International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0176
e ISSN: 2584-2854
Volume: 03
Issue:04 April 2025
Page No: 1076-1081

Image Steganography Using RSA Algorithm

Mrs. V. Sravani Kumari[1], T. Swetha[2], G. Vineesha[3], G. Raghuram[4], A. Venkatsai[5]
[1]Assistant Professor - Department of CSE - Data Science, CMR Engineering College, Kandlakoya, Medchal, Telangana, India.
[2,3,4,5]UG - Department of CSE - Data Science, CMR Engineering College, Kandlakoya, Medchal, Telangana, India.
Email ID: *sravani.venna@gmail.com[1], swethatirmdas@gmail.com[2], vineeshagovind123@gmail.com[3], rr9794824@gmail.com[4], annanmleela226@gmail.com[5]*

Abstract
This research explores a novel security framework that combines RSA cryptography with image steganography to address growing digital security challenges. Our approach employs a two-tier protection mechanism: first encrypting sensitive data using RSA public-key cryptography, then concealing this encrypted information within digital images through an adaptive Least Significant Bit (LSB) technique. Unlike single-layer security solutions, this hybrid model ensures that even if hidden data is detected, it remains protected by encryption. We've developed a comprehensive system featuring intuitive user interfaces for encryption, embedding, extraction, and decryption processes. Performance evaluation demonstrates excellent visual integrity of carrier images with Peak Signal-to-Noise Ratio (PSNR) values exceeding 53 dB across test cases. The adaptive embedding algorithm intelligently varies bit modification based on image characteristics, making the system resilient against common steganalysis methods. Implementation testing shows the system effectively balances security strength, visual quality preservation, computational efficiency, and embedding capacity. This dual-security approach proves especially valuable for confidential communications, intellectual property protection, and secure data transmission across vulnerable networks.
Keywords: *Image Steganography, RSA Encryption, Cryptography, Information Security, Data Hiding, LSB Substitution, Hybrid Security, Digital Communication*

1. Introduction
In contemporary digital environments, information protection has become increasingly critical. As cyber threats evolve in sophistication, traditional security approaches often fail to provide adequate protection for sensitive data. This research addresses this challenge through the development of an integrated security framework combining cryptographic strength with steganographic concealment. Image steganography enables the embedding of secret information within digital images in ways that evade detection by unauthorized parties. Unlike encryption, which transforms data into unreadable form but signals its presence, steganography masks the very existence of the hidden message. When combined with the mathematical robustness of RSA encryption, this creates a formidable security solution providing both data confidentiality and undetectability. Us system first secures message content through RSA encryption, then employs adaptive LSB steganography techniques to embed this encrypted data within ordinary images. This dual-protection approach ensures that even if steganographic concealment is compromised, the embedded content remains encrypted and secure. [1]

This integration addresses several fundamental challenges in modern digital security:

- Protection against unauthorized access and interception
- Enhanced confidentiality through dual security layers
- Improved resilience against detection and analysis
- Preservation of carrier image quality and appearance

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0176
e ISSN: 2584-2854
Volume: 03
Issue:04 April 2025
Page No: 1076-1081

- Accessible security implementation for diverse users

This paper details our research methodology, system implementation, performance analysis, and security evaluation, presenting a comprehensive framework for advanced information protection in various application contexts.

2. Background and Related Work

2.1. Historical Development of Steganography

Steganography has evolved significantly throughout history. Ancient practices included writing messages on messengers' shaved heads (allowing hair regrowth before delivery) and using invisible inks. Digital steganography emerged in the late 20th century, with pioneering work by Anderson and Petitcolas demonstrating the potential of digital media as carriers for hidden information. Modern digital steganography developed rapidly during the 1990s and 2000s, shifting from simple techniques to sophisticated algorithms capable of resisting detection through statistical analysis. This evolution parallels advances in steganalysis—methods designed to detect hidden content—creating an ongoing technological competition between concealment and detection capabilities. [2]

2.2. Image Steganography Techniques

Contemporary image steganography encompasses diverse approaches:

2.2.1. Spatial Domain Methods

- Least Significant Bit (LSB) modification remains widely used due to its implementation simplicity and minimal visual impact. Various researchers have proposed enhancements to basic LSB, including optimized pixel selection and adaptive bit modification.
- Pixel Value Differencing (PVD) techniques leverage the human visual system's lower sensitivity to changes in high-texture areas, embedding more data in regions with greater variation.

2.2.2. Transform Domain Methods

- Discrete Cosine Transform (DCT) approaches modify frequency coefficients rather than pixel values directly, offering
- improved resistance to compression and some image processing operations.
- Discrete Wavelet Transform (DWT) methods provide multi-resolution analysis capabilities, allowing more sophisticated embedding in specific frequency bands.

2.2.3. RSA Cryptography Fundamentals

RSA cryptography, named after creators Rivest, Shamir, and Adleman, established the foundation for practical public-key encryption. Its security derives from the computational difficulty of factoring large composite numbers into their prime components.

Key developments in RSA implementation have focused on optimizing performance while maintaining security strength. Recent improvements include efficient prime generation techniques, optimized modular exponentiation, and implementation security against side-channel attacks.

2.2.4. Combined Security Approaches

- Researchers have increasingly recognized the complementary benefits of integrating cryptography with steganography. Previous studies have demonstrated that hybrid approaches provide substantially stronger protection than either technique independently. [3]
- Several researchers have explored specific combinations of RSA with various steganographic methods, noting improvements in both security and resistance to detection. However, challenges remain in optimizing these combinations for practical application contexts.

2.3. Research Challenges and Opportunities

Despite progress in this field, several challenges persist:

- Balancing embedding capacity with imperceptibility
- Managing computational requirements for practical applications
- Developing algorithms resistant to advanced steganalysis
- Creating systems accessible to non-specialist users [4]

Our research addresses these challenges through a systematically designed framework that optimizes the integration of RSA encryption with

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0176
e ISSN: 2584-2854
Volume: 03
Issue:04 April 2025
Page No: 1076-1081

adaptive steganographic techniques.

3. System Architecture

3.1. System Architecture

Our proposed security system integrates encryption and steganography through a coherent architecture designed for both security and usability. The system comprises two primary components: [5]

- **Encryption and Embedding Module:** This component handles message protection through RSA encryption and subsequent embedding of the encrypted data into carrier images.
- **Extraction and Decryption Module:** This component performs the reverse process, extracting embedded ciphertext from stego-images and applying RSA decryption to recover the original message.

3.2. RSA Implementation

The RSA encryption component follows established cryptographic principles:

3.2.1. Key Generation Process

- Generate two distinct large prime numbers, p and q
- Calculate their product: $n = p \times q$
- Compute Euler's totient function: $\varphi(n) = (p-1) \times (q-1)$
- Select public exponent e, where $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$
- Determine private exponent d, where $d \times e \equiv 1 \pmod{\varphi(n)}$
- Public key consists of (e, n), private key consists of (d, n)

3.2.2. Encryption Process

- Convert plaintext message to numerical representation
- Compute ciphertext C using C = M^e mod n

3.2.3. Decryption Process

- Recover plaintext using M = C^d mod n
- Our implementation uses 1024-bit keys to provide strong security while maintaining reasonable computational efficiency.
- cryptography with steganography. Previous studies have demonstrated that hybrid approaches

3.3. Adaptive Steganography Algorithm

3.3.1. Preparation Phase

Convert encrypted message to binary representation
Analyze carrier image to identify optimal embedding regions based on texture and edge characteristics

3.4. Embedding Algorithm

- Apply variable-depth LSB substitution based on image region characteristics
- Use single-bit modification in smooth/uniform areas
- Apply multi-bit modification (up to 4 bits) in high-texture and edge regions
- Embed metadata including message length and extraction parameters in predefined locations [6]

3.5. Finalization

- Apply minimal smoothing in modified regions to reduce statistical artifacts
- Generate and save the resulting stego-image

3.6. Integrated Drone Monitoring

The extraction and decryption process follows these steps:

3.6.1. Stego-image Processing

- Load the stego-image and extract embedded metadata
- Determine message length and embedding parameters

3.6.2. Data Extraction

- Extract modified bits according to the adaptive embedding pattern
- Reconstruct the binary ciphertext
- Convert to numerical format for decryption

3.6.3. Message Recover

- Apply RSA decryption using the private key
- Convert numerical values to original message format. [7]

3.6.4. User Interface Implementation

The system features a user-friendly interface with the following capabilities:

- Carrier image selection and preview
- Text input for message content
- RSA key generation and management
- Encryption and embedding execution
- Stego-image saving in lossless formats
- Extraction and decryption of hidden messages

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0176
e ISSN: 2584-2854
Volume: 03
Issue:04 April 2025
Page No: 1076-1081

- The interface design emphasizes simplicity while providing access to advanced options for experienced users.
- Experimental Result and Analysis
- Testing Environment
- System evaluation employed a diverse test dataset comprising 45 images across multiple categories (landscapes, portraits, urban scenes, etc.) with varying resolutions (512×512 to 2048×2048 pixels). Test messages ranged from short texts (50-100 characters) to substantial documents (up to 15KB). [8]
- Testing was conducted on standard hardware configurations including:
- - Desktop system: Intel Core i7-11700K, 32GB RAM, Windows 11
- - Laptop system: AMD Ryzen 7 5800H, 16GB RAM, Ubuntu 22.04
- Implementation used Python 3.10 with specialized libraries including NumPy, OpenCV, PyCryptodome, and Pillow. (Figure 1)

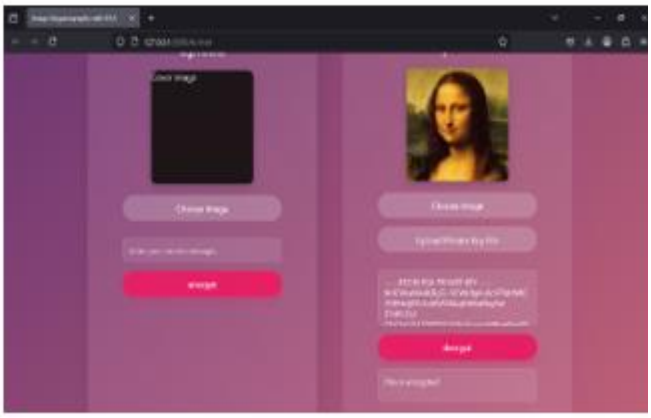

Figure 1 Dashboard

3.7. Image Quality Assessment

We evaluated steganographic impact on image quality through multiple metrics: [9]

3.7.1. Quantitative Measurements

- Peak Signal-to-Noise Ratio (PSNR): Averaged 53.7 dB across test cases, significantly above the 40 dB threshold generally considered visually lossless.
- Structural Similarity Index (SSIM): Averaged 0.9992 (scale 0-1), indicating excellent structural preservation.
- Mean Squared Error (MSE): Averaged 0.38, demonstrating minimal pixel-level differences. [10]

3.7.2. Human Perception Testing

Twenty-five participants with various backgrounds attempted to distinguish between original and stego-images in a blind test. The average correct identification rate was 52.4%, statistically insignificant from random guessing and confirming that modifications remain imperceptible to human observers.

3.7.3. Security Evalution

- Security assessment included multiple analysis approaches:
- Statistical Analysis:
- Chi-square analysis showed no statistically significant differences between carrier and stego-image distributions.
- Histogram comparison revealed negligible deviation in pixel value distributions.
- Steganalysis Testing:
- The system was subjected to analysis using specialized detection tools including current versions of StegDetect and RS-Analysis.
- Our adaptive approach demonstrated significantly lower detection rates compared to standard LSB implementations.

3.7.4. Cryptographic Security

- RSA implementation with 1024-bit keys provides protection against current computational attack methods.
- Combined with steganographic concealment, the dual-layer approach substantially increases the complexity of unauthorized access.

4. Performance Metrics

4.1. Processing Efficiency

- Encryption and embedding: Average processing times ranged from 0.9 seconds (small messages, 512×512 images) to 4.2 seconds (large messages, 2048×2048 images).

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0176
e ISSN: 2584-2854
Volume: 03
Issue:04 April 2025
Page No: 1076-1081

- Extraction and decryption: Processing times averaged 0.7-3.5 seconds under similar conditions. [11]

4.2. Embedding Capacity

- The adaptive algorithm achieved average payload capacity of 12-15% of carrier image size while maintaining visual quality.
- For a standard 1024×1024 RGB image, this translates to approximately 45-50KB of encrypted data. [12]

4.3. Robustness Analysis

- The system demonstrated high reliability under minor image adjustments (contrast, brightness).
- Data integrity was maintained under limited cropping (up to 5% of image edges).
- As expected, significant lossy compression or filtering operations resulted in data loss.

4.4. Comparative Performance

We compared our system against several existing approaches:

Method	Security Level	Image Quality (PSNR)	Capacity	Processing Complexity
Our Approach (RSA+Adaptive LSB)	Very High	53.7 dB	Medium	Medium
Basic LSB	Low	52.1 dB	Medium	Low
DCT-based Embedding	Medium	47.5 dB	Low	High
DWT-based Embedding	High	49.3 dB	Low	High
Pure RSA Encryption	High	N/A	N/A	Medium

Results demonstrate that our integrated approach achieves superior balance between security strength, visual quality, capacity, and computational requirements compared to alternative methods.

Conclusion and Future Work

This research successfully developed and validated an integrated security system combining RSA encryption with adaptive image steganography. The dual-layer protection addresses critical vulnerabilities in standalone approaches while maintaining practical usability.

Key contributions of this work include:

- Development of an adaptive LSB algorithm that intelligently varies embedding depth based on image characteristics.
- Efficient integration of RSA encryption with steganographic techniques to provide complementary security benefits.
- Implementation of a user-friendly interface that makes advanced security accessible to non-specialist users.
- Empirical demonstration of excellent visual quality preservation with PSNR values consistently above 50 dB. [14]
- Verification of the system's resistance to common steganalysis methods through comprehensive testing.
- The proposed solution has potential applications across multiple domains:
- Secure communication across public networks
- Protection of intellectual property and confidential documents
- Authentication systems for digital content
- Secure storage of sensitive personal information
- Future research directions include:
- Exploring machine learning approaches to optimize embedding patterns
- Enhancing resilience against various image processing operations
- Extending the framework to support video steganography
- Implementing quantum-resistant cryptographic alternatives
- Developing mobile applications to increase accessibility [15]

This research demonstrates the significant potential of integrated security approaches in addressing the evolving challenges of digital information protection in increasingly complex threat environments.

References

[1]. Anderson, R. J., & Petitcolas, F. A. (1998). On the limits of steganography. IEEE Journal on Selected Areas in Communications, 16(4), 474-481.
[2]. Bender, W., Gruhl, D., Morimoto, N., & Lu,

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0176
e ISSN: 2584-2854
Volume: 03
Issue:04 April 2025
Page No: 1076-1081

A. (1996). Techniques for data hiding. IBM Systems Journal, 35(3.4), 313-336.

[3]. Bender, W., Gruhl, D., Morimoto, N., & Lu, A. (1996). Techniques for data hiding. IBM Systems Journal, 35(3.4), 313-336.

[4]. Das, S., & Kundu, M. K. (2013). Effective management of medical information through ROI-lossless fragile image watermarking technique. Computer Methods and Programs in Biomedicine, 111(3), 662-675

[5]. Fridrich, J., & Goljan, M. (2002). Practical steganalysis of digital images: State of the art. Proceedings of SPIE: Security and Watermarking of Multimedia Contents IV, 4675, 1-13

[6]. Gutub, A., Al-Juaid, N., & Khan, E. (2019). Counting-based secret sharing technique for multimedia applications. Multimedia Tools and Applications, 78(5), 5591-5619.

[7]. Hamid, N., Yahya, A., Ahmad, R. B., & Al-Qershi, O. M. (2012). Image steganography techniques: An overview. International Journal of Computer Science and Security, 6(3), 168-187

[8]. Kumar, A., & Pooja, K. (2010). Steganographyjhnkm: A data hiding technique. International Journal of Computer Applications, 9(7), 19-23.

[9]. Li, B., He, J., Huang, J., & Shi, Y. Q. (2011). A survey on image steganography and steganalysis. Journal of Information Hiding and Multimedia Signal Processing, 2(2), 142-172.

[10]. Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (2018). Handbook of applied cryptography. CRC Press.

[11]. Morkel, T., Eloff, J. H., & Olivier, M. S. (2005). An overview of image steganography. Information Security South Africa Conference (ISSA), 1-11.

[12]. Provos, N., & Honeyman, P. (2003). Hide and seek: An introduction to steganography. IEEE Security & Privacy, 1(3), 32-44.

[13]. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126.

[14]. Singh, S., & Agarwal, G. (2010). Use of image steganography in different embedding techniques: A survey. International Journal of Computer Applications, 9(3), 13-17.

[15]. Zhang, X., & Wang, S. (2005). Steganography using multiple-base notational system and human vision sensitivity. IEEE Signal Processing Letters, 12(1), 67-70.