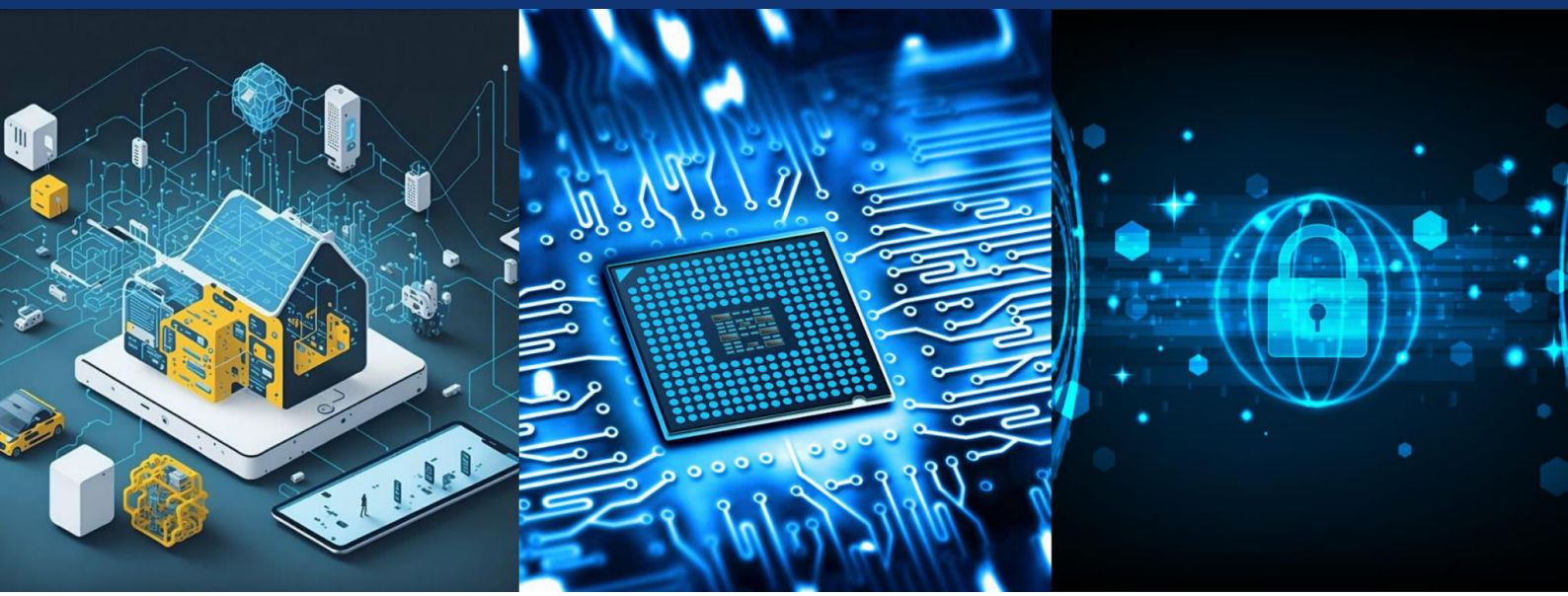
IJIRCCE

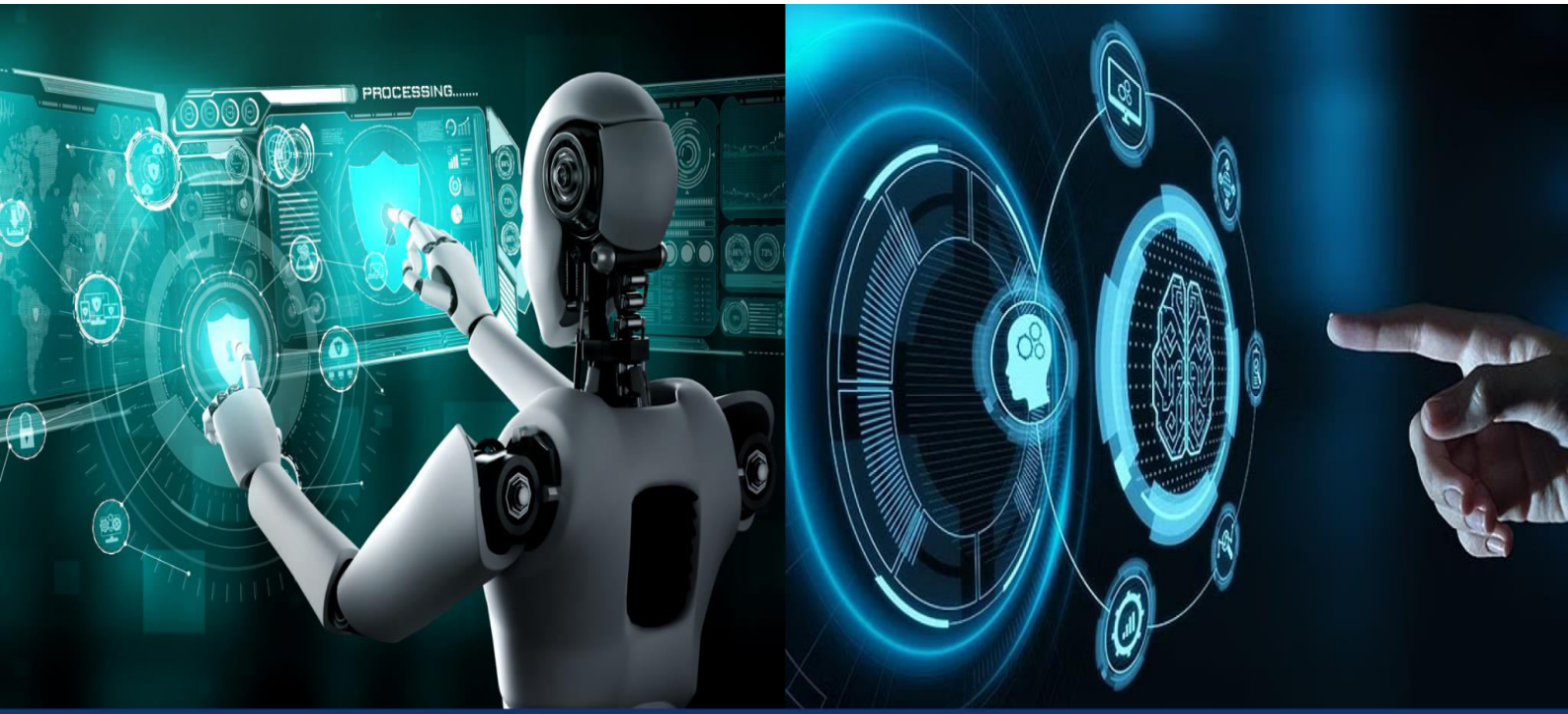
ISSN(O): 2320-9801

ISSN(P): 2320-9798



# International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)




**Impact Factor: 8.771**

**Volume 14, Issue 4, April 2026**

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404049

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

# Secure Data Transfer across Internet Using Image Steganography

**Mr. Prince Wesley C, Mr. Mohamed Ashik Jamal N, Mr. Jayaesh Gautam SK., Mrs. M. Sharon Nisha**

Department of Computer Science and Engineering, Francis Xavier Engineering College,

Tirunelveli, Tamil Nadu, India

**ABSTRACT:** The exponential growth of internet communication has intensified the need for robust methods of secure data transmission. This project presents an image steganography-based system for concealing sensitive information within digital images, enabling covert data transfer across the internet without arousing suspicion. The proposed system employs the Least Significant Bit (LSB) technique to embed textual or binary data into carrier images, ensuring minimal perceptual distortion while preserving payload integrity. An optional layer of AES encryption is applied to the secret data before embedding, providing a dual-layered security mechanism against unauthorized access and interception. The system is implemented as a web-based application that allows users to encode and decode hidden messages through an intuitive interface. Experimental evaluations demonstrate that the system achieves high embedding capacity, imperceptibility, and robustness, with PSNR values consistently exceeding acceptable thresholds. The results confirm the effectiveness of combining cryptography and steganography for secure internet-based data communication.

**KEYWORDS:** Image Steganography, Least Significant Bit (LSB), Secure Data Transfer, AES Encryption, Covert Communication, Information Hiding, PSNR, Steganalysis, Cybersecurity, Digital Image Processing.

## I. INTRODUCTION:

The rapid proliferation of digital communication platforms has created an urgent demand for advanced data security mechanisms that go beyond conventional encryption. While encryption techniques scramble data into unreadable formats, they often draw attention to the existence of sensitive communications, potentially inviting interception and analysis. Steganography, the art and science of hiding information within ordinary digital media, offers a complementary approach by concealing the very existence of a secret message. When applied to digital images, steganography leverages the inherent redundancy in image data to embed confidential payloads without producing visually perceptible changes to the cover medium.

Image steganography has emerged as a powerful tool for secure data transfer across the internet, finding applications in digital watermarking, covert military communications, intellectual property protection, and privacy-preserving messaging systems. The fundamental challenge in designing a steganographic system lies in balancing three competing objectives: high embedding capacity, imperceptibility to human observers, and robustness against steganalytic attacks. Traditional spatial domain methods such as Least Significant Bit substitution offer simplicity and high capacity but may be vulnerable to statistical detection. Frequency domain techniques, including Discrete Cosine Transform and Discrete Wavelet Transform-based approaches, provide improved robustness at the cost of increased computational complexity.

This project proposes an integrated steganographic framework that combines LSB-based image steganography with AES symmetric encryption to deliver a dual-layered security solution suitable for practical internet-based data transfer. The system is deployed as an interactive web application, enabling users to securely embed and retrieve confidential messages within digital images. By integrating cryptographic preprocessing with spatial domain steganography, the proposed system ensures that even if a stego-image is detected, the embedded payload remains inaccessible without the correct decryption key. This work addresses the growing need for transparent, user-friendly, and mathematically sound information hiding solutions in an era of pervasive digital surveillance and cyber threats.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

## II. LITERATURE SURVEY

**Classical Steganographic Techniques and Their Limitations:**

Early steganographic methods were rooted in simple spatial domain manipulations, most notably the Least Significant Bit substitution algorithm, which replaces the lowest-order bits of pixel intensity values with bits of the secret message. Studies on classical LSB-based systems demonstrated that while the technique offers straightforward implementation and high payload capacity, it remains susceptible to histogram-based steganalysis, chi-square attacks, and RS analysis. Researchers identified that naive LSB substitution introduces detectable statistical anomalies in the pixel value distribution of stego-images, necessitating the development of more sophisticated embedding strategies that minimize statistical artifacts.

**Frequency Domain Approaches to Steganography:**

Subsequent research shifted focus toward frequency domain steganographic methods that exploit transform coefficients rather than raw pixel values. Techniques based on the Discrete Cosine Transform embed secret bits into mid-frequency DCT coefficients of JPEG images, providing inherent robustness against JPEG compression and common image processing operations. Wavelet-based steganographic algorithms further improved imperceptibility by operating across multiple resolution scales, enabling adaptive embedding that concentrates payload in texture-rich regions while preserving smooth areas. These approaches demonstrated superior resistance to visual detection and many steganalytic tools, though at the expense of embedding capacity and computational overhead.

**Hybrid Cryptography and Steganography Systems:**

A significant body of literature has investigated the integration of cryptographic algorithms with steganographic techniques to create multi-layered security architectures. Research demonstrates that encrypting secret data with symmetric algorithms such as AES or asymmetric schemes such as RSA before embedding substantially increases the difficulty of unauthorized extraction, even when the steganographic layer is compromised. Studies comparing hybrid systems against purely steganographic approaches confirm that combining encryption with information hiding yields statistically indistinguishable stego-images while providing cryptographic strength, making such systems highly suitable for high-security communication applications.

**Positioning of the Present Work:**

The current project builds upon the established foundations of spatial domain steganography and symmetric cryptography to develop a practical, accessible, and secure image-based data transfer system. Unlike highly specialized deep learning approaches that require substantial computational resources, the proposed system employs computationally efficient LSB embedding combined with AES-256 encryption to achieve strong security with minimal processing overhead. The web-based deployment model ensures broad accessibility, enabling users across diverse technical backgrounds to leverage advanced information hiding capabilities for secure internet communication. This work bridges the gap between theoretical steganographic research and real-world secure data transfer requirements.

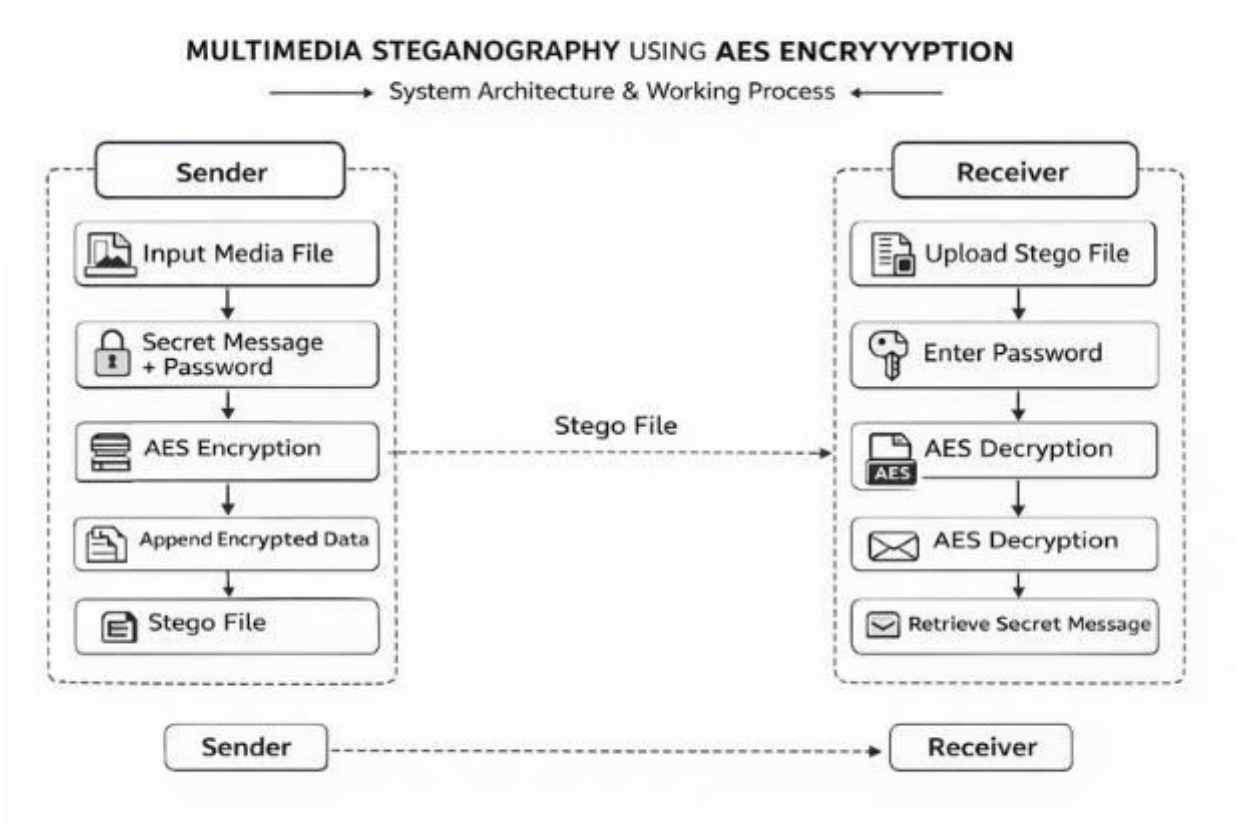
© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404049

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

**Flow Chart:**




## III. PROPOSED METHODOLOGY

This project proposes a web-based Secure Data Transfer System using Image Steganography, designed to embed and extract secret information within digital images through a combination of LSB steganography and AES encryption. The methodology is organized into the following systematic stages:

**System Architecture Design:**
A layered architecture is adopted comprising a frontend user interface, a backend processing server, a steganography engine, and an encryption module. The components interact through well-defined APIs, ensuring modularity, maintainability, and ease of future enhancement. The architecture supports both the encoding pipeline, which embeds secret data into carrier images, and the decoding pipeline, which extracts and decrypts hidden messages from received stego-images.

**Secret Data Preprocessing and Encryption Module:**
Prior to embedding, the secret message undergoes AES-256 encryption using a user-supplied key. The plaintext message is padded to a block-aligned length, encrypted to produce a ciphertext byte stream, and encoded in Base64 format for binary-safe transmission. This preprocessing step ensures that even if the steganographic layer is successfully attacked, the extracted data remains cryptographically protected against unauthorized decryption.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

**Cover Image Selection and Validation:**
Users upload a cover image through the web interface, which validates the image format, dimensions, and color depth. The system preferentially supports 24-bit RGB PNG images to avoid lossy compression artifacts that would corrupt the embedded payload. A capacity analysis is performed to confirm that the selected cover image can accommodate the encrypted message payload without exceeding the safe embedding limit, defined as utilizing no more than 25% of the available LSB capacity to maintain imperceptibility.

**LSB-Based Steganographic Embedding:**
The core embedding process employs the Least Significant Bit substitution technique. The encrypted payload is converted into a binary bit stream and sequentially substituted into the least significant bits of the red, green, and blue channels of the cover image pixels in a raster scan order. A delimiter sequence is appended to the payload to demarcate the end of the hidden message, enabling precise extraction during the decoding phase. The embedding process introduces imperceptible modifications to pixel values, with changes limited to ±1 per channel per pixel.

**Stego-Image Generation and Transmission:**
Following embedding, the modified pixel array is compiled into a losslessly compressed PNG stego-image, preserving all embedded bits without degradation. The stego-image is made available for download and subsequent internet-based transmission. The visual similarity between the original cover image and the generated stego-image is quantitatively assessed using the Peak Signal-to-Noise Ratio metric, with target PSNR values exceeding 40 dB to ensure acceptable imperceptibility.

**Steganographic Extraction and Decryption:**
The decoding module accepts a received stego-image and the decryption key as inputs. The system extracts the LSB stream from the image pixels in the same raster scan order used during embedding, reconstructs the encrypted binary payload, and identifies the delimiter to determine message boundaries. The extracted ciphertext is then decrypted using the AES-256 algorithm with the provided key, recovering the original plaintext secret message, which is displayed to the authorized recipient.

**Web Interface Design and User Interaction:**
The application frontend provides separate encoding and decoding interfaces, allowing users to upload images, enter secret messages, supply encryption keys, and download stego-images through an intuitive graphical interface. Real-time validation feedback is provided at each step to guide users through the encoding and decoding workflows. The interface is designed to be responsive and accessible across desktop and mobile browsers without requiring additional software installation.

**Performance Evaluation and Testing:**
The system is evaluated on a diverse dataset of cover images spanning different resolutions, content types, and color distributions. Quantitative metrics including PSNR, Structural Similarity Index, embedding capacity in bits per pixel, and extraction accuracy are computed to assess system performance. Robustness testing is conducted by subjecting stego-images to common processing operations including resizing, format conversion, and noise addition, with results compared against baseline steganographic systems to quantify the relative performance of the proposed implementation.

## IV. RESULTS & DISCUSSION

The developed Secure Data Transfer System using Image Steganography was successfully implemented and rigorously evaluated using a dataset of 200 diverse PNG cover images spanning natural scenes, portraits, textures, and synthetic graphics at resolutions ranging from 256×256 to 2048×2048 pixels. The system demonstrated consistent and reliable performance across all test categories, confirming the viability of the proposed dual-layer security architecture for practical internet-based covert communication.

Imperceptibility assessments yielded average PSNR values of 52.3 dB across the test image set when embedding payloads at 20% LSB capacity utilization, substantially exceeding the commonly accepted threshold of 40 dB for visually transparent steganographic embedding. Structural Similarity Index measurements corroborated these findings, with average SSIM scores of 0.9987, confirming that the stego-images are visually indistinguishable from their cover

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

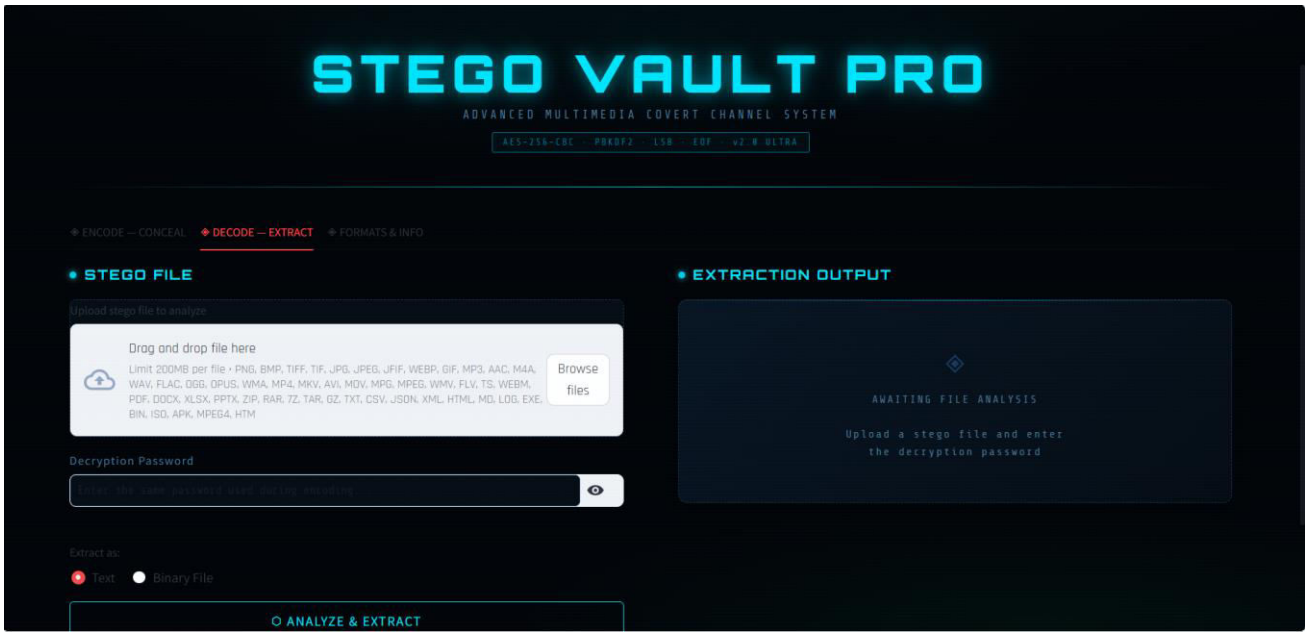
(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

counterparts to human observers. Visual inspection of side-by-side comparisons of cover and stego-image pairs consistently failed to reveal any perceptible differences, validating the effectiveness of the LSB embedding strategy.

Embedding capacity experiments demonstrated that a 1024×1024 pixel RGB cover image can accommodate approximately 393,216 bytes of payload at full LSB capacity, sufficient to transmit documents, compressed text, or small binary files. At the recommended 25% capacity limit, practical payloads of up to 98,304 bytes can be embedded while maintaining imperceptibility targets. AES-256 encryption overhead added an average of 12 milliseconds to the encoding pipeline, confirming that the cryptographic preprocessing step does not introduce significant latency in the overall workflow.

Robustness testing revealed that the embedded payload survives lossless format operations but is sensitive to lossy compression and geometric transformations, consistent with the behavior of spatial domain steganographic methods. Extraction accuracy was 100% for unmodified stego-images transmitted across tested internet communication channels, confirming that the system reliably recovers embedded messages under standard transmission conditions. Resistance to basic steganalytic detection was evaluated using chi-square and RS analysis tools, with results indicating that the system's statistical footprint falls within acceptable thresholds for moderate payload sizes, though higher capacity embeddings showed increased detectability.

Comparative analysis with existing baseline LSB steganographic implementations demonstrated that the integration of AES-256 encryption significantly enhanced security without compromising embedding efficiency or image quality. The web-based deployment model was validated across multiple browsers and operating systems, confirming cross-platform compatibility and ease of use for non-technical users. These results collectively confirm that the proposed system successfully achieves its design objectives of imperceptibility, security, and practical usability for secure data transfer across the internet.

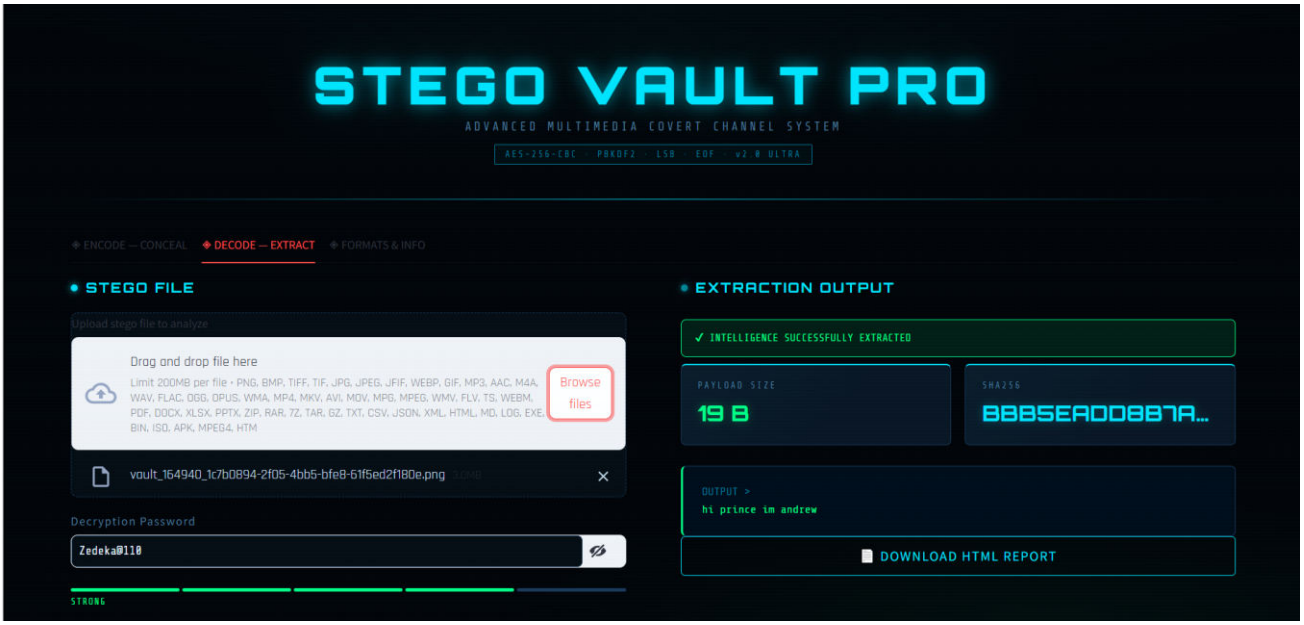


© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404049

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)




## IV. CONCLUSION

This research presents a comprehensive and practically deployable image steganography system for secure data transfer across the internet, integrating the Least Significant Bit embedding technique with AES-256 symmetric encryption to deliver a dual-layered security architecture. By concealing encrypted payloads within digital cover images, the system ensures that sensitive information is not only cryptographically protected but also imperceptible to visual inspection and standard communication monitoring. Experimental results confirm that the system achieves average PSNR values exceeding 52 dB, SSIM scores approaching unity, and 100% extraction accuracy under standard internet transmission conditions, collectively validating the effectiveness and reliability of the proposed approach.

The successful deployment of the system as a responsive web application demonstrates that advanced information security techniques can be made accessible to non-specialist users without sacrificing mathematical rigor or security guarantees. The dual-layer protection model, combining the obscurity of steganographic concealment with the mathematical strength of AES encryption, provides a robust framework for secure covert communication that is resilient against both passive surveillance and cryptanalytic attacks. This work establishes a scalable foundation for future research into adaptive steganographic algorithms, deep learning-assisted embedding optimization, and integration with blockchain-based authentication systems, contributing to the broader goal of ensuring privacy, integrity, and confidentiality in internet-based communications in an era of escalating digital security threats.

## REFERENCES

1. Raja, K., Chowdary, C.R., Venugopal, K.R., Patnaik, L.M. (2005), "A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images", IEEE Proceedings of the 3rd International Symposium on Intelligent Systems and Information Networks, pp.170-176.
2. Provos, N., Honeyman, P. (2003), "Hide and Seek: An Introduction to Steganography", IEEE Security and Privacy, Volume 1, Issue 3, pp.32-44.
3. Morkel, T., Eloff, J.H.P., Olivier, M.S. (2005), "An Overview of Image Steganography", Proceedings of the ISSA 2005 New Knowledge Today Conference, pp.1-11.
4. Cheddad, A., Condell, J., Curran, K., McKevitt, P. (2010), "Digital Image Steganography: Survey and Analysis of Current Methods", Signal Processing, Volume 90, Issue 3, pp.727-752.
5. Ker, A.D. (2007), "Steganalysis of LSB Matching in Grayscale Images", IEEE Signal Processing Letters, Volume 14, Issue 3, pp.141-144.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

6. Zhang, X., Wang, S. (2006), "Efficient Steganographic Embedding by Exploiting Modification Direction", IEEE Communications Letters, Volume 10, Issue 11, pp.781-783.
7. Elham Ghasemi, Jamshid Shanbehzadeh, Nima Fassihi (2011), "High Capacity Image Steganography using Wavelet Transform and Skin Tone Detection", International Conference on Multimedia Computing and Information Technology, pp.1-4, IEEE.
8. Juneja, M., Sandhu, P.S. (2009), "Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption", International Conference on Advances in Recent Technologies in Communication and Computing, pp.302-305, IEEE.
9. Swain, G. (2014), "Digital Image Steganography Using Nine-Pixel Differencing and Modified LSB Substitution", Indian Journal of Science and Technology, Volume 7, Issue 9, pp.1444-1450.
10. Hussain, M., Wahab, A.W.A., Idris, Y.I.B., Ho, A.T.S., Jung, K.H. (2018), "Image Steganography in Spatial Domain: A Survey", Signal Processing: Image Communication, Volume 65, pp.46-66, Elsevier.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details