

Cryptographic Methods for Digital Image Security: A Review of Conventional, Specialized, and Intelligent Approaches

Buthello Joshua¹, Vijay Baviskar², Ramkrishna Patil³

Department of Electronics Engineering,
SSVPS Bapusaheb Shivajirao Deore College of Engineering, Dhule, Maharashtra, India

Abstract: *The rapid growth of digital imaging, cloud computing, wireless communication, medical information systems, satellite imaging, surveillance, and social media has increased the need to protect image data from unauthorized access, modification, interception, and disclosure. Unlike ordinary text, images contain substantial spatial redundancy and strong relationships among neighboring pixels, creating requirements that must be considered when applying cryptographic techniques. This review examines conventional cryptography, permutation–diffusion architectures, chaos-based encryption, DNA-based methods, transform-domain encryption, compressive-sensing approaches, deep-learning-based encryption, lightweight cryptography, and hybrid schemes. Security and performance measures including entropy, correlation coefficient, NPCR, UACI, key sensitivity, key-space analysis, computational complexity, and encryption/decryption time are discussed. The review also considers common attack models and practical deployment challenges. The analysis indicates that no single metric or technique is sufficient to establish security. Future systems should emphasize reproducibility, authenticated encryption, efficient key management, application-specific design, and careful integration of standardized cryptographic primitives with image-processing and intelligent techniques.*

Keywords: Image security, image encryption, cryptography, AES, RSA, chaos theory, DNA cryptography, deep learning, lightweight cryptography, permutation, diffusion, NPCR, UACI.

I. INTRODUCTION

Digital images are now a major form of information in medical imaging, satellite observation, biometrics, industrial inspection, surveillance, military systems, smartphones, cloud storage, IoT devices, and multimedia communication. The source document identifies confidentiality, integrity, and authentication as the principal objectives of image security. Cryptography converts a plaintext representation, such as a grayscale or color pixel matrix, into ciphertext using a cryptographic key. However, the high volume and statistical redundancy of images mean that an encryption system must provide both cryptographic protection and practical computational efficiency.

Neighboring pixels in natural images usually have strong statistical relationships. A secure image-encryption system therefore aims to conceal recognizable structures, reduce adjacent-pixel correlation, and prevent an attacker from exploiting statistical properties. The source review classifies approaches into conventional cryptography, specialized image-encryption methods, and intelligent methods. AES and RSA represent established cryptographic primitives; chaos, DNA encoding, transform-domain techniques, compressive sensing, and hybrid architectures are specialized approaches; and neural networks represent an emerging intelligent direction.

II. REQUIREMENTS OF IMAGE CRYPTOGRAPHY

An effective image-encryption system should provide a sufficiently large key space to resist exhaustive search, high cipher-image entropy, low correlation among adjacent pixels, resistance to differential attacks, and acceptable computational efficiency. For an 8-bit grayscale image, entropy approaching 8 bits per pixel is commonly used as an indicator of high uncertainty. NPCR and UACI are frequently used to assess how strongly small plaintext changes propagate into the ciphertext. In practical systems, memory consumption, throughput, encryption time, hardware requirements, and authentication must also be considered.

Security should be evaluated against the intended attack model rather than inferred from a single numerical indicator. High entropy or low correlation is useful evidence of statistical concealment, but it does not constitute a cryptographic security proof. Key generation, storage, exchange, parameter selection, cryptographic mode, and implementation details can substantially affect actual security.

III. CONVENTIONAL CRYPTOGRAPHIC METHODS

3.1 Advanced Encryption Standard (AES). AES is a standardized symmetric block cipher with AES-128, AES-192, and AES-256 variants operating on 128-bit blocks. Its core transformations include SubBytes, ShiftRows, MixColumns, and AddRoundKey. AES provides an established security foundation and is widely used for general-purpose cryptographic applications. For large images, appropriate modes of operation, nonce/IV management, authentication, and careful handling of image data are necessary.

3.2 RSA and Hybrid AES–RSA. RSA uses public- and private-key pairs and is computationally more expensive than symmetric encryption. It is therefore generally more appropriate for protecting keys or small data rather than directly encrypting complete high-resolution images. A practical hybrid architecture encrypts the image using AES and protects the AES session key using RSA. This combines the efficiency of symmetric encryption with the key-management advantages of public-key cryptography.

IV. PERMUTATION–DIFFUSION AND CHAOS-BASED ENCRYPTION

Permutation changes pixel positions without necessarily changing pixel values, thereby disrupting spatial relationships. Diffusion changes pixel values so that a small change in one plaintext pixel can affect many ciphertext pixels. Multiple rounds of permutation and diffusion are commonly combined in image-encryption architectures.

Chaos-based approaches use properties such as sensitivity to initial conditions and pseudo-random behavior. Common maps and systems include the logistic map, tent map, Henon map, Arnold cat map, Baker map, Lorenz system, sine map, and Chebyshev map. The logistic map is represented as $x(n+1) = r x(n)(1-x(n))$. Chaotic sequences may be used for permutation, diffusion, or parameter generation. Nevertheless, chaotic behavior alone does not guarantee cryptographic security. Finite-precision effects, weak key generation, short cycles, poor parameter selection, and inadequate cryptanalysis can reduce practical security.

V. DNA-BASED AND TRANSFORM-DOMAIN METHODS

DNA-based cryptography uses encoding rules inspired by biological DNA sequences. Two-bit representations can be assigned to DNA bases according to a selected coding rule, and DNA operations can be combined with chaotic sequences to generate permutation and diffusion parameters. The review emphasizes that DNA cryptography should be regarded as a computational encoding paradigm rather than a replacement for mathematically established cryptographic primitives. Security claims must therefore be supported by rigorous cryptanalysis.

Frequency-domain methods transform image data using representations such as the Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), or Discrete Wavelet Transform (DWT). Encryption can then be applied to transform coefficients. These methods can integrate with compression and can support selective encryption of important frequency components. Their limitations include transform overhead and the possibility of information leakage if coefficient selection or the encryption layer is poorly designed.

VI. COMPRESSIVE SENSING AND DEEP-LEARNING-BASED ENCRYPTION

Compressive sensing exploits sparse signal representations and can combine sampling, transformation, and compression with security. Its principal challenge is maintaining reconstruction quality while avoiding exploitable measurement structure. The measurement process and its parameters must therefore be evaluated as part of the security design.

Deep-learning-based encryption incorporates neural networks into key generation, feature transformation, permutation, diffusion, or learned encryption/decryption. Candidate architectures include CNNs, autoencoders, GANs, transformer-based models, neural permutation networks, and other learned transformations. Their adaptability to complex image distributions is attractive, but these systems introduce training-data dependence, model-storage requirements, reproducibility issues, adversarial-attack concerns, computational cost, and difficulty in formally proving security. Thus, learning-assisted encryption should be evaluated using cryptographic as well as machine-learning criteria.

VII. LIGHTWEIGHT CRYPTOGRAPHY AND PRACTICAL DEPLOYMENT

IoT cameras, embedded vision systems, wireless sensors, and edge devices require cryptography with low memory, energy, and computational demands. The source document notes that NIST finalized SP 800-232 in August 2023 for Ascon-based lightweight cryptographic functions for constrained devices, including Ascon-AEAD128, Ascon-Hash256, Ascon-XOF128, and Ascon-CXOF128. For embedded image systems, algorithm selection should consider security level, throughput, RAM/ROM requirements, energy consumption, hardware support, and authentication.

High-resolution images may contain millions of pixels, making real-time applications particularly demanding. Surveillance, telemedicine, autonomous systems, and video communication may require low latency. Cloud and edge environments further require security mechanisms that operate across heterogeneous platforms. These constraints motivate hardware acceleration and carefully designed hybrid systems.

VIII. SECURITY AND PERFORMANCE EVALUATION

A research-oriented image-encryption system should be assessed with multiple independent measures. Histogram analysis examines whether ciphertext intensity distributions appear uniform and lack obvious relationships with the plaintext. Information entropy indicates uncertainty, with values approaching 8 bits per pixel commonly considered desirable for 8-bit images. Correlation should be examined horizontally, vertically, and diagonally.

NPCR measures the percentage of changed pixels produced by a small plaintext modification, while UACI measures the average intensity difference between ciphertexts generated from slightly different inputs. Key sensitivity evaluates the effect of small key changes and whether an incorrect key produces an unrecognizable result. Encryption/decryption time provides a practical performance measure. MSE, PSNR, and SSIM may be used to assess reconstruction quality, with lossless recovery normally requiring the decrypted image to match the original exactly.

Attack analysis should include brute-force, statistical, differential, known-plaintext, chosen-plaintext, and ciphertext-only attacks as appropriate to the deployment. A robust evaluation should combine statistical evidence with attack analysis, reproducible experimental conditions, and an explicit security model.

IX. COMPARATIVE ANALYSIS

Method	Main principle	Security / maturity	Cost	Typical application
AES	Symmetric block cipher	High when correctly deployed	Low–Medium	General image storage/transmission
RSA	Public-key cryptography	High when correctly deployed	High	Key exchange
AES–RSA	Symmetric + asymmetric	High potential	Medium	Secure image communication
Chaos-based	Chaotic	Design-dependent	Low–	Research image encryption

	permutation/diffusion		Medium	
DNA-based	DNA encoding/operations	Construction-dependent	Medium	Experimental/hybrid schemes
DCT/DWT	Frequency transformation	Architecture-dependent	Medium	Multimedia systems
Compressive sensing	Sampling transformation +	Measurement/key dependent	Medium	Secure compression
Deep learning	Learned transformation	Research-dependent	High	Intelligent image-security systems
Lightweight	Resource-efficient primitives	Standardized options	Low	IoT and edge devices
Hybrid	Combination of methods	Potentially high	Medium–High	Advanced research systems

The comparison is conceptual rather than a universal ranking. Actual security depends on implementation, key management, cryptographic mode, parameter selection, attack model, and formal analysis.

X. CHALLENGES AND FUTURE RESEARCH DIRECTIONS

Major challenges include the trade-off between security and computational complexity, key management, large image sizes, real-time operation, cloud and edge deployment, standardization, and reproducibility. A secure algorithm can still fail operationally if keys are poorly generated, stored, exchanged, or revoked. Research papers should report key-generation procedures, initial conditions, parameter ranges, image dimensions, datasets, hardware configuration, experiment counts, and security-test methodology to enable meaningful comparison.

Promising directions include hybrid cryptography that combines established primitives with image-processing methods; AI-assisted parameter selection and optimization; lightweight image security for IoT and edge AI; post-quantum key establishment; authenticated image encryption; privacy-preserving machine learning; and FPGA, GPU, ASIC, and embedded implementations. These directions should be evaluated conservatively, with security claims supported by appropriate cryptanalysis rather than by complexity or novelty alone.

XI. PROPOSED GENERAL FRAMEWORK AND EXPERIMENTAL METHODOLOGY

A generalized secure image-communication framework consists of image acquisition, preprocessing, key/nonce generation, pixel permutation, cryptographic diffusion, authenticated encryption, secure transmission, receiver verification, authenticated decryption, inverse permutation, and image recovery. The separation of preprocessing, cryptographic transformation, authentication, transmission, and recovery helps clarify system responsibilities.

For experimental validation, researchers can select grayscale and RGB images from public datasets, normalize experimental conditions, apply selected algorithms such as AES, chaos-based, DNA-chaos, DWT-based, deep-learning-based, and lightweight cryptography, and recover the original image using the corresponding key. Security, performance, and attack analyses should then be conducted. Experiments should be repeated across multiple images and parameter settings to establish statistical validity.

XII. CONCLUSION

Cryptographic protection of digital images requires attention to both established cryptographic principles and image-specific characteristics. AES provides a standardized symmetric foundation, while RSA can support secure session-key exchange. Specialized research has explored permutation–diffusion, chaotic maps, DNA encoding, transform-domain methods, compressive sensing, deep learning, lightweight cryptography, and hybrid constructions. Each approach introduces specific benefits and limitations.

No single numerical metric is sufficient to establish the security of an image-encryption algorithm. Entropy, correlation, NPCR, UACI, key sensitivity, computational complexity, reconstruction quality, and attack resistance

should be considered together. Future systems should emphasize reproducibility, authenticated encryption, effective key management, computational efficiency, and application-specific security models. The integration of standardized cryptography with carefully evaluated image-processing, lightweight, privacy-preserving, hardware, and AI techniques provides a practical direction for continued research.

REFERENCES

- [1] National Institute of Standards and Technology, "Advanced Encryption Standard (AES)," FIPS 197, updated May 2023.
- [2] M. Sönmez Turan, K. McKay, J. Kang, J. Kelsey, and D. Chang, "Ascon-Based Lightweight Cryptography Standards for Constrained Devices: Authenticated Encryption, Hash, and Extendable Output Functions," NIST SP 800-232, Aug. 2025.
- [3] D. Singh, S. Kaur, M. Kaur, S. Singh, M. Kaur, and H.-N. Lee, "A systematic literature review on chaotic maps-based image security techniques," Computer Science Review, vol. 54, Art. no. 100659, 2024.
- [4] "A comprehensive survey on image encryption: Taxonomy, challenges, and future directions," Chaos, Solitons & Fractals, vol. 178, Art. no. 114361, 2024.
- [5] B. Yogi and A. K. Khan, "Advancements in image encryption: A comprehensive review of design principles and performance metrics," Computer Science Review, vol. 57, Art. no. 100759, 2025.
- [6] T. Gupta, A. Selwal, and A. K. Sharma, "A survey on image cryptography mechanisms: Hitherto, and future directions," Computer Science Review, vol. 58, Art. no. 100783, 2025.
- [7] K. Mahalakshmi and S. Nagarajan, "Comprehensive Review and Analysis of Image Encryption Techniques," IEEE Access, vol. 13, pp. 109783–109813, 2025.
- [8] "Deep learning-based encryption for secure transmission digital images: A survey," Computers & Electrical Engineering, 2024.
- [9] "Deep learning-based image encryption techniques: Fundamentals, current trends, challenges and future directions," Neurocomputing, vol. 612, Art. no. 128714, 2025.
- [10] "Chaotic Image Security Techniques and Developments: A Review," Mathematics, vol. 13, no. 12, Art. no. 1976, 2025.