791.
19. Zhou, S., Wei, Y., Wang, S., Iu, H. H. C., & Zhang, Y. (2024). Novel chaotic image cryptosystem based on dynamic RNA and DNA computing. Journal of Applied Physics, 136(18).
20. Audhkhasi, R., & Povinelli, M. L. (2021). Generalized multi-channel scheme for secure image encryption. Scientific reports, 11(1), 22669.
21. Chowdhary, C. L., Patel, P. V., Kathrotia, K. J., Attique, M., Perumal, K., & Ijaz, M. F. (2020). Analytical study of hybrid techniques for image encryption and decryption. Sensors, 20(18), 5162.
22. Zhao, Y., Shi, Q., & Ding, Q. (2025). Cryptanalysis of an Image Encryption Algorithm Using DNA Coding and Chaos. Entropy, 27(1), 40.
23. Jirjees, S. W., Alkalid, F. F., & Shareef, W. F. (2023). Image encryption using dynamic image as a key based on multilayers of chaotic permutation. Symmetry, 15(2), 409.
24. Qin, Y., & Zhang, B. (2023). Privacy-preserving biometrics image encryption and digital signature technique using Arnold and ElGamal. Applied Sciences, 13(14), 8117.
25. Hwang, H. B., Lee, J., Kwon, H., Chung, B., Lee, J., & Kim, I. Y. (2024). Preliminary Study of Novel Bio-Crypto Key Generation Using Clustering-Based Binarization of ECG Features. Sensors, 24(5), 1556.
26. Rahul, B., Kuppusamy, K., & Senthilrajan, A. (2023). Dynamic DNA cryptography-based image encryption scheme using multiple chaotic maps and SHA-256 hash function. Optik, 289, 171253.
27. Lin, C. H., Hu, G. H., Chan, C. Y., & Yan, J. J. (2021). Chaos-based synchronized dynamic keys and their application to image encryption with an improved AES algorithm. Applied Sciences, 11(3), 1329