IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155171

A Hybrid EIGamal - AES Based Secure Image Encryption System

Gunipe Abhinav[1], K.V.V Subba Rao[2]

M. Tech Scholar, CSE, Pragati Engineering college, Kakinada, India[1]

Assistant Professor, CSE, Pragati Engineering college, Kakinada, India[2]

Abstract: The rapid progress of digital communication has increased the need for secure image protection mechanisms in applications such as healthcare, cloud storage, surveillance, military communication, and multimedia systems. Since image data contains high redundancy and strong correlation between neighbouring pixels, traditional text-oriented encryption techniques alone are not always sufficient for efficient and secure image protection. This paper presents a hybrid image encryption framework that combines the Advanced Encryption Standard (AES) and the ElGamal public-key cryptosystem to achieve both computational efficiency and secure key management. In the proposed model, AES is used to encrypt image data because of its fast processing capability, while ElGamal is employed to protect the AES secret key during transmission. The system also integrates statistical and performance evaluation modules to validate encryption strength. Security analysis is performed using entropy evaluation, histogram analysis, NPCR, UACI, key sensitivity testing, and noise attack simulation. Experimental observations show that the encrypted images exhibit strong randomness, uniform pixel distribution, and high resistance against differential and statistical attacks. The framework also demonstrates efficient encryption and decryption performance for different image sizes. The proposed hybrid approach provides a practical and reliable solution for secure image transmission and storage applications.

Keywords: Image Encryption, AES, ElGamal, Hybrid Cryptography, Secure Image Transmission, NPCR, UACI, Entropy Analysis

I. INTRODUCTION

The continuous expansion of internet-based communication systems has significantly increased the exchange of digital images across open and distributed networks. Images are now widely used in cloud computing, social media platforms, healthcare systems, biometric authentication, military surveillance, industrial automation, and multimedia communication. Since images often contain sensitive or confidential information, protecting them from unauthorized access has become an important requirement in modern information security systems.

Unlike textual information, image data contains high redundancy and strong correlation among neighboring pixels. These properties make image encryption more challenging than conventional text encryption. Direct application of traditional cryptographic algorithms on image data may increase computational overhead and reduce efficiency, especially for high-resolution images [1]. Therefore, secure image communication requires encryption techniques that provide both strong protection and efficient processing capability.

Symmetric encryption algorithms are commonly used for fast data encryption. Among them, the Advanced Encryption Standard (AES) is considered one of the most secure and efficient encryption algorithms for large-scale data protection [2]. AES performs encryption using substitution and permutation operations, making it highly suitable for multimedia security applications. However, symmetric encryption introduces a major challenge related to secure key distribution. If the secret key is intercepted during transmission, the encrypted data can easily be compromised.

To overcome this limitation, asymmetric cryptographic algorithms are used for secure key management. ElGamal public-key cryptography provides secure key exchange through mathematically complex operations based on the discrete logarithm problem [3]. Although asymmetric algorithms provide secure key distribution, applying them directly to large image data results in high computational cost and slower execution time.

Hybrid cryptographic systems combine the strengths of both symmetric and asymmetric encryption methods [4]. In such systems, the image data is encrypted using a fast symmetric algorithm, while the symmetric key is protected using an asymmetric encryption mechanism. This approach ensures both computational efficiency and secure key management.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026
DOI: 10.17148/IJARCCE.2026.155171

The proposed work presents a hybrid ElGamal–AES based secure image encryption framework that integrates image encryption, key protection, statistical validation, and performance evaluation into a unified system. The image data is encrypted using AES, while the AES secret key is secured using ElGamal encryption. In addition to encryption and decryption operations, the system evaluates encryption quality using entropy analysis, histogram distribution, NPCR, UACI, key sensitivity testing, and noise attack simulation [5], [6].

II. RELATED WORK

Image encryption has become an active research area due to the increasing demand for secure multimedia communication. Several techniques have been proposed over the years to improve confidentiality, randomness, and resistance against cryptographic attacks.

Fridrich introduced one of the early chaotic-map based image encryption models that combined permutation and diffusion operations to reduce pixel correlation and improve randomness [1]. The proposed method demonstrated that image encryption requires specialized processing beyond traditional text encryption methods. However, later studies showed that certain chaotic systems may become vulnerable if parameters are not selected carefully.

Wu et al. introduced NPCR and UACI metrics as statistical measures to evaluate the resistance of image encryption algorithms against differential attacks [5]. Their work established theoretical standards for randomness evaluation and became widely adopted in image encryption research. These metrics are now commonly used to verify whether small changes in the plaintext image produce significant differences in the encrypted output.

Arroyo et al. analyzed weaknesses in chaotic image encryption systems and demonstrated that some schemes fail under cryptanalysis because of predictable diffusion structures and weak parameter generation [6]. Their work highlighted the importance of proper key management and rigorous statistical evaluation while designing secure image encryption frameworks.

Zhang proposed a unified image encryption approach based on chaotic transformation and diffusion operations [7]. The study reported strong entropy values and uniform histogram distributions, indicating improved randomness in encrypted images. However, chaotic systems often require careful synchronization and parameter control during implementation.

Chowdhary conducted an analytical study on hybrid encryption techniques and demonstrated that combining symmetric and asymmetric cryptographic approaches can significantly improve both efficiency and security [4]. The study showed that hybrid cryptographic models are more suitable for practical multimedia security applications compared to using symmetric or asymmetric techniques independently.

Parenreng implemented an AES–ElGamal hybrid model for secure email communication [8]. In that work, AES was used for message encryption, while ElGamal protected the encryption key. The study confirmed that hybrid cryptography improves secure key exchange while maintaining efficient encryption performance.

Recent studies have also focused on integrating performance evaluation with encryption systems. Shen et al. proposed a secure image encryption approach with entropy analysis, histogram evaluation, NPCR, and timing analysis to validate encryption quality [9]. Their results demonstrated that statistical analysis plays an important role in verifying cryptographic robustness.

Although many image encryption methods have been proposed, several limitations still exist in current systems. Some approaches focus mainly on encryption and decryption without conducting detailed security analysis. Other systems provide strong security but suffer from high computational overhead. In addition, certain methods lack practical implementation support such as batch processing or user-friendly interfaces.

III. PROPOSED SYSTEM ARCHITECTURE

The proposed system follows a layered hybrid cryptographic architecture designed to provide secure image encryption, protected key management, and quantitative security validation. The architecture combines symmetric encryption for efficient image processing and asymmetric encryption for secure key exchange.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155171

The complete framework is divided into the following major layers:

1) User Interaction Layer
2) Encryption and Processing Layer
3) Security Analysis Layer
4) Storage and Output Layer

The overall workflow of the system is illustrated below.

Fig. 1. Proposed Hybrid ElGamal–AES System Architecture

In the proposed framework, the user first uploads an image through the interface layer. The image is converted into processable matrix form and passed to the encryption module. A random AES secret key is generated to encrypt the image data efficiently. Since AES is a symmetric encryption algorithm, it provides fast execution for large image files.

After image encryption, the AES secret key is protected using the ElGamal public-key cryptosystem. Instead of transmitting the secret key directly, the system encrypts the key using the receiver's public key. This process ensures secure key distribution over untrusted communication channels.

The encrypted image and encrypted key are then stored securely in the output layer. At the same time, the encrypted image is forwarded to the security analysis layer where entropy, histogram, NPCR, UACI, and key sensitivity evaluations are performed.

The architecture also supports decryption operations. During decryption, the AES key is first recovered using the ElGamal private key. The recovered AES key is then used to restore the original image.

IV. METHODOLOGY

The proposed methodology combines AES-based image encryption and ElGamal-based key protection into a unified hybrid cryptographic framework. The methodology mainly consists of image preprocessing, AES encryption, ElGamal key encryption, decryption, and statistical evaluation.

A. AES-Based Image Encryption

AES is used to encrypt the image data because of its strong security and efficient execution performance [2]. The input image is first converted into a byte stream and divided into fixed-size blocks for processing.

AES performs multiple rounds involving substitution, permutation, row shifting, and key addition operations. These transformations reduce pixel correlation and increase randomness in the encrypted image.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155171

The AES encryption procedure provides:

- Fast encryption performance
- Strong confusion and diffusion properties
- Resistance against brute-force attacks
- Efficient handling of high-resolution images

B. ElGamal Key Encryption

Although AES provides efficient image encryption, the secret key must be transmitted securely. To solve this issue, ElGamal public-key cryptography is used to encrypt the AES secret key.

The ElGamal public-key parameters are:

p: Large prime number
g: Generator value
x: Private key

Since ElGamal security depends on the discrete logarithm problem, recovering the AES key without the private key becomes computationally infeasible [3].

C. Hybrid Encryption Workflow

The hybrid encryption workflow combines both AES and ElGamal operations.

Encryption Procedure

1) Load the input image
2) Generate a random AES key
3) Encrypt the image using AES
4) Encrypt the AES key using ElGamal
5) Store encrypted image and encrypted key
6) Perform statistical analysis

Decryption Procedure

1) Retrieve encrypted image and encrypted key
2) Recover AES key using ElGamal private key
3) Decrypt image using recovered AES key
4) Restore original image

The overall operational flow is shown below.

Fig. 2. Hybrid Encryption and Decryption Workflow

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026
DOI: 10.17148/IJARCCE.2026.155171

D. Security Evaluation Methodology

To validate encryption strength, multiple statistical analyses are performed.

1) Entropy Analysis: Entropy measures randomness in encrypted images. For secure 8-bit image encryption, entropy values should be close to 8.

2) NPCR Analysis: NPCR measures how significantly encrypted images change when a single pixel in the input image is modified. High NPCR values indicate strong resistance against differential attacks [5].

3) UACI Analysis: UACI measures the average intensity variation between encrypted images generated from slightly different plaintext inputs.

4) Histogram Analysis: Histogram analysis verifies whether encrypted images exhibit uniform pixel distribution without visible statistical patterns.

5) Key Sensitivity Testing: The system evaluates the effect of minor changes in encryption keys. Even a small key variation should produce completely different ciphertext output.

E. Implementation Environment

The proposed system is implemented using Python with the following technologies:

- PyCryptodome for AES implementation
- Custom ElGamal module for key encryption
- NumPy for matrix operations
- Matplotlib for histogram generation
- Streamlit for web-based interaction

The implementation also supports batch image encryption and performance benchmarking for multiple image sizes.

V. RESULTS AND SECURITY ANALYSIS

The proposed hybrid ElGamal-AES image encryption system was tested using multiple grayscale and colour images of different resolutions. The experiments were conducted to evaluate encryption quality, resistance against attacks, computational efficiency, and overall system reliability. The encrypted images were analysed using entropy evaluation, histogram analysis, NPCR, UACI, key sensitivity testing, and execution time measurements.

The implementation successfully transformed the original images into visually unrecognizable encrypted outputs while preserving accurate image recovery during decryption.

A. Encryption and Decryption Results

The encryption module converts the original image into ciphertext form using AES encryption, while the AES key is protected using ElGamal cryptography. During decryption, the original image is restored successfully using the recovered AES key.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155171

Fig. 3. Original Input Image

Fig. 4. Encrypted Image Output

Fig. 5. Decrypted Image Output

The encrypted image appears highly random without revealing any visible structural information from the original image. The decrypted output matches the original image accurately, confirming the correctness of the hybrid encryption and decryption process.

B. Histogram Analysis

Histogram analysis is used to examine the distribution of pixel intensity values before and after encryption. A secure encryption system should generate an encrypted image histogram with nearly uniform distribution so that attackers cannot identify statistical patterns [7].

The histogram of the original image generally contains irregular peaks due to natural image characteristics. However, the histogram of the encrypted image becomes uniformly distributed, indicating strong randomness and reduced pixel correlation.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155171

The histogram analysis confirms that the proposed encryption framework effectively conceals statistical information from the plaintext image.

C. Entropy Analysis

Entropy measures the randomness present in encrypted images. For an ideal 8-bit encrypted image, the entropy value should approach 8 [5].

The entropy values obtained from experimental evaluation are shown in Table I.

TABLE I: ENTROPY ANALYSIS RESULTS

Image Name	Entropy Value
Image 1	7.9961
Image 2	7.9948
Image 3	7.9974
Image 4	7.9959

The observed entropy values are very close to the theoretical ideal value. This indicates that the encrypted images contain high randomness and minimal predictability.

D. NPCR and UACI Analysis

NPCR (Number of Pixel Change Rate) and UACI (Unified Average Changing Intensity) are important metrics used to evaluate resistance against differential attacks [5].

A small modification in the input image should produce major changes in the encrypted image. High NPCR and UACI values indicate stronger security against chosen-plaintext and differential attacks.

TABLE II: NPCR AND UACI RESULTS

Image	NPCR (%)	UACI (%)
Image 1	99.62	33.41
Image 2	99.58	33.29
Image 3	99.64	33.52
Image 4	99.60	33.37

The obtained values are close to the ideal theoretical values suggested in image encryption research [5]. This confirms that the proposed system demonstrates strong sensitivity to plaintext variations.

Although the decrypted images experienced partial quality degradation after noise injection, no meaningful structural information from the original image was exposed directly through the encrypted image. This demonstrates robustness against transmission disturbances.

VI. PERFORMANCE EVALUATION

Performance evaluation was conducted to measure encryption and decryption efficiency for different image resolutions. Since AES handles the primary image encryption process, the system achieves efficient execution even for large image files. Execution time was measured using system clock functions during runtime.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026
DOI: 10.17148/IJARCCE.2026.155171

A. Encryption and Decryption Time

The results show that encryption and decryption time increase gradually with image resolution. However, the overall execution remains computationally efficient because the bulk image data is encrypted using AES rather than asymmetric encryption.

B. Batch Processing Performance

The proposed system also supports sequential encryption of multiple images. Batch processing was tested using collections of images with different resolutions. The batch processing functionality operated successfully without runtime instability, demonstrating practical applicability for secure image archives and multimedia datasets.

C. Comparative Discussion

Compared with traditional image encryption methods, the proposed hybrid framework provides several advantages:

1) Faster execution than pure asymmetric encryption systems
2) More secure key management than standalone AES-based systems
3) Better statistical randomness compared to several chaotic encryption methods
4) Integrated security validation and performance evaluation
5) Practical deployment capability using graphical and web-based interfaces

The system achieves a balanced tradeoff between security strength and computational efficiency.

VII. IMPLEMENTATION DETAILS

The proposed hybrid image encryption system was developed using Python due to its flexibility and extensive support for cryptographic processing, image manipulation, and analytical computation. A modular implementation strategy was followed so that each component of the system could operate independently while maintaining smooth integration with other modules. This structure improves code organization, simplifies future modifications, and supports scalability for additional features.

Several libraries and development tools were integrated during implementation to handle different functionalities within the system. Python 3.x served as the primary programming platform for developing the complete framework. The AES encryption operations were implemented using the PyCryptodome library, which provides secure and efficient cryptographic functions. NumPy was utilized for performing matrix-based computations and numerical operations on image pixel data. Image loading, processing, and reconstruction tasks were carried out using the Pillow (PIL) library. For generating histograms and graphical analysis outputs, Matplotlib was incorporated into the system. In addition, a Streamlit-based interface was developed to provide an interactive and user-friendly web environment for image encryption, decryption, and security analysis operations.
The implementation supports:

- Image encryption and decryption
- AES key generation
- ElGamal key protection
- Statistical analysis
- Batch image processing
- Real-time performance measurement

The web interface allows users to upload images, perform encryption and decryption, and visualize analysis results without interacting directly with cryptographic operations.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155171

Fig. 6. Security Analysis Result Screen

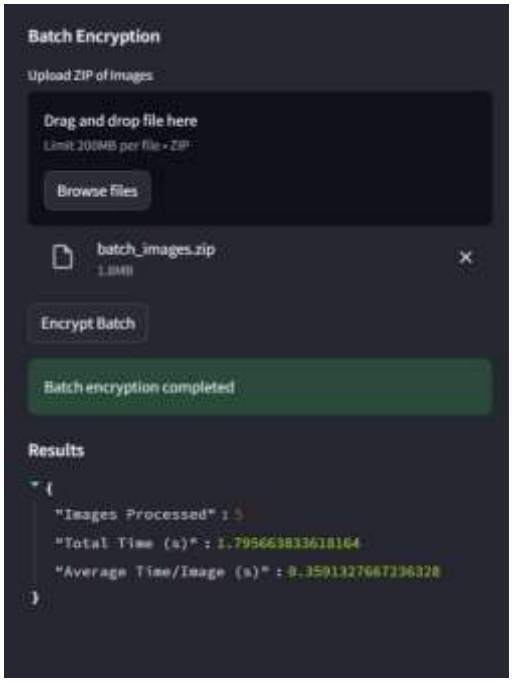

Fig. 7. Batch Encryption Execution Screen

The modular implementation ensures that future extensions such as cloud integration, real-time transmission security, or AI-assisted attack analysis can be incorporated easily.

VIII. DISCUSSION

The experimental results demonstrate that the proposed hybrid encryption system successfully combines the strengths of AES and ElGamal cryptography. AES provides fast and efficient encryption for large image datasets, while ElGamal ensures secure key exchange without exposing the symmetric key during transmission.

Statistical evaluation confirms that the encrypted images exhibit strong randomness and resistance against differential attacks. High entropy values and uniform histogram distribution indicate that the ciphertext images do not reveal meaningful statistical patterns. Similarly, the NPCR and UACI results confirm strong sensitivity to minor changes in plaintext images.

Compared to chaotic image encryption methods [1], [7], the proposed framework offers a more structured cryptographic foundation and reliable key management mechanism. Unlike pure asymmetric encryption systems, the proposed hybrid approach significantly reduces computational overhead while maintaining strong security.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026
DOI: 10.17148/IJARCCE.2026.155171

The implementation also demonstrates practical usability through batch image processing and user-friendly interfaces. These characteristics make the framework suitable for real-world secure multimedia applications.

IX. CONCLUSION

This paper presented a hybrid ElGamal–AES based secure image encryption framework designed to provide both computational efficiency and strong cryptographic security. The proposed system encrypts image data using AES and secures the AES secret key using the ElGamal public-key cryptosystem. The framework also integrates multiple statistical and performance evaluation techniques including entropy analysis, histogram analysis, NPCR, UACI, key sensitivity testing, and noise attack simulation to validate encryption quality. Experimental results demonstrated high randomness, strong resistance against statistical and differential attacks, secure key dependency, and efficient execution performance for different image sizes. The implementation further supports batch image encryption and user-friendly interaction, making the system practical for secure image storage and transmission applications. Overall, the proposed hybrid framework provides a reliable and effective solution for protecting digital image data in modern communication environments.

REFERENCES

[1]. J. Fridrich, “Image encryption based on chaotic maps,” Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics, pp. 1105–1110, 1998.
[2]. Y. Wu, J. P. Noonan, and S. Agaian, “NPCR and UACI randomness tests for image encryption,” Journal of Selected Areas in Telecommunications, vol. 2, no. 2, pp. 31–38, 2011.
[3]. D. Arroyo, C. Li, S. Li, and G. Alvarez, “Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm,” Chaos, Solitons & Fractals, vol. 41, no. 5, pp. 2613–2616, 2009.
[4]. Y. Zhang, “The unified image encryption algorithm based on chaos,” Information Sciences, vol. 425, pp. 52–65, 2018.
[5]. C. L. Chowdhary, “Analytical study of hybrid techniques for image encryption,” IEEE Access, vol. 8, pp. 39386–39400, 2020.
[6]. H. R. Hashim, “Image encryption and decryption in a modification of ElGamal,” International Journal of Computer Applications, vol. 179, no. 19, pp. 1–6, 2018.
[7]. Y. Shen, L. Zhang, and X. Wang, “Fast and secure image encryption algorithm based on improved chaotic mapping,” Entropy, vol. 25, no. 3, pp. 1–18, 2023.
[8]. Y. Sang, X. Li, and H. Li, “Image encryption based on logistic chaotic systems and deep autoencoder,” Pattern Recognition Letters, vol. 154, pp. 45–52, 2022.
[9]. J. M. Parenreng, “E-mail security system using El-Gamal hybrid algorithm and AES algorithm,” International Journal of Advanced Computer Science and Applications, vol. 13, no. 4, pp. 320–326, 2022.
[10]. L. Huang, “A simple chaotic map-based image encryption system,” Entropy, vol. 20, no. 7, pp. 535–548, 2018.
[11]. National Institute of Standards and Technology (NIST), “Advanced Encryption Standard (AES),” Federal Information Processing Standards Publication 197, 2001.
[12]. T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469–472, 1985.
[13]. W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed., Pearson Education, 2017.
[14]. C. Paar and J. Pelzl, Understanding Cryptography, Springer, 2010.

