iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** V **Month of publication:** May 2026

DOI: https://doi.org/10.22214/ijraset.2026.83009

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

An Efficient Image Encryption Framework Integrating CPL-IES with Feature-Based Dynamic Key Generation, ECC, and AES

Vasavi Sridevi Seelam[1], Dr. Dasari Haritha[2]
[1]*M. Tech,* [2]*Professor, Computer Science Engineering Dept, UCEK, JNTU Kakinada, Andhra Pradesh, India*

Abstract: ***This study presents an efficient encryption framework for an image to enhance visual data security. The system combines a Collision-Parity Lightweight Image Encryption Scheme (CPL-IES) with dynamic keys derived from image features, further reinforced by Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) protocols. For establishing a rigorous plaintext-dependence, encryption keys are derived dynamically from intrinsic statistical attributes of the source image, specifically its mean intensity, standard deviation, and information entropy. ECC facilitates the secure establishment of a shared secret between communication endpoints without direct key transmission, while AES is deployed to protect the extracted feature metadata. To counteract statistical and differential cryptanalysis, a hyperchaotic map is leveraged to execute multi-dimensional pixel permutation and diffusion, yielding high cryptographic entropy. The proposed architecture natively accommodates both color and grayscale images by executing independent channel-wise processing. Empirical evaluation across diverse benchmark datasets indicates that the framework guarantees robust security parameters alongside minimized computational complexity, making it highly viable for real-time secure visual data transmission.***

Keywords: Secure communication, Hyperchaotic systems, Advanced Encryption Standard (AES), Image cryptosystem, Dynamic key derivation, Elliptic Curve Cryptography (ECC), CPL-IES framework.

I. INTRODUCTION

The exponential expansion of digital communication channels and multimedia technologies has rendered the preservation of image data a paramount security concern in the contemporary era. Images are extensively utilized in fields such as medical diagnostics, defence communication, cloud-based services, and Internet of Things (IoT) applications. Growing cyber vulnerabilities necessitate advanced measures to secure the confidentiality and integrity of transmitted images. Compared to data in text, images are represented by large data volumes, more redundancy and strong relationships among neighbouring pixels, which limits the effectiveness of conventional encryption methods when applied directly.

In response to these limitations, we propose a secure image cryptosystem that merges the Collision-Parity Lightweight Image Encryption Scheme (CPL-IES) with an image-feature-based dynamic key generation mechanism, alongside a combination of ECC and AES. The proposed approach aims to create a system that achieves both strong security and computational efficiency. Since many traditional methods tend to favour either speed or security, integrating multiple cryptographic techniques into a unified hybrid model helps enhance both performance and protection levels.

A. The Need for Secure Image Encryption

Images are widely shared and stored across digital environments, including social media platforms, healthcare infrastructures, surveillance systems, and secure communication networks. Unauthorized exposure of such data can result in significant privacy breaches and security threats. Traditional encryption methods are primarily designed for text and do not effectively address the unique properties of images. As images contain large data volumes and have strong relationships among neighbouring pixels, dedicated encryption strategies are necessary. Moreover, an effective image protection scheme must be capable of withstanding differential, statistical, and brute-force attacks. This method secures images by transforming them into unreadable formats using encryption keys derived directly from the images' unique visual features. This creates a strong link between the key and the image content, reducing vulnerability to chosen-plaintext attacks. Elliptic Curve Cryptography (ECC) aim to enable the key exchange securely at each end, while the Advanced Encryption Standard (AES) safeguards the extracted feature data. By combining these techniques, the system adopts a layered security structure that enhances overall protection.

B. Dynamic Key Generation Based on Image Features

To strengthen the security of the system, a dynamic key generation mechanism based on image features is employed. Key parameters are derived from statistical characteristics of the input image, including average intensity, standard deviation, and entropy. The method becomes highly sensitive to even slight modifications in the input as the key is linked directly to the original image. Consequently, the system yields drastically different encrypted results for different input images. This high variability strengthens defenses against both chosen-plaintext and known-plaintext cryptanalysis.

C. Combined ECC and AES Security Framework

A major challenge in encryption systems is the safe exchange of keys. To overcome this, Elliptic Curve Cryptography (ECC) is employed to create a shared secret between the communicating parties without exposing sensitive key details during transmission. ECC offers formidable cryptographic strength with minimal key lengths, making it an ideal choice for infrastructures with bounded computational overhead. To complement this, the framework integrates AES to secure the image's inherent feature matrices. This dual-layered implementation preserves data confidentiality and shields the transmission channel against unauthorized data exposure.

D. Proposed Encryption Framework Using CPL-IES

The proposed approach integrates the Collision-Parity Lightweight Image Encryption Scheme (CPL-IES) with a hyperchaotic mapping technique to carry out pixel-level permutation and diffusion. These processes enhance randomness and remove identifiable statistical structures from the image, thereby improving security. This approach is equally compatible with grayscale and multi-channel color images, as it evaluates and processes each color channel independently. Also, its effectiveness is assessed using a varied set of images to evaluate performance for security strength, computational efficiency, and robustness.

E. Applications of Secure Image Encryption

The efficient encryption scheme can be applied in various real-world scenarios, including:

1) Secure image transmission in IoT and cloud environments.
2) Protection of medical images and patient records.
3) Military and surveillance systems.
4) Secure storage and sharing of multimedia data.
5) Privacy preservation in digital communication platforms.

F. Finalization

As digital vulnerabilities become increasingly complex, the field of information security requires advanced image cryptosystems capable of ensuring high-tier confidentiality without sacrificing processing performance. By combining CPL-IES, feature-driven dynamic key generation, ECC, and AES, the proposed approach forms a layered security architecture that can withstand contemporary cryptographic attacks. It successfully maintains a balance between strong protection and computational efficiency. Future research can explore adapting this method for real-time video encryption and developing lightweight solutions tailored for edge computing environments.

II. RELATED WORKS

Modern security demands have led researchers to integrate established cryptographic standards, such as AES, with the unpredictable nature of chaotic systems. This fusion has birthed hybrid encryption methodologies where chaotic maps and block ciphers work in tandem to deliver comprehensive, multi-tiered security.

Recent advancements in image security highlight diverse approaches to encryption. To balance performance and security, a parallel encryption scheme introduced by Gao et al. (2025) utilizes a 2D Logistic-Rulkov neuron map. The system operates by merging cross-channel relationships with chaotic keystream generation. Similarly, Lazaros Moysis et al. [2] designed an image cryptosystem that utilizes a Soboleva-based chaotic map paired with circular shifts to execute rapid bit-level permutations and substitutions. Addressing the constraints of resource-limited environments, Biswarup Yogi et al. [3] developed HL-CAIoT—a lightweight, hybrid scheme fusing cellular automata with chaotic maps to deliver robust, efficient security tailored for IoT networks.

Bibhudendra Acharya et al. [4] utilized PWLCM and SHA-256 for dynamic key generation in their MIE-SPD multi-image encryption scheme, which executes synchronous permutation–diffusion alongside circular shifts. Addressing deployment constraints, Samuel Souza da Silva et al. [5] built a hardware-efficient chaotic PRNG leveraging a Sugeno-approximated sine map paired with perturbation methods and posit arithmetic.

Lastly, a unique approach called GRTPHM was put forward by Yu-Chi Lan and Chung-Ming Wang [6], combining a 5-D hyperchaotic map, generalized rectangular transform, bit-level permutations, and SHA-512 key generation for secure multi-image processing.

Qiang Lai et al. [7] introduced a 3-D medical model encryption scheme leveraging a memristive hyperchaotic map (LC-CMHM), while Rasha S. Ali et al. [11] integrated multi-chaotic maps with a hybrid CNN-Transformer model for medical image defense. Other researchers focus on complex matrix operations and spatial mappings; Pengbo Liu et al. [8] utilized a sine–cosine coupled mapping lattice (SCCML) for multi-face encryption, and Yunlong Liao et al. [12] constructed an image security framework based on the 3D-LMM, which integrates three-dimensional substitution boxes (S-boxes) alongside fractal sorting and Fibonacci Q-matrix operations. Additionally, Renjie Song and Haixia Zhao [9] combined optimized S-boxes with a hyperchaotic system to achieve rigorous multi-stage diffusion.

Designed specifically for IoT networks, the MMCBIE framework developed by Kurunandan Jain et al. [14] is an approach that offers a low-overhead image security framework that combines multiple chaotic maps to enhance the system's resistance to both confusion and diffusion attacks. Aiming to refine map dynamics, Abdurrahim Toktas et al. [15] developed a multiobjective optimized 2-D hyperchaotic system tuned via a Leader Pareto Grey Wolf Optimizer (LP-GWO). Meanwhile, the OSMRD-IE framework, engineered by Ugur Erkan et al. [16], utilizes a 2-D hybrid Michalewicz–Ackley hyperchaotic system coupled with base-8 permutation and multi-tier rotational diffusion. Suo Gao et al. [17] developed a 2-D memristive cubic map (2D-MCM) tailored for securing video streams, utilizing memristor-based hyperchaotic behaviors to synthesize superior pseudorandom sequences and elevate overall cryptosystem robustness.

To mitigate modeling vulnerabilities, an LFSR-APUF lightweight authentication protocol featuring dynamic challenge obfuscation and secure CRP handling was put forward by Yao Wang et al. [18]. Xiuli Chai et al. [19] introduced a medical image protection framework optimized for cloud-assisted healthcare, which unifies chaotic diffusion mechanisms with semi-tensor product compressed sensing for secure transmission. Finally, focusing on the fundamental generation of chaotic signals, Han Bao et al. [20] constructed a memristor-based 3-D hyperchaotic map model tailored to yield maximum randomness for next-generation security applications.

III. METHODS AND METHODOLOGIES

The proposed system is illustrated below in Figure 1. The input coloured image undergoes dynamic key generation which is used in AES encryption and decryption. The key is used to generate the initial hyperchaotic sequence values which is used for scrambling and diffusion of pixels before sending the image for AES encryption.

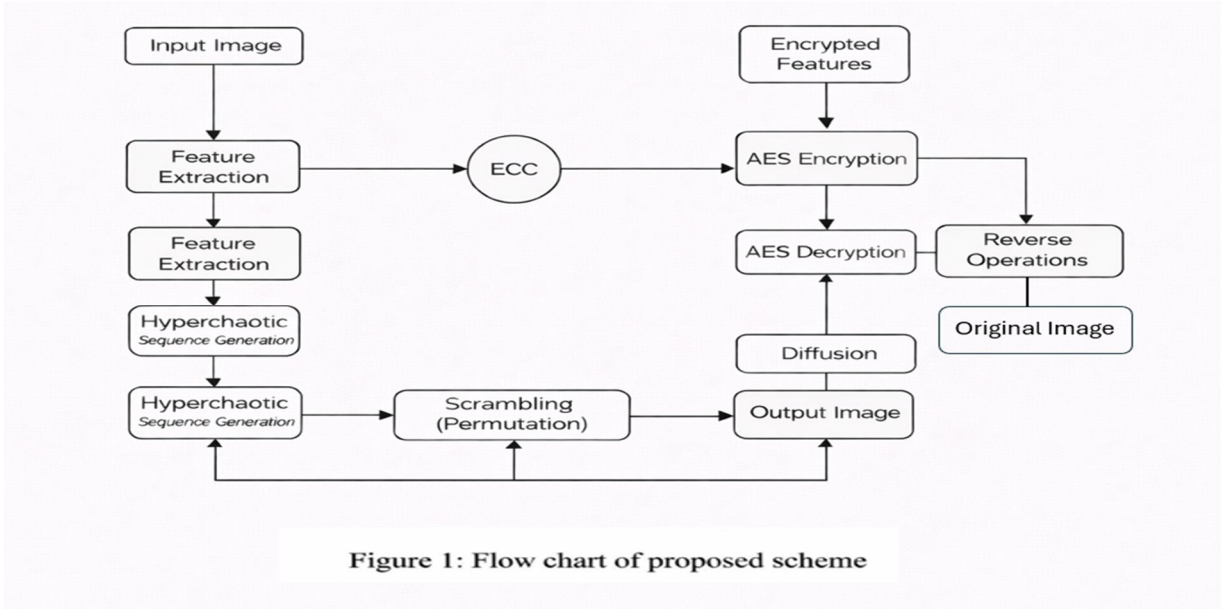


Figure 1: Flow chart of proposed scheme

A. *Feature Extraction*

Feature extraction is the initial step in the proposed system. To establish plaintext dependency, the mean intensity, standard deviation, and entropy profiles are mathematically derived from the initial image data. These features uniquely represent the image and are used to generate dynamic keys.

```
Input:  Image (I)
Output: Feature vector (F)

1: Read input image (I)
2: Convert image to grayscale (if required)
3: Compute mean intensity:  mu = mean(I)
4: Compute standard deviation:  sigma = std(I)
5: Compute entropy:  H = -sum[ p(i)*log2(p(i)) ]
6: Form feature vector:  F = (mu, sigma, H)
7: Convert F into byte format
8: return F
```

B. *Dynamic Key Generation*

The extracted features are combined with a shared secret key and a randomly generated nonce. A cryptographic hash function (BLAKE2b) is applied to generate a strong and unpredictable key. This key is used to initialize the chaotic system parameters.

```
Input:  Feature vector (F), shared key (Ks), nonce (N)
Output: Dynamic key (Kd)

1: Convert feature vector F to byte stream
2: Concatenate inputs:  D = F || Ks || N
3: Apply cryptographic hash:  Kd = BLAKE2b(D)
4: Normalize key values for chaotic system parameters
5: return Kd
```

C. *Elliptic Curve Cryptography (ECC)*

ECC is responsible for secure session key exchange between communication endpoints. A private-public key pair is generated, and a shared secret is derived using elliptic curve operations. This shared key is never transmitted directly over the channel.

```
Input:  Receiver public key (Qr)
Output: Shared secret key (Ks)

1: Select elliptic curve parameters
2: Generate sender private key (ds)
3: Compute sender public key:  Qs = ds * G
4: Compute shared secret point:  S = ds * Qr
5: Extract x-coordinate of S
6: Apply hash function:  Ks = SHA-256(Sx)
7: return Ks
```

D. AES-Based Feature Protection

To protect the extracted image features during transmission, AES encryption is applied in CBC mode. The feature data is encrypted using a symmetric key derived from the ECC shared secret, ensuring confidentiality and preventing information leakage.

Input: Feature vector (F), key (Ks)
Output: Encrypted features (Cf), IV

1: Generate random Initialization Vector (IV)
2: Select AES mode (CBC)
3: Apply padding to feature data
4: Encrypt feature vector: Cf = AES_Encrypt(F, Ks, IV)
5: return Cf, IV

E. Hyperchaotic Sequence Generation

A hyperchaotic map generates pseudo-random sequences based on the dynamic key parameters. These sequences demonstrate extreme sensitivity to their starting values, which serves to drive and control the subsequent image scrambling and diffusion phases.

Input: Secret key (Kd), image size (R X C)
Output: Chaotic sequence (A)

1: Extract parameters from Kd: u0, v0, w0, c1, c2, c3
2: Initialize chaotic variables
3: For each iteration index j from 1 to R X C do
4: $u_{j+1} = c_1 v_j + c_2 \cos(w_j) v_j$
5: $v_{j+1} = c_3 \cos(u_j + v_j)$
6: $w_{j+1} = 0.1(w_j + v_j)$
7: $A_j = |u_{j+1}| (\mathrm{mod}\ 1)$
8: end for
9: Reshape A into grid R x C
10: return A

F. Scrambling Process (Permutation)

The algorithm utilizes the chaotic sequence to alter pixel positions during the scrambling phase, disrupting the spatial correlation of the image. This operation disrupts the dense spatial correlation inherently present among neighbouring pixels, thereby successfully inducing confusion across the image matrix. Scrambling indices are stored for use during decryption.

G. Diffusion Process

After scrambling, the diffusion process modifies pixel values using the chaotic sequence and previously encrypted pixels. By ensuring that slight variations in the source image completely transform the encrypted matrix, the system achieves the high plaintext sensitivity required to resist differential security threats.

H. Dataset-Based Implementation

The system is implemented on a dataset of multiple images to evaluate performance across different types, sizes, and patterns, validating its robustness and scalability. Encrypted and decrypted outputs are stored separately for evaluation.

IV. RESULTS AND PERFORMANCE ANALYSIS

The security performance of this cryptographic scheme is verified using standard metrics for statistical and differential analysis. The performance of the developed framework is tested using a varied selection of images with diverse resolutions and visual properties to thoroughly analyze its computational throughput and defensive capabilities.

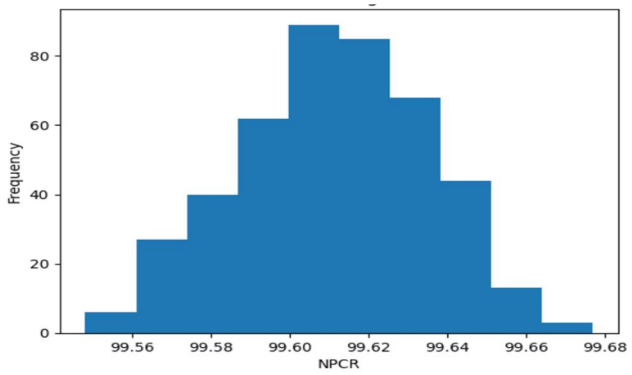
A. *Number of Pixel Change Rate (NPCR)*

The Number of Pixels Change Rate (NPCR) measures the percentage of different pixels between two ciphertexts generated from a pair of plaintext images differing by only a single pixel. A elevated NPCR metric indicates an enhanced ability to resist differential cryptanalysis. NPCR calculation formula [13] is as follows:

$$NPCR = \left(\frac{\sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j)}{M \times N} \right) \times 100\%$$

To quantify the pixel-level differences between the pair of cipherimages C_1 and C_2, the function D(i, j) is implemented. In this context, M and N specify the vertical and horizontal pixel bounds, respectively, with the function defined as:

$$D(i,j) = \begin{cases} 0, & \text{if } C_1(i,j) = C_2(i,j) \\ 1, & \text{if } C_1(i,j) \neq C_2(i,j) \end{cases}$$

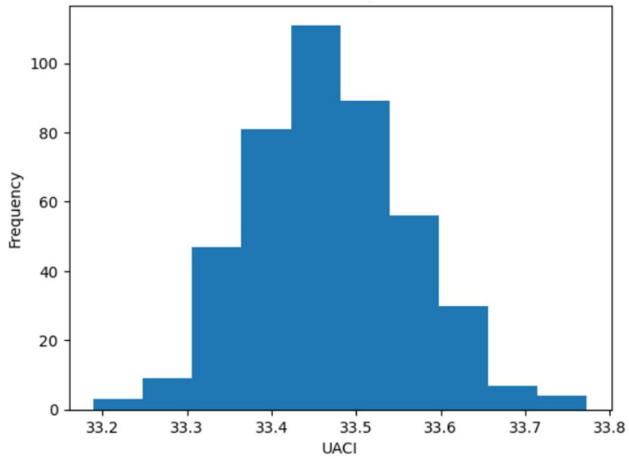


B. *Unified Average Changing Intensity (UACI)*

UACI quantifies the average intensity discrepancies between two cipher-images derived from a pair of plaintext inputs with a single-pixel variance. It indicates the extent to which pixel values vary when a minor change is introduced into the original image. The UACI calculation formula is [13] as follows:

$$\mathbf{UACI} = \frac{1}{M \times N} \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100$$

Here, C_1 and C_2 denote the ciphertext pairs derived from two original images that are identical except for one pixel. To evaluate pixel-level changes, the absolute difference $|C_1(i, j) - C_2(i, j)|$ is used to compute the local intensity variation at coordinate (i, j).



C. Experimental Results

The numerical results for NPCR and UACI, which evaluate the different test images, are compiled below in Table I.

Image Name	NPCR (%)	UACI (%)
Buildings	99.61	33.46
Forest	99.59	33.45
Glacier	99.64	33.32
Sea	99.60	33.56
Street	99.56	33.47
Mountain	99.62	33.41

Table I: NPCR and UACI values

D. Results Analysis

The empirical results show that NPCR metrics consistently exceed \$99\%\$, demonstrating that the proposed encryption architecture is highly responsive to single-pixel alterations in the input data. Furthermore, the corresponding UACI values closely approximate the theoretical ideal of 33.46%, which verifies a substantial and uniform intensity divergence between the evaluated cipher-images. These findings validate that the proposed CPL-IES cryptosystem offers robust immunity against differential cryptanalysis. By synergizing chaotic maps, dynamic key synthesis, Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC), the framework successfully guarantees an exceptional degree of entropy and unpredictability across the cipher-images.

E. Security Evaluation

The elevated NPCR and UACI metrics confirm that the encryption framework achieves a highly effective diffusion mechanism, successfully propagating localized pixel modifications throughout the entire ciphertext matrix. Furthermore, the strategic deployment of ECC for secure key management alongside AES for feature-level protection substantially fortifies the comprehensive security posture of the cryptosystem.

F. Distribution Histogram

The uniformity of the encrypted pixel distribution is evaluated via histogram analysis, confirming that the framework completely conceals the original image's statistical and visual characteristics. In a normal image, the histogram contains irregular peaks and varying intensity distributions because neighbouring pixels are highly correlated. The resulting cipherimage histogram displays a highly uniform distribution, indicating a comprehensive randomization of pixel intensities that successfully obscures the original data patterns. Given below in Fig. 2, the changes occurred on the various images for encryption and decryption.

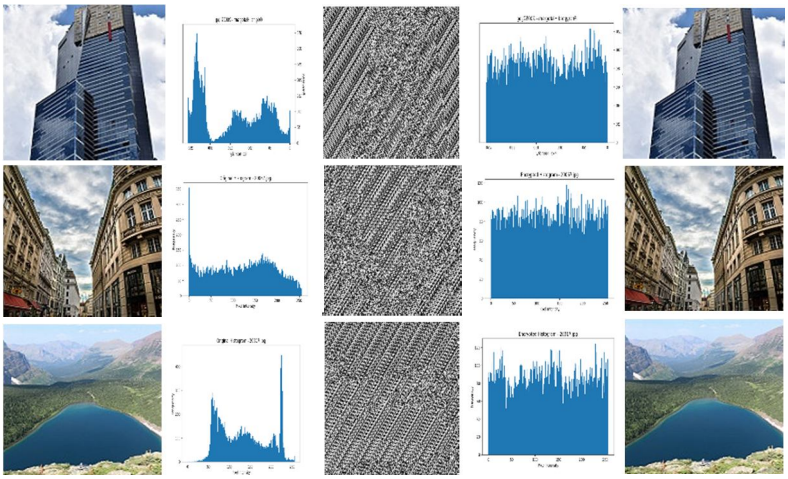


Fig. 2 Histogram of the source image, the encryption and decryption results

V. DISCUSSION

Integrating a hyperchaotic approach with ECC-driven key exchange and AES protection for feature information significantly enhances image encryption security. Runtime key generation guarantees that the encryption framework is inherently responsive to the structural features of the source image, effectively neutralizing linear and differential security threats. This operational efficiency is evidenced through empirical NPCR and UCAI results; the extensive flip rate of the output bits strongly demonstrates the exceptional diffusion characteristics of the proposed algorithm.

Furthermore, the deployment of ECC facilitates secure and highly optimized key management utilizing significantly reduced key lengths. Due to its minimal computational overhead, the proposed framework is ideally optimized for deployment on resource-limited hardware, including mobile devices and IoT nodes, while preserving robust cryptographic defense. The feature-oriented key generation method links the encryption process directly to the image content, whereas AES preserves data confidentiality and integrity during communication.

In conclusion, the introduced cryptographic architecture successfully strikes an optimal trade-off between performance and strong security, making it applicable to real-world scenarios including healthcare, financial systems, government communications, and cloud services. The results highlight that integrating advanced chaotic techniques with hybrid key management strategies offers a reliable defense against modern cryptographic threats.

VI. CONCLUSION

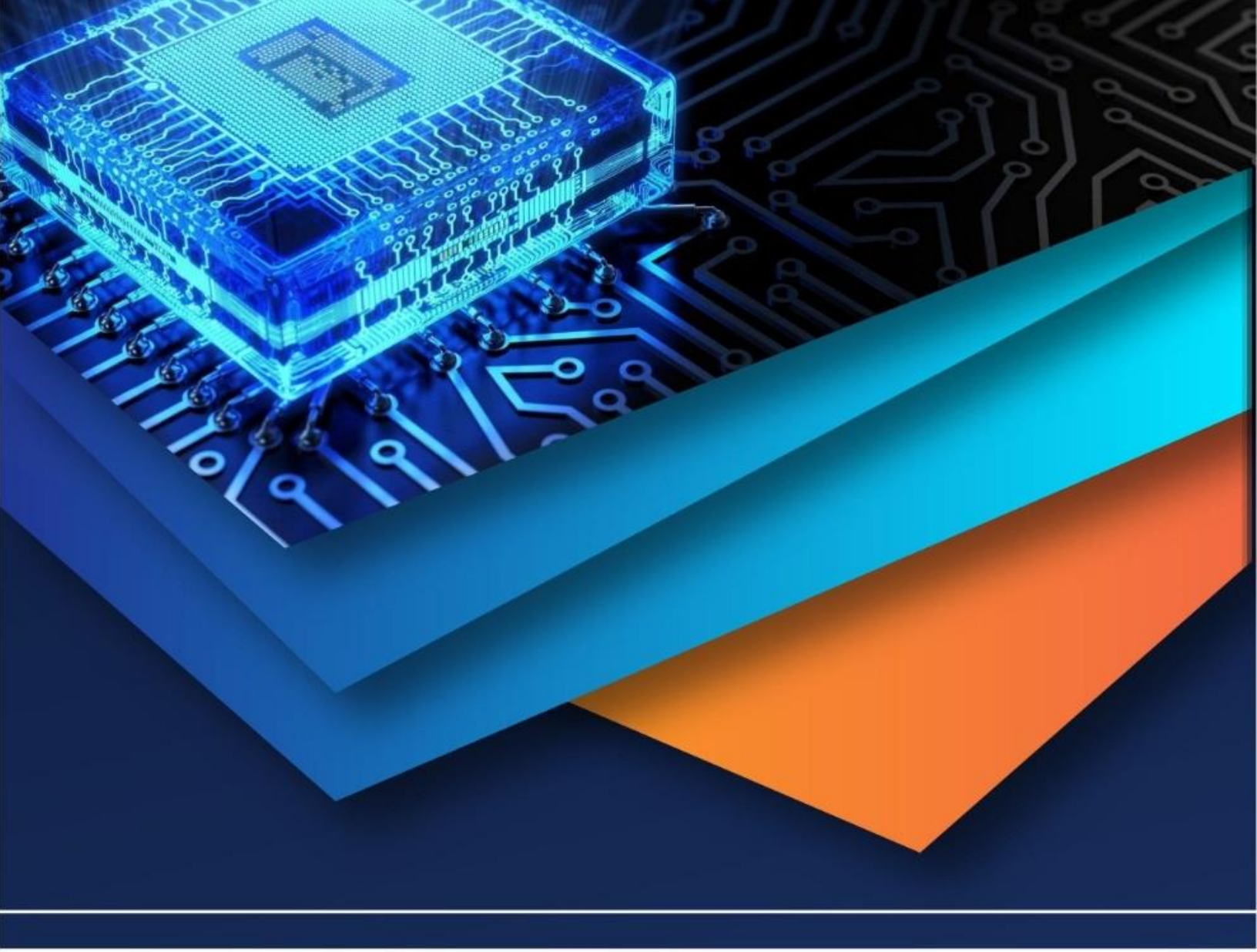
The effectiveness of image encryption is notably enhanced by integrating a hyperchaotic encryption technique with feature-based dynamic key generation and ECC-driven key exchange. The dynamic key approach introduces variability tied to the image content, strengthening resistance against attacks, while ECC ensures secure and efficient sharing of keys.

The proposed approach incorporates a hyperchaotic mechanism for pixel permutation and diffusion, AES to protect extracted feature data, and ECC for secure key distribution. Together, these elements form a reliable, efficient, and secure framework for modern image protection, with potential extensions toward real-time video encryption and lightweight solutions for edge computing systems.

REFERENCES

[1] 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. 18115–18124, 2025.
[2] L. Moysis et al., "Exploiting circular shifts for efficient chaotic image encryption," IEEE Access, vol. 13, pp. 92997–93016, 2025.
[3] B. Yogi, A. K. Khan, and S. Roy, "HL-CAIoT: Hybrid lightweight cipher for IoT with chaotic maps and cellular automata," IEEE Access, vol. 13, pp. 168067–168086, 2025.
[4] B. Acharya et al., "MIE-SPD: A new and highly efficient chaos-based multiple image encryption technique with synchronous permutation diffusion," IEEE Access, vol. 13, pp. 62773–62797, 2025.
[5] S. S. Silva et al., "A hardware-efficient chaotic PRNG exploring posit arithmetic for secure image encryption," IEEE Access, vol. 13, pp. 209813–209828, 2025.
[6] Y.-C. Lan and C.-M. Wang, "A novel multi-image encryption scheme using generalized rectangular transform and advanced 5-D hyperchaotic map," IEEE Access, vol. 13, pp. 43316–43337, 2025.
[7] Q. Lai, H. Hua, and L. Yang, "Encryption design and analysis of 3-D medical models in Internet of Medical Things using a novel memristive hyperchaotic map," IEEE Internet of Things Journal, vol. 12, no. 18, pp. 39019–39028, Sept. 2025.
[8] P. Liu et al., "Enhancing image security with a novel chaotic system: A focus on multiface image encryption in smart applications," IEEE Internet of Things Journal, vol. 12, no. 12, pp. 20087–20098, 2025.
[9] R. Song and H. Zhao, "Security-enhanced image encryption: Combination of S-boxes and hyperchaotic integrated systems," IEEE Access, vol. 13, pp. 105151–105164, 2025.
[10] S. Zhou et al., "A new class of Hamiltonian chaotic systems with simple structure and complex behaviors," IEEE Internet of Things Journal, vol. 12, no. 18, pp. 36880–36892, 2025.
[11] R. S. Ali et al., "Proposal medical image protection system based on hybrid CNN-transformer model and chaotic maps," IEEE Access, vol. 13, pp. 123793–123807, 2025.
[12] Y. Liao et al., "Using 3D-LMM-based encryption to secure digital images with 3-D S-box and Fibonacci Q-matrix," IEEE Internet of Things Journal, vol. 12, no. 24, pp. 55182–55195, 2025.
[13] Q. Lai and L. Ji, "A lightweight image encryption scheme using hyperchaotic map and collision-parity principle," IEEE Internet of Things Journal, vol. 12, no. 11, pp. 17977–17986, Jun. 2025.
[14] K. Jain et al., "A lightweight multi-chaos-based image encryption scheme for IoT networks," IEEE Access, vol. 12, pp. 62118–62148, 2024.
[15] A. Toktas et al., "Multiobjective design of 2D hyperchaotic system using leader Pareto grey wolf optimizer," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 54, no. 9, pp. 5237–5247, Sept. 2024.
[16] U. Erkan et al., "OSMRD-IE: Octal-based shuffling and multilayer rotational diffusing image encryption using 2-D hybrid Michalewicz–Ackley map," IEEE Internet of Things Journal, vol. 11, no. 21, pp. 35113–35123, Nov. 2024.

[17] S. Gao et al., "Design, hardware implementation, and application in video encryption of the 2-D memristive cubic map," IEEE Internet of Things Journal, vol. 11, no. 12, pp. 21807–21815, Jun. 2024.
[18] Y. Wang et al., "A lightweight authentication protocol against modeling attacks based on a novel LFSR-APUF," IEEE Internet of Things Journal, vol. 11, no. 1, pp. 283–295, Jan. 2024.
[19] Q. Lai and G. Hu, "A nonuniform pixel split encryption scheme integrated with compressive sensing and its application in IoMT," IEEE Transactions on Industrial Informatics, vol. 20, no. 9, pp. 11262–11272, Sept. 2024.
[20] X. Chai et al., "Exploiting semi-tensor product compressed sensing and hybrid cloud for secure medical image transmission," IEEE Internet of Things Journal, vol. 10, no. 8, pp. 7380–7392, Apr. 2023.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY