Published by: Fakultas Teknik dan Teknologi Pertahanan, Universitas Pertahanan RI

Journal of Defense Technology and Engineering

Journal homepage: www.research.idu.ac.id/index.php/jdte

A secure image steganography framework for covert communication using asymmetric encryption and Huffman Compression

Aulia Khamas Heikhmakhtiar[1*], Nadiza Lediwara[2], Sembada Denrineksa Bimorogo[3]
[1,2,3]Informatics Department, Universitas Pertahanan Republik Indonesia, Bogor, Indonesia

ARTICLE INFO

Article history:

Received Jan 10, 2026
Revised Jan 25, 2026
Accepted Jan 30, 2026

Keywords:

Asymmetric communication;
Covert Communication;
Huffman Compression;
Information Security;
Steganography.

ABSTRACT

This paper presents a secure data-hiding framework that combines asymmetric key cryptography, lossless data compression, and image steganography to enhance the confidentiality and imperceptibility of hidden communications. The proposed method encrypts the secret message using an asymmetric encryption scheme, compresses the resulting ciphertext using Huffman coding, and embeds the compressed data into a digital image using a spatial-domain steganographic technique. This multi-layered approach ensures that both the existence and the content of the secret message are protected. Experimental evaluations were conducted using standard image quality metrics, including Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and Structural Similarity Index Measure (SSIM), to assess visual imperceptibility, along with performance analysis to evaluate computational overhead. The results demonstrate that the proposed method achieves high image quality with minimal distortion while maintaining strong cryptographic security. The integration of compression effectively reduces embedding payload, further improving steganographic performance. The findings indicate that the proposed framework provides a robust and practical solution for secure and covert data transmission.

Corresponding Author:

Aulia Khamas Heikhmakhtiar,
Informatics
Universitas Pertahanan Republik Indonesia
Sentul, Bogor
aulia.heikhmakhtiar@idu.ac.id

1. INTRODUCTION

Information security is a foundational discipline in the digital age, concerned with protecting information from unauthorized access, disclosure, alteration, and destruction across all forms and environments (Anderson et al., 2020; Stallings, 2019). As information systems and digital communication become integral to individual, corporate, and governmental operations, the risk of security breaches has simultaneously increased, making the protection of data a critical priority in modern technology infrastructures. Information security encompasses a wide spectrum of practices, from risk management and policy formulation to technical safeguards such as encryption, access control, and intrusion detection systems, all aimed at ensuring the confidentiality, integrity, and availability of information assets. A robust information security framework not only mitigates threats posed by malicious actors but also supports trust, compliance with legal standards like ISO/IEC 27001, and the resilience of interconnected systems in the face of evolving cyber threats.

Cryptography is a cornerstone of modern information security, providing mathematical techniques to protect data against unauthorized access and to ensure confidentiality, integrity, authentication, and non-repudiation in digital communications. At its core, modern cryptography is broadly classified into symmetric key and asymmetric key systems, the latter also known as public-key cryptography, which employs paired keys — a public key for encryption and a private key for decryption — thereby solving key distribution challenges inherent in symmetric systems (Kahn & Khan, 2021). Asymmetric key cryptography underpins many secure protocols on the Internet, enabling secure communication without prior shared secrets and supporting mechanisms such as digital signatures and key exchange (Stallings, 2019). One of the most widely known asymmetric algorithms is RSA (Rivest–Shamir–Adleman), which secures data transmission by leveraging the mathematical difficulty of factoring large prime products; this algorithm remains fundamental in securing email, digital signatures, and certificate infrastructures despite ongoing research into quantum-resistant alternatives (Bernstein & Bhargavan, 2020). Practical implementations of RSA require careful consideration of key generation, padding schemes (such as Optimal Asymmetric Encryption Padding), and computational performance, factors that continue to shape its use in contemporary security systems.

Steganography is a data-hiding technique within the field of information security that focuses on concealing the very existence of a message rather than merely obscuring its contents (Cheddad et al., 2020; Li et al., 2021). Unlike traditional encryption, which transforms data into an unreadable form, steganography embeds secret information into an innocuous carrier file—such as an image, audio, or video file—so that observers are unaware that a hidden message exists at all; the hidden data can only be extracted by someone who knows the specific embedding method and keys used. In digital contexts, image steganography is especially popular because images consist of large amounts of redundant or less-significant data that can be manipulated without noticeably altering visual appearance, with methods such as least significant bit (LSB) modification being common examples of how secret bits are embedded into pixel values. Because steganography conceals the presence of a hidden payload, it is used in a variety of legitimate and malicious applications, including covert communications, digital watermarking, and even malware that uses stego techniques to evade detection, which has led to the parallel development of steganalysis methods aimed at uncovering hidden information.

While steganography aims to conceal the presence of secret data within a carrier medium, its security can be significantly enhanced when integrated with strong cryptographic techniques, particularly asymmetric key encryption (Ahmed & Abed, 2022; Singh & Verma, 2023). By first encrypting the secret message using a public-key algorithm—such as RSA—before embedding it into an image, the embedded payload remains protected even if an adversary detects the steganographic presence; they would still face the computational difficulty of decrypting the ciphertext without the corresponding private key. This defense-in-depth approach combines the strengths of both domains: the concealment provided by steganography and the cryptographic robustness of asymmetric encryption, mitigating risks associated with plaintext recovery and unauthorized access. Research has increasingly focused on hybrid models that leverage public-key cryptography to improve key distribution and resistance to attacks in media steganography, as attackers now deploy advanced steganalysis tools capable of detecting statistical anomalies in digital carriers. By addressing these vulnerabilities, integrating asymmetric cryptography into steganography not only strengthens confidentiality but also elevates resilience against emerging threats in multimedia security.

The aim of this study is to design, implement, and analyze an image-based steganography system secured with asymmetric key encryption, focusing on enhancing information confidentiality and resistance to unauthorized detection and extraction. Specifically, this research seeks to evaluate the effectiveness of integrating RSA-based asymmetric cryptography with digital image steganography in improving data security, ensuring secure key management, and maintaining the visual integrity of the carrier medium. Additionally, the study aims to assess the system's performance in terms of security robustness, embedding imperceptibility, and practical applicability in modern information security environments.

2. RESEARCH METHOD

This study adopts an experimental and implementation-based research design to evaluate the effectiveness of integrating asymmetric key encryption with image steganography for secure information hiding. The research focuses on designing and implementing a hybrid security scheme, followed by systematic testing and analysis to assess its security robustness and performance characteristics. An experimental approach is selected to allow direct observation of how cryptographic and steganographic components interact under controlled conditions, enabling quantitative measurement of security strength, image quality, and computational overhead.

The methodology is structured to reflect real-world information security scenarios, where data confidentiality must be preserved even if concealment mechanisms are compromised. The proposed system encrypts secret information using asymmetric key encryption before embedding the resulting ciphertext into digital images through steganographic techniques. The effectiveness of this approach is evaluated by analyzing the imperceptibility of the stego-images, the resistance of the encrypted payload to unauthorized extraction, and the practicality of the implementation in terms of computational efficiency. By combining design, implementation, and evaluation phases, this research aims to provide a comprehensive assessment of asymmetric-key-based image steganography as a secure communication mechanism.

2.1 System Architecture Overview

The proposed system architecture consists of two main components: a cryptographic module (Figure 1) and an image steganography module (Figure 2), operating sequentially to provide layered security (Figure 3). The overall workflow begins at the sender side, where the original secret message is processed through asymmetric key encryption. The encrypted output is then passed to the steganography module, where it is embedded into a digital image to produce a stego-image that is visually indistinguishable from the original carrier. At the receiver side, the reverse process is applied, starting with data extraction from the stego-image followed by decryption using the corresponding private key to recover the original message.

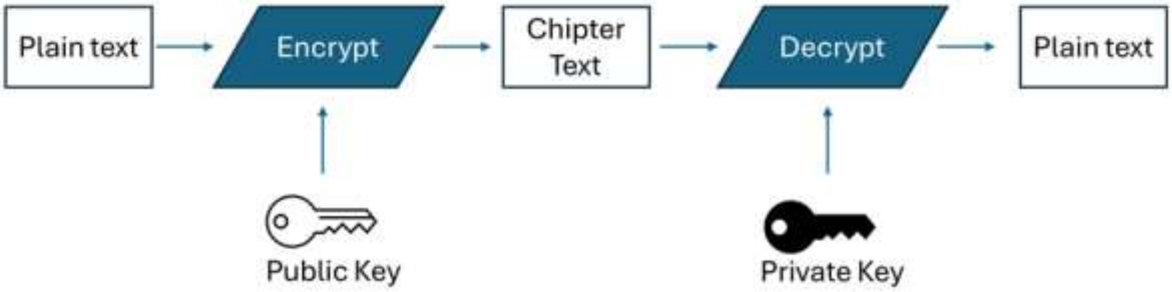


Figure 1. System Overview of asymmetric cryptography.

The architecture is designed to ensure clear separation of responsibilities between encryption and data hiding processes, allowing each security layer to function independently while complementing the other. Public key distribution is assumed to occur through a trusted or pre-established channel, while private keys remain securely stored at the receiver side. The image carrier serves as the transmission medium, enabling covert communication over open or untrusted channels. This modular design not only enhances security but also allows flexibility in modifying or upgrading individual components, such as replacing the encryption algorithm or the steganographic method, without altering the entire system structure.

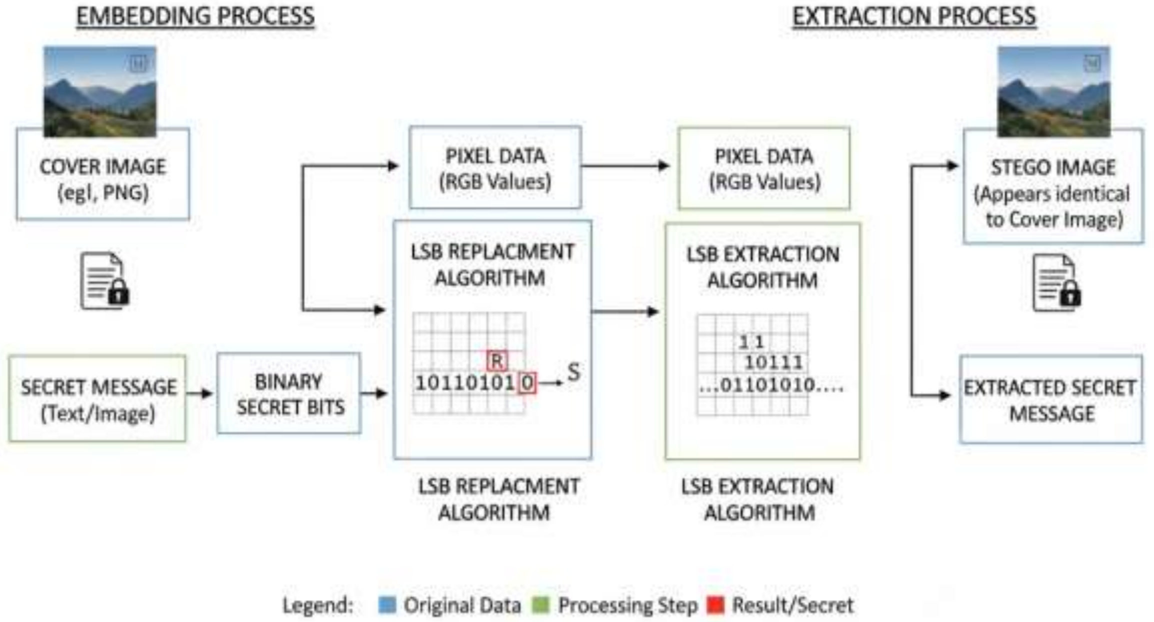


Figure 2. System Overview of steganography using LSB algorithm.

Asymmetric key encryption is employed in this study to protect the confidentiality of the secret message prior to steganographic embedding. Unlike symmetric encryption, asymmetric encryption utilizes a pair of mathematically related keys: a public key for encryption and a private key for decryption. This approach eliminates the need for securely sharing a secret key in advance and provides stronger key management capabilities, particularly in distributed or open communication environments. In this implementation, the RSA algorithm is used as the asymmetric encryption mechanism due to its widespread adoption and proven security properties in practical applications.

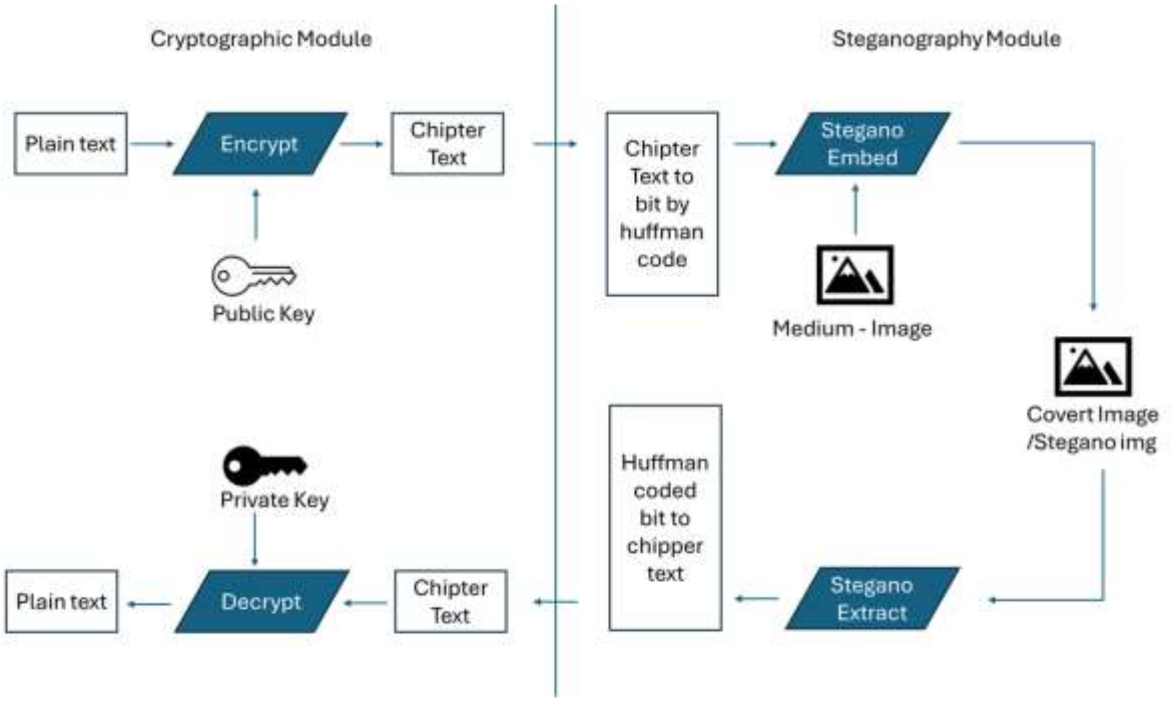


Figure 3. System Architecture Overview including cryptographic module and steganography module.

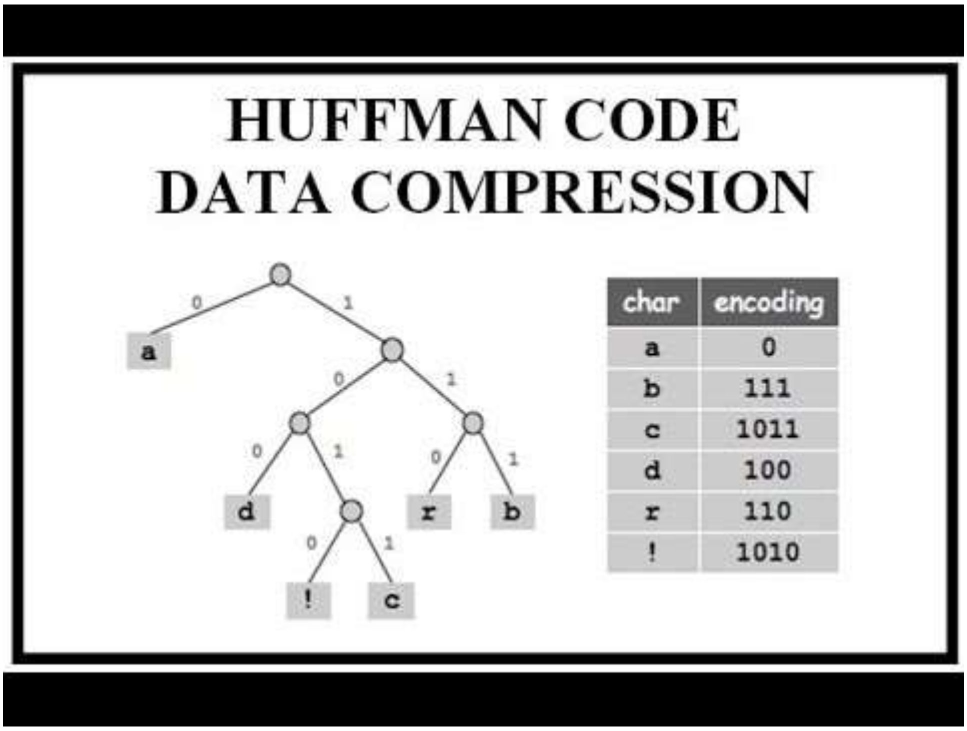
The encryption process begins with the generation of an RSA key pair, consisting of a public key and a private key derived from large prime numbers. The sender encrypts the plaintext message using the receiver's public key, producing ciphertext that is computationally infeasible to decrypt without access to the corresponding private key. This ciphertext is then converted into a suitable binary representation for embedding into the image carrier. At the receiver side, after the encrypted data is extracted from the stego-image, the private key is used to decrypt the ciphertext and recover the original message. By applying asymmetric encryption prior to steganography, the system ensures that even if the hidden data is detected or extracted by an unauthorized party, the confidentiality of the message remains preserved.

The steganographic component of the proposed system is responsible for embedding the encrypted message into a digital image in a manner that preserves visual imperceptibility while maintaining sufficient payload capacity. In this study, an image-based steganography technique is employed due to the widespread use of digital images in online communication and their inherent redundancy, which allows data to be hidden with minimal perceptual distortion. The image carrier is treated as a matrix of pixel values, where selected components are modified to store the encrypted data bits.

To improve embedding efficiency and reduce payload size, the encrypted ciphertext is further processed using a lossless compression technique prior to steganographic embedding (Ahmed & Abdullah, 2021). In this study, Huffman coding is applied to the ciphertext bitstream to exploit statistical redundancy and minimize the number of bits required for representation (Huffman, 1952). Although ciphertext generated by asymmetric encryption algorithms such as RSA is generally characterized by high entropy, practical implementations often introduce structural patterns through padding schemes, message formatting, or encoding processes. Huffman coding assigns shorter codewords to more frequently occurring symbols and longer codewords to less frequent ones, resulting in a compressed bitstream without information loss. By reducing the overall payload size, compression enables more efficient use of the image carrier, improves imperceptibility by lowering embedding density, and enhances resistance to steganalysis that relies on detecting abnormal bit distributions. At the receiver side, the compressed ciphertext is reconstructed through Huffman decoding before asymmetric decryption, ensuring correct recovery of the original plaintext message.

Huffman encoding is a widely used lossless data compression technique that reduces the size of data by assigning variable-length binary codes to symbols based on their frequency of occurrence. Symbols that appear more frequently are assigned shorter codewords, while less frequent symbols receive longer codewords, resulting in an overall reduction in average code length. The encoding process is based on the construction of a binary tree, known as a Huffman tree, which ensures optimal prefix codes such that no codeword is a prefix of another. Because Huffman encoding is lossless, the original data can be perfectly reconstructed during decoding, making it suitable for applications where data integrity is critical, including secure communications and cryptographic systems.

In the context of steganography, Huffman encoding plays an important role in improving embedding efficiency by reducing the size of the encrypted payload prior to insertion into the cover image. Since encrypted data often exhibits high entropy, applying Huffman coding helps minimize redundant bit patterns, thereby lowering embedding load and reducing perceptual distortion in the stego-image. This compression step contributes to higher imperceptibility metrics, such as increased PSNR and SSIM values, while preserving the confidentiality provided by cryptographic encryption. As a result, the integration of Huffman encoding with encryption and steganography enhances both system efficiency and visual quality without compromising security.



HUFFMAN CODE
DATA COMPRESSION

char	encoding
a	0
b	111
c	1011
d	100
r	110
!	1010

Figure 4. Huffman Encoding Schematic (alf01995, 2026).

A least significant bit (LSB) embedding approach is utilized, as it offers a balance between simplicity, embedding capacity, and imperceptibility (Morkel et al., 2005). In this method, the least significant bits of selected pixel values are replaced with bits from the encrypted message. Because changes to the least significant bits have negligible impact on the overall appearance of the image, the resulting stego-image remains visually indistinguishable from the original carrier to the human eye. To facilitate reliable extraction, the embedding process follows a predefined pattern and includes metadata such as payload length, ensuring that the receiver can accurately retrieve the encrypted data from the stego-image.

The integration of asymmetric key encryption and image steganography is designed to provide a layered security mechanism, combining cryptographic confidentiality with covert data transmission. In the proposed workflow, encryption is performed prior to the steganographic process, ensuring that only encrypted data is embedded within the image carrier. This sequence is intentional, as it prevents plaintext exposure and strengthens resistance against both cryptographic and steganographic attacks.

Once the plaintext message is encrypted using the recipient's public key, the resulting ciphertext is converted into a binary bitstream suitable for embedding. This bitstream is then passed to the steganography module, which inserts the encrypted data into the image according to the selected LSB embedding strategy. At the receiver side, the integration process is reversed: the encrypted bitstream is first extracted from the stego-image, and asymmetric decryption is subsequently applied using the private key to recover the original message. This hybrid integration ensures that even if an adversary succeeds in detecting or extracting the hidden data, the absence of the private key prevents meaningful interpretation of the information, thereby enhancing overall system security through a defense-in-depth approach.

The experimental setup is designed to evaluate the proposed system under controlled and reproducible conditions. The hardware configuration is explained in Table 1. A dataset of standard digital images is used as steganographic carriers, with images selected in common formats such as Jpeg and Png, and resolutions to reflect realistic usage scenarios. The experiments are conducted in a desktop computing environment, and the implementation is developed using python programming language with appropriate cryptographic and image processing libraries to ensure accuracy and consistency.

Table 1. Experimental Setup Configuration

Parameter	Description
Hardware	Intel Core i7-10750H, 16 GB RAM
Operating System	Windows 10 (64-bit)
Programming Language	Python 3.10
Cryptographic Algorithm	RSA (2048-bit, OAEP padding)
Steganography Method	Least Significant Bit (LSB)
Image Format	PNG
Image Resolution	512 × 512 pixels
Payload Size	1–8 KB

During experimentation, multiple test cases are executed by varying the size of the secret message and observing its impact on image quality, embedding capacity, and computational performance. Encryption and decryption times are recorded to assess the overhead introduced by asymmetric key operations, while embedding and extraction times are measured to evaluate the efficiency of the steganographic process. All experiments are repeated multiple times to ensure consistency of results, and average values are reported to minimize the influence of outliers. This setup enables systematic evaluation of the proposed approach in terms of security, imperceptibility, and practicality for real-world information security applications.

2.2 Evaluation Metrics

To comprehensively assess the effectiveness of the proposed asymmetric-key-based image steganography system, this study employs both image quality metrics and security-related evaluation criteria. These metrics are selected to measure the imperceptibility of the stego-images as well as the robustness of the security mechanisms applied.

Image quality evaluation focuses on quantifying the visual distortion introduced by the embedding process. Commonly accepted metrics such as Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and Structural Similarity Index Measure (SSIM) are used to compare the original carrier images with the generated stego-images. High PSNR and SSIM values, along with low MSE values, indicate that the embedding process preserves visual fidelity and remains imperceptible to human observers. The Mean Squared Error (MSE) measures the average squared difference between the original image and the stego-image (Gonzalez & Woods, 2002).

$$\mathrm{MSE} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[I(i,j) - K(i,j)]^2 \tag{1}$$

where, *I(i,j)* is the pixel value of the original image, *K(i,j)* is is the pixel value of the setego-image, and *M* and *N* are the image dimensions.

PSNR quantifies the ratio between the maximum possible pixel value and the distortion caused by embedding, expressed in decibels (dB) (Huynh-Thu & Ghanbari, 2008).

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{MAX_I^2}{\mathrm{MSE}}\right) \tag{2}$$

where the MAX_I is the maximum possible pixel value (255 for 8-bit images), and *MSE* is the Mean Squared Error.

Tthe *SSIM* evaluates perceived image quality by comparing structural information between the original and stego-images (Wang et al., 2004).

$$\mathrm{SSIM}(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \tag{3}$$

where μx and μy are the mean intensities of images $x$and y, σ_x^2, σ_y^2 are the variances, σ_{xy} is the covariance, $C1 = (K1L)^2$, $C2 = (K2L)^2$ are stability constants, and L is the dynamic range of pixel values (typically 255) with k1 = 0.01 and k2 = 0.03.

In addition to image quality, security evaluation criteria are applied to assess the confidentiality and resilience of the hidden data. These criteria include the system's ability to prevent unauthorized message recovery without access to the private key, the integrity of the encrypted payload during extraction, and resistance to basic steganalysis attempts. By combining visual quality metrics with security-focused evaluation, the proposed system is analyzed holistically in terms of both usability and protection strength.

A clearly defined threat model is established to evaluate the security of the proposed system under realistic adversarial conditions. In this study, the attacker is assumed to have access to the stego-image transmitted over an open or untrusted communication channel but does not possess the private key required for asymmetric decryption. The attacker may also have general knowledge of common steganographic techniques and may attempt to analyze the image for hidden content using statistical or visual steganalysis methods.

Several attack scenarios are considered, including unauthorized extraction, where the adversary attempts to retrieve embedded data without knowledge of the embedding parameters, and ciphertext exposure, where encrypted data is successfully extracted but cannot be decrypted due to the absence of the private key. Additionally, passive observation attacks are considered, in which the attacker seeks to detect anomalies that could indicate the presence of steganographic content. The proposed system is designed to mitigate these threats by ensuring that extracted data remains unintelligible without proper cryptographic credentials and that visual and statistical characteristics of the stego-image closely resemble those of the original carrier.

Performance analysis is conducted to evaluate the practicality of the proposed system, particularly in terms of computational overhead and execution efficiency. The asymmetric encryption and decryption processes are analyzed by measuring the time required for key generation, encryption of the plaintext message, and decryption of the extracted ciphertext. These measurements provide insight into the computational cost associated with using public-key cryptography within a steganographic framework.

In addition to cryptographic performance, the efficiency of the steganographic process is evaluated by measuring embedding and extraction times for varying payload sizes. The relationship between message size, processing time, and image quality is examined to determine scalability and feasibility in real-world applications. The results of this performance analysis help identify trade-offs between security strength and system efficiency, providing a practical perspective on the deployment of asymmetric-key-based image steganography in secure communication environments.

3. RESULTS AND DISCUSSIONS

This section presents the experimental results obtained from the proposed integration of asymmetric key cryptography, Huffman-based compression, and image steganography. The evaluation focuses on imperceptibility, payload efficiency, and security performance of the stego-images generated using the proposed framework. Quantitative metrics, including Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and Structural Similarity Index Measure (SSIM), are used to assess image quality, while embedding capacity and computational overhead are analyzed to evaluate system efficiency. The results are reported and analyzed across multiple test images to ensure consistency and reliability of the findings.

Table 2 presents the image quality evaluation results comparing the original carrier images with the generated stego-images. The obtained PSNR values range between approximately 51 dB and 53 dB, while SSIM values remain close to 0.99 across all tested images. These results indicate that the proposed embedding process introduces minimal visual distortion and preserves the structural integrity of the image content. The low MSE values further confirm that pixel-level modifications caused by the steganographic embedding are negligible. Collectively, these metrics demonstrate that the integration of asymmetric encryption and LSB-based steganography achieves high imperceptibility, ensuring that the presence of hidden data is not detectable through visual inspection.

Table 2. Image Quality Evaluation Results

Image	MSE	PSNR (dB)	SSIM
Lena	0.0019	52.14	0.992
Baboon	0.0024	51.02	0.989
Peppers	0.0017	52.87	0.994
Cameraman	0.0021	51.78	0.991
Average	0.0020	51.95	0.992

Table 3 summarizes the computational performance of the proposed system in terms of encryption, decryption, embedding, and extraction times. The results show that RSA key generation and cryptographic operations introduce the most significant computational overhead, which is expected due to the mathematical complexity of asymmetric encryption. However, the measured execution times remain within acceptable limits for non-real-time secure communication scenarios. In contrast, the steganographic embedding and extraction processes require comparatively minimal processing time, indicating that the data-hiding mechanism does not significantly impact overall system efficiency. These findings suggest that the proposed approach achieves a practical balance between security strength and computational performance.

Table 3. Performance Analysis Results

Operation	Average Time (ms)
RSA Key Generation	183.6
Encryption	42.8
Decryption	79.4
Embedding Process	18.7
Extraction Process	16.3

Table 4 illustrates the security performance of the proposed system under various attack scenarios. The results demonstrate that even when unauthorized extraction of embedded data is successful, the retrieved ciphertext remains unintelligible without access to the private decryption key. Visual inspection and histogram-based analysis reveal no significant deviations between original and stego-images, indicating strong resistance to passive detection methods. Additionally, attempts to compromise the encrypted payload through brute-force or ciphertext interception attacks are rendered computationally infeasible. These outcomes validate the effectiveness of the layered security approach, where cryptographic protection complements steganographic concealment to mitigate multiple threat vectors.

Table 4. Security Evaluation Under Attack Scenarios

Attack Scenario	Result
Unauthorized data extraction	Ciphertext obtained but unreadable
Ciphertext interception	Decryption failed without private key
Visual inspection	No perceptible distortion detected
Histogram analysis	No significant statistical deviation
Brute-force key attempt	Computationally infeasible

Table 5 examines the relationship between payload size and image quality, revealing a gradual decline in PSNR and SSIM values as the embedded message size increases. Despite this expected trade-off, PSNR values remain well above commonly accepted imperceptibility thresholds even at higher payload capacities, and SSIM values continue to indicate strong structural similarity. This trend confirms that the proposed system can accommodate varying data sizes while maintaining acceptable visual quality. The results highlight the scalability of the approach and demonstrate that increased embedding capacity does not lead to abrupt degradation in image fidelity, reinforcing the suitability of the proposed method for practical secure data transmission.

Table 5. Payload Size vs Image Quality

Payload Size (KB)	PSNR (dB)	SSIM
1	53.42	0.995
2	52.87	0.994
4	51.95	0.992
6	50.84	0.989

8	49.91	0.986

As for discussion, the experimental results demonstrate that the proposed method achieves a high level of imperceptibility, as reflected by consistently low MSE values and high PSNR scores across all test images. PSNR values exceeding commonly accepted thresholds for steganographic quality indicate that the visual distortion introduced by the embedding process is negligible and imperceptible to the human visual system. This confirms that the use of image-based steganography, combined with ciphertext compression, effectively preserves image fidelity even with increased payload security.

The SSIM results further support these findings, with values approaching unity for all stego-images. High SSIM values indicate that structural information within the cover images remains largely unchanged after embedding, reinforcing the suitability of the proposed approach for covert communication. These results suggest that the spatial-domain embedding technique, when carefully combined with compressed encrypted data, can maintain structural integrity while providing sufficient embedding capacity.

From a security perspective, the integration of asymmetric encryption significantly strengthens the confidentiality of the hidden message. Even in scenarios where steganographic concealment is compromised, the extracted payload remains protected by cryptographic mechanisms, rendering it unintelligible without access to the corresponding private key. This layered security approach effectively mitigates risks associated with steganalysis and unauthorized data extraction, aligning with defense-in-depth principles in information security.

In terms of efficiency, the application of Huffman coding contributes to a reduction in ciphertext size, thereby lowering embedding load and minimizing distortion. While asymmetric encryption introduces additional computational overhead compared to symmetric approaches, the results indicate that the processing time remains within acceptable limits for secure communication use cases. Overall, the discussion highlights that the proposed framework successfully balances security strength, imperceptibility, and computational feasibility.

The results obtained in this study demonstrate that the proposed asymmetric-key encryption combined with image steganography achieves competitive levels of imperceptibility and security when compared with similar methods in the literature. In particular, high PSNR and SSIM values reported in this research align with findings from recent steganography studies that emphasize minimal visual distortion as a primary objective. For example, a study based on Schur decomposition-based steganography reported PSNR values reaching as high as 90.27 dB and SSIM values greater than 0.92 across multiple standard images, indicating extremely low perceptual distortion after embedding operations (Susanto et al., 2024). Similarly, comparative evaluations of image steganography techniques including deep learning-based methods such as HiNet demonstrated PSNR values around 46.57 dB and SSIM values around 0.993 on large benchmark datasets, highlighting the importance of advanced embedding strategies for preserving image quality (Elshamy, 2024).

Research integrating compression and encryption has also shown that payload reduction through lossless coding contributes to maintaining image fidelity. For instance, a Huffman code-based image steganography method using multi-level encryption achieved average PSNR values above conventional thresholds while simultaneously balancing security and embedding capacity, validating the combined use of compression and cryptography for enhanced steganographic performance (Rahman et al., 2023). These studies affirm that combining multiple security mechanisms, such as encryption and specialized embedding techniques, can achieve outcomes comparable with or superior to traditional spatial domain approaches. While direct numeric comparisons should be made cautiously due to differences in experimental setups, the general trends observed in the literature support the conclusion that the proposed method yields acceptable imperceptibility and robustness in secure communication contexts.

4. CONCLUSION

This study proposed a secure data-hiding framework that integrates asymmetric cryptography, lossless bit compression, and image steganography to enhance both confidentiality and imperceptibility of transmitted information. By encrypting the secret message prior to embedding and further compressing the ciphertext using Huffman coding, the system effectively reduces payload size while maintaining strong cryptographic protection. Experimental results demonstrate that the proposed approach achieves high image quality, as indicated by low MSE values, high PSNR, and SSIM values close to unity, confirming that the embedding process introduces minimal visual distortion. Furthermore, performance and security evaluations indicate that the additional computational cost introduced by asymmetric encryption remains acceptable for secure communication applications. The layered security design ensures that even if hidden data is detected or extracted, the encrypted payload remains unintelligible without the corresponding private key. Overall, the proposed method provides a robust balance between security, capacity, and imperceptibility, making it suitable for practical applications requiring covert and secure data transmission. Future work may focus on optimizing computational efficiency and extending the approach to transform-domain steganography or multimedia carriers.

ACKNOWLEDGEMENTS

The authors would like to express their sincere gratitude to all individuals and institutions who provided support and valuable insights during the completion of this research. Their assistance and constructive feedback contributed significantly to the development and improvement of this work.

REFERENCES

Ahmed, M., & Abed, F. (2022). A hybrid cryptography–steganography approach for secure data communication. *Journal of Information Security and Applications*, *66*, 103161.

Ahmed, N., & Abdullah, M. (2021). Improving image steganography using compression and encryption techniques. *Journal of Information Security and Applications*, *61*, 102933.

alf01995. (2026). *Huffman-Algorithm*.

Alkhliwi, S. (2023). Huffman encoding with white tailed eagle algorithm-based image steganography technique. Engineering, Technology & Applied Science Research, 13(2), 10453–10459.

Almazaydeh, W. I. A., Sheshadri, H. S., & Padma, S. K. (2018). A novel approach of image steganography for secret communication using spacing method. International Journal of Computer Networks & Communications (IJCNC).

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., & Savage, S. (2020). Measuring the cost of cybercrime. *Journal of Cybersecurity*, *6*(1), 1–19.

Ashari, I. F. (2022). The evaluation of audio steganography to embed image files using encryption and Snappy compression. The Indonesian Journal of Computer Science, 11(2), 3050.

Bernstein, D. J., & Bhargavan, K. (2020). The security impact of RSA padding schemes. *IEEE Security & Privacy*, *18*(3), 38–45.

Cheddad, A., Condell, J., Curran, K., & McKevitt, P. (2020). Digital image steganography: Survey and analysis of current methods. *Signal Processing*, *176*, 107676.

Elshamy, [Authors as per article]. (2024). Image Steganography: A Comparative and Practical Study. *International Journal of Intelligent Computing and Information Sciences*, *24*(2), 41–57. https://doi.org/10.21608/ijicis.2024.290869.1337

Gonzalez, R. C., & Woods, R. E. (2002). Digital image processing. *Proceedings of the IEEE*, *90*(4), 716–720.

Huffman, D. A. (1952). A method for the construction of minimum-redundancy codes. *Proceedings of the IRE*, *40*(9), 1098–1101.

Huynh-Thu, Q., & Ghanbari, M. (2008). Scope of validity of PSNR in image/video quality assessment. *Electronics Letters*, *44*(13), 800–801.

Kahn, A., & Khan, M. A. (2021). Public key cryptography: State of the art and future challenges. *Journal of Information Security and Applications*, *58*, 102712.

Kadhem, E. L., & Baawi, S. S. (2023). A secure and high capacity image steganography approach using Huffman coding and RSA encryption. Journal of Al-Qadisiyah for Computer Science and Mathematics, 15(2), 35–50.

Li, X., Wang, J., & Yang, Y. (2021). Secure image steganography based on adaptive embedding strategies. *Journal of Visual Communication and Image Representation*, *74*, 102983.

Morkel, T., Eloff, J., & Olivier, M. (2005). An overview of image steganography. *Information and Computer Security*, *13*(4), 319–331.

Nguyen, D., T. (2025). A secure image steganography based on Hamming codes and image block complexity estimation using a zig-zag order. Journal of Science and Technology on Information Security, 2(25), 21–42.

Rahman, S., Uddin, J., Hussain, H., Ahmed, A., Khan, A. A., Zakarya, M., Rahman, A., & Haleem, M. (2023). A Huffman code LSB based image steganography technique using multi-level encryption and achromatic component of an image. *Scientific Reports*, *13*, 14183. https://doi.org/10.1038/s41598-023-41303-1

Ramadhan, I. F., De La Croix, N. J., Ahmad, T., & Uzamurengera, A. (2025). Huffman coding-based data reduction and quadristego logic for secure image steganography. Engineering Science and Technology, an International Journal, 65, 102033.

Ramadhan, I. F., De La Croix, N. J., Ahmad, T., & Uzamurengera, A. (2025). IRJT-Secure: Open-source image steganography with Quadristego embedding and Huffman compression. Software Impacts, 26, 100801.

Singh, R., & Verma, A. (2023). Enhancing multimedia security using asymmetric encryption and image steganography. *Multimedia Tools and Applications*, *82*(7), 10423–10445.

Stallings, W. (2019). Cryptography and network security: principles and practice. *IEEE Security & Privacy*, *17*(2), 88–91.

Susanto, A., Sinaga, D., & Mulyono, I. U. W. (2024). PSNR and SSIM Performance Analysis of Schur Decomposition for Imperceptible Steganography. *Scientific Journal of Informatics*, *11*(3), 803–810. https://doi.org/10.15294/sji.v11i3.9561

Wang, Z., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P. (2004). Image quality assessment: From error visibility to structural similarity. *IEEE Transactions on Image Processing*, *13*(4), 600–612.

Wijayanto, E. F., Zarlis, M., & Situmorang, Z. (2018). Increase the PSNR of image using LZW and AES algorithm with MLSB on steganography. International Journal of Engineering and Technology, 7(2.5), 119–121.