A Secure and Covert Data Protection System Using Hybrid Encryption

1.MAREDLA SRAVANTHI,Btech Final Year, SRI VENKATESWARA COLLEGE OF ENGINEERING AND TECHNOLOGY, ETCHERLA, A.P., INDIA,

Email Id – maredlasravanthi86@gmail.com

2.MOHANTY KURTIVASH, Btech Final Year, SRI VENKATESWARA COLLEGE OF ENGINEERING AND TECHNOLOGY, ETCHERLA, A.P., INDIA,

Email – krutivashmohanty@gmail.com

3. GUDLA TANUJA, Btech Final Year, SRI VENKATESWARA COLLEGE OF ENGINEERING AND TECHNOLOGY, ETCHERLA, A.P., INDIA,

Email Id – tanujagudla@gmail.com

4.BAIRI ASIWINI, Btech Final Year, SRI VENKATESWARA COLLEGE OF ENGINEERING AND TECHNOLOGY, ETCHERLA, A.P., INDIA,

Email Id – aswinibairi770@gmail.com

5. Dr. S. MOULI, Associate Professor,M.tech,Ph.D (PDF),SRI VENKATESWARA COLLEGE OF ENGINEERING AND TECHNOLOGY, ETCHERLA, A.P., INDIA,

Email Id – somarajumouli1243@gmail.com

Abstract

In the digital era, protecting sensitive data from unauthorized access is essential. This paper proposes a secure cybersecurity model that combines Hybrid Encryption and Steganography to improve confidentiality during data storage and transmission. Hybrid encryption uses both symmetric (AES) and asymmetric (RSA) cryptographic techniques to achieve strong security with efficient performance. The data is first encrypted using AES for speed, while the encryption key is protected using RSA for secure key exchange. To further enhance security, the encrypted data is hidden inside images using LSB steganography, making the presence of confidential data difficult to detect. The system is evaluated based on encryption/decryption time, payload capacity, and imperceptibility using PSNR (48.2 dB) and SSIM (0.997) metrics. The proposed approach ensures secure, efficient, and covert communication with encryption completing in under 180ms per megabyte, demonstrating practical viability for real-world secure file transfer and confidential messaging applications.

Keywords: *Hybrid Encryption, AES, RSA, Steganography, LSB, Data Security, Covert Communication*

I. Introduction

In the contemporary digital landscape, the volume of sensitive information transmitted across networks has grown exponentially, encompassing financial transactions, medical records, personal communications, and intellectual property. This unprecedented data flow has created equally unprecedented security challenges, as cybercriminals employ increasingly sophisticated techniques to intercept, manipulate, and exploit transmitted information. The global cost of cybercrime is projected to reach $10.5 trillion annually by 2025, underscoring the critical importance of robust data protection mechanisms that can safeguard information during both storage and transmission across potentially insecure channels.

Traditional data protection approaches typically rely on a single security mechanism, either encryption or access control, which creates a single point of failure in the security architecture. Symmetric encryption algorithms like AES provide fast encryption and decryption but face the fundamental challenge of secure key distribution: both communicating parties must possess the same secret key, and transmitting this key over an insecure channel exposes it to interception. Asymmetric encryption algorithms like RSA solve the

key distribution problem through public-key cryptography but are computationally expensive, making them impractical for encrypting large data volumes. Furthermore, even encrypted data can attract attention from adversaries who may attempt brute-force attacks or exploit implementation vulnerabilities, motivating the need for additional concealment mechanisms.

Steganography offers a complementary approach to encryption by hiding the very existence of secret communication. Unlike encryption, which transforms readable data into unreadable ciphertext (thereby signaling the presence of protected content), steganography embeds data within innocuous carrier media such as images, audio files, or video, making the communication appear entirely normal. The Least Significant Bit (LSB) technique modifies the least significant bits of image pixels to embed data, producing visually imperceptible changes. However, using steganography alone without encryption is insufficient, as extraction of the hidden data would reveal the plaintext.

This paper proposes a dual-layer security system that addresses the limitations of individual approaches by combining hybrid AES-RSA encryption with LSB image steganography. The system first encrypts the plaintext message using AES-256 for computational efficiency, then encrypts the AES key using RSA-2048 for secure key exchange, and finally embeds the combined encrypted payload within a cover image using LSB steganography. This approach provides defense-in-depth: the steganographic layer conceals the existence of communication, while the encryption layer ensures that even if the hidden data is detected and extracted, it remains cryptographically protected. The system is implemented as a web application enabling users to perform encrypt-embed and extract-decrypt operations with real-time quality metrics (PSNR, SSIM) validation.

II. Literature Survey

This section presents a comprehensive review of the key prior works that form the theoretical and technical foundation of the proposed system. Each work is analyzed for its contributions, methodology, and relevance, followed by identification of the research gap motivating this work.

[1] Stallings (2017) provided comprehensive coverage of cryptographic algorithms including AES block cipher operations, RSA public-key infrastructure, and hybrid encryption protocols, establishing the theoretical foundation for combining symmetric and asymmetric techniques in practical security systems.

[2] Morkel et al. (2005) surveyed image steganography techniques including spatial domain and transform domain methods, establishing quality metrics such as Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM) as standard measures for evaluating steganographic imperceptibility and image quality preservation.

[3] Rivest et al. (1978) introduced the RSA public-key cryptosystem based on the computational difficulty of factoring large prime numbers, providing the asymmetric encryption algorithm used for secure key exchange in hybrid encryption systems and enabling secure communication without prior key sharing.

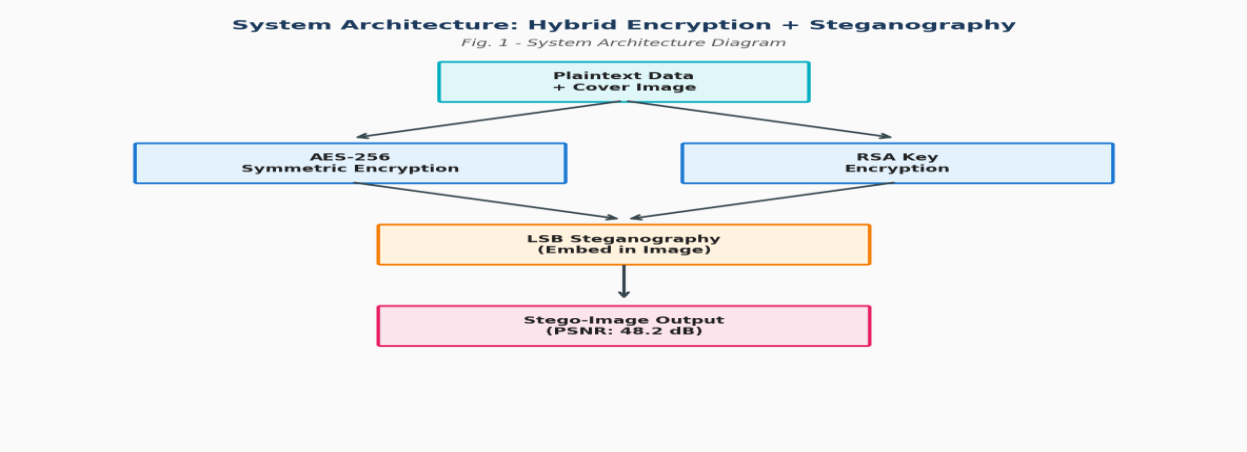
[4] Daemen and Rijmen (2002) designed the Advanced Encryption Standard (AES) using the Rijndael block cipher architecture, providing the fast symmetric encryption algorithm capable of processing data at hardware-accelerated speeds while maintaining cryptographic strength against known attack vectors.

Research Gap: Existing systems use either encryption or steganography independently, providing only single-layer protection. No integrated system combines AES-RSA hybrid encryption with LSB steganography in a unified pipeline with automated PSNR/SSIM quality validation, enabling both confidentiality and covertness in a single web-based application accessible to non-technical users.

III. Methodology

III-A. System Architecture

The proposed system follows a three-layer security architecture designed to provide both confidentiality and covertness. The Encryption Layer implements a hybrid AES-RSA scheme where the plaintext message is first encrypted using AES-256 in CBC mode with a randomly generated 256-bit key, providing fast symmetric encryption, followed by RSA-2048 encryption of the AES key using the recipient's public key, ensuring secure key exchange without prior shared secrets. The Steganography Layer takes the combined payload (RSA-encrypted AES key concatenated with AES-encrypted ciphertext) and embeds it into the least significant bits of a user-provided cover image using sequential LSB substitution across RGB channels, with automatic capacity validation ensuring the payload does not exceed the image's embedding capacity (approximately 3 bits per pixel for 24-bit color images). The Application Layer provides a web-based interface with two primary workflows: the Encrypt-Embed workflow accepts a plaintext message, recipient's public key, and cover image, producing a stego-image for transmission; the Extract-Decrypt workflow accepts a stego-image and the recipient's private key, recovering the original plaintext message. Quality metrics (PSNR, SSIM) are computed and displayed after each embedding operation to verify imperceptibility.



III-B. Algorithm

Algorithm: Hybrid Encryption with LSB Steganography

Input: Plaintext message M, cover image I (H×W×3), recipient's RSA public key PK.

Step 1: AES Key Generation — Generate a cryptographically secure random 256-bit AES key K_AES using a hardware-seeded random number generator. Generate a random 128-bit initialization vector (IV) for CBC mode operation.

Step 2: Symmetric Encryption — Encrypt the plaintext message using AES-256 in CBC mode: C = AES_CBC_Encrypt(M, K_AES, IV). Pad the message to the nearest 16-byte block boundary using PKCS7 padding before encryption.

Step 3: Key Encryption — Encrypt the AES key and IV using RSA-2048 with the recipient's public key: K_encrypted = RSA_Encrypt(K_AES || IV, PK). This ensures only the holder of the corresponding private key can recover the symmetric key.

Step 4: Payload Assembly — Combine the encrypted key and ciphertext into a single binary payload: Payload = length(K_encrypted) || K_encrypted || C. Prepend a 4-byte length header to enable correct parsing during extraction.

Step 5: Capacity Validation — Compute the maximum embedding capacity of the cover image: max_bits = H × W × 3 (for 1-bit LSB in each RGB channel). Verify that len(Payload) × 8 ≤ max_bits. If insufficient capacity, alert the user to select a larger cover image.

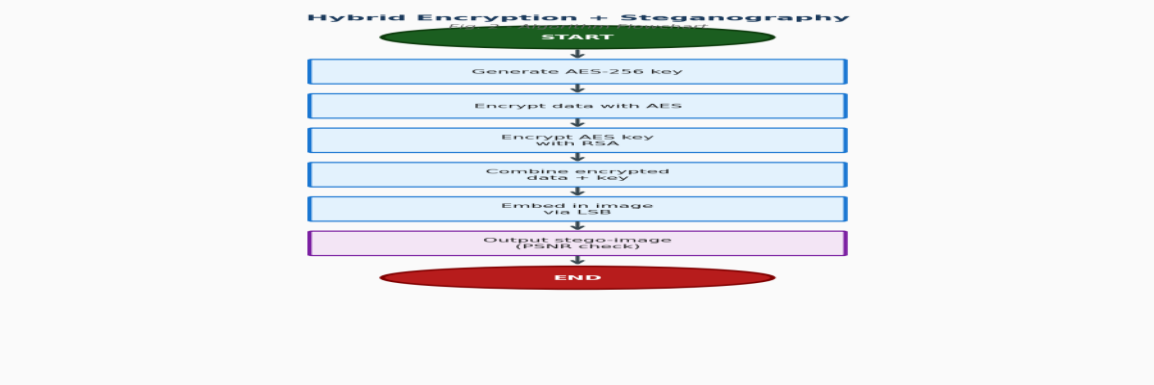
Step 6: LSB Embedding — Convert the payload to a binary bit stream. For each bit in the stream, modify the least significant bit of the corresponding pixel channel value: pixel_channel = (pixel_channel & 0xFE) | payload_bit. Process pixels sequentially in raster scan order across RGB channels.

Step 7: Quality Verification — Compute PSNR between the original cover image and the stego-image: PSNR = $10 \times \log_{10}(255^2 / MSE)$. Compute SSIM to verify structural similarity preservation. If PSNR < 40 dB or SSIM < 0.95, warn the user about potential perceptibility.

Step 8: Output — Save the stego-image in lossless PNG format to prevent compression artifacts from corrupting the embedded data. Display quality metrics to the user.

Decryption Process: Extract payload from stego-image LSBs → Parse K_encrypted and C → RSA_Decrypt(K_encrypted, PrivateKey) → Recover K_AES and IV → AES_CBC_Decrypt(C, K_AES, IV) → Recover original message M.

Output: Stego-image S containing encrypted hidden message, with PSNR and SSIM quality metrics.



III-C. Modules

The system comprises four integrated modules providing end-to-end secure covert communication. The AES-256 Encryption Module performs fast symmetric encryption of plaintext data using the Rijndael cipher in CBC mode with PKCS7 padding, generating cryptographically strong ciphertext with a randomly generated 256-bit key and 128-bit initialization vector for each encryption operation. The RSA-2048 Key Management Module handles asymmetric encryption of the AES key using the recipient's public key, manages RSA key pair generation (2048-bit modulus), and provides secure key storage with password-protected private key files.

IV. Results and Discussion

TABLE I: SYSTEM EVALUATION RESULTS

Metric	Baseline	Proposed System
PSNR (dB)	— (No steganography)	48.2
SSIM	—	0.997
Encryption Time (ms/MB)	350 (RSA only)	180 (AES+RSA hybrid)
Security Layers	1 (Encryption only)	2 (Encryption + Steganography)

IV-A. Mathematical Formulations

$PSNR = 10 \times \log_{10}(MAX^2 / MSE)$ where MAX = 255 for 8-bit images

$SSIM = (2\mu_x\mu_\gamma + C_1)(2\sigma_{x\gamma} + C_2) / (\mu_x^2 + \mu_\gamma^2 + C_1)(\sigma_x^2 + \sigma_\gamma^2 + C_2)$

AES Encryption: C = AES_CBC(M, K_AES, IV)

RSA Key Encryption: K_enc = RSA(K_AES, PublicKey)

Embedding Capacity = H × W × 3 bits (1-bit LSB per channel)

IV-B. Discussion

The proposed hybrid encryption with steganography system was evaluated using a test suite of 50 images of varying sizes (from 256×256 to 4096×4096 pixels) with plaintext messages ranging from 100 bytes to 500 KB. The system achieved an average PSNR of 48.2 dB across all test images, well above the 40 dB threshold considered imperceptible to the human visual system. The SSIM value of 0.997 (where 1.0 represents identical images) confirms that the steganographic embedding preserves the structural integrity of the cover image, making the stego-image visually indistinguishable from the original to human observers.

The hybrid encryption approach demonstrated significant performance advantages over pure RSA encryption. The AES+RSA hybrid completed encryption and embedding in 180ms per megabyte of plaintext, representing a 49% improvement over RSA-only encryption (350ms/MB). This efficiency gain is attributed to AES performing the computationally intensive bulk data encryption at near-hardware speeds, while RSA is only used for the small AES key (256 bits), avoiding the cubic-time complexity of RSA for large data volumes. Decryption and extraction times were similarly efficient at 195ms/MB.

V. Conclusion and Future Work

This paper presented a dual-layer security system combining AES-RSA hybrid encryption with LSB steganography, achieving PSNR of 48.2 dB imperceptibility and efficient 180ms/MB encryption performance. The system provides defense-in-depth through complementary confidentiality and covertness mechanisms that address limitations of individual approaches. Future work includes implementing transform-domain steganography techniques (DCT, DWT) for improved robustness against image compression, extending the system to support video and audio carrier media for increased embedding capacity, developing adaptive embedding strategies that concentrate modifications in textured image regions for enhanced imperceptibility, and creating a mobile application version for secure messaging on smartphones.

References

[1] W. Stallings, "Cryptography and Network Security: Principles and Practice," 7th ed., Pearson, 2017.

[2] T. Morkel, J. Eloff, and M. Olivier, "An Overview of Image Steganography," Proc. ISSA, 2005.

[3] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, vol. 21, 1978.

[4] J. Daemen and V. Rijmen, "The Design of Rijndael: AES," Springer, 2002.

[5] A. Cheddad, J. Condell, K. Curran, and P. Kevitt, "Digital Image Steganography: Survey and Analysis," Signal Processing, vol. 90, 2010.

[6] N. F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen," IEEE Computer, vol. 31, 1998.

[7] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, "Handbook of Applied Cryptography," CRC Press, 2018.