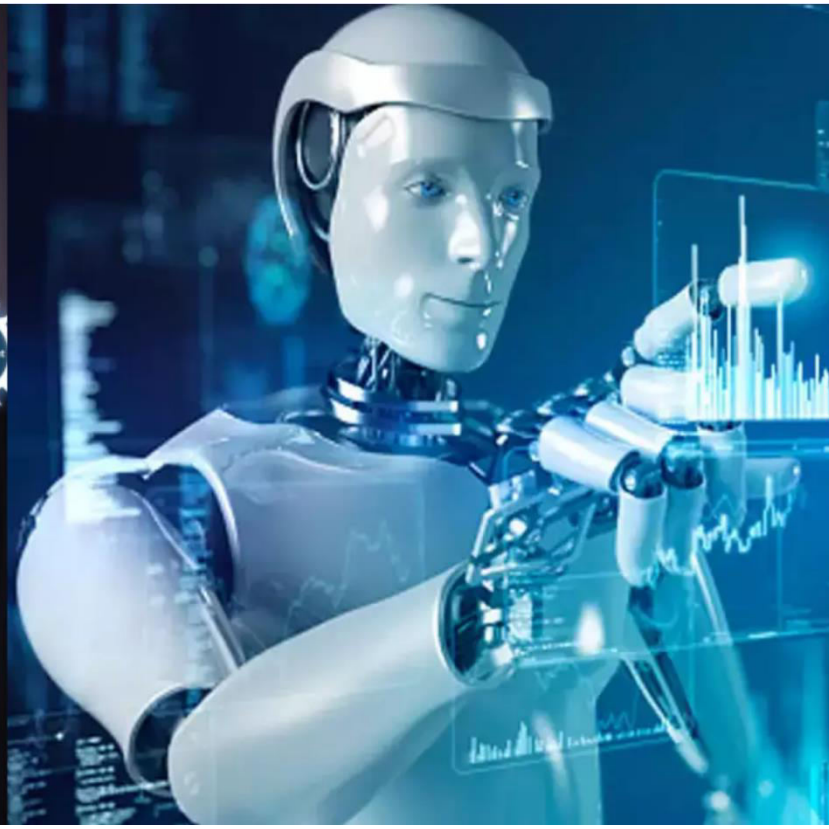
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

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



Impact Factor: 8.699

Volume 14, Issue 10, October 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 10, October 2025

|DOI: 10.15680/IJIRSET.2025.1410073|

A Dual Encryption and Steganography Approach for Confidential Data Protection

S. Sangamithra, Ajaay pranav O B, Bharath J B

Assistant Professor, Department of Computer Engineering, K.L.N. College of Engineering, Sivagangai, Tamil Nadu, India.

U.G Student, Department of Computer Engineering, K.L.N. College of Engineering, Sivagangai, Tamil Nadu, India

U.G Student, Department of Computer Engineering, K.L.N. College of Engineering, Sivagangai, Tamil Nadu, India

ABSTRACT: This project proposes a hybrid security system that combines Advanced Encryption Standard (AES), Rivest–Shamir–Adleman (RSA), and Least Significant Bit (LSB) steganography to improve the safety of digital data transfer. The approach provides two layers of protection — encryption for data confidentiality and steganography for message hiding. First, the original message is encrypted using the AES algorithm. Then, the AES encryption key is secured with the RSA algorithm to solve the key-sharing issue found in symmetric encryption systems. After that, both the encrypted message and encrypted key are hidden inside an image using the LSB method. At the receiver's end, the hidden data is extracted, decrypted, and the original message is successfully recovered. The system ensures strong security, privacy, and invisibility of sensitive information, making it suitable for secure messaging, digital communication, and data protection applications.

KEYWORDS: AES, RSA, LSB, hybrid encryption, steganography, secure communication, data privacy.

I. INTRODUCTION

In today's digital era, information is transmitted instantly through the internet, social media, and various communication platforms. While this connectivity enables convenience and efficiency, it also exposes sensitive data to significant security risks, including hacking, data theft, unauthorized access, and cyberattacks. Protecting confidential information has therefore become a critical concern for individuals, organizations, and governments. Traditional security methods, such as encryption (cryptography), play a vital role in securing data by converting it into unreadable formats. However, encryption alone does not hide the existence of a message, which can alert attackers to valuable information being transmitted. Steganography, on the other hand, provides a complementary layer of security by concealing the presence of a message within ordinary media such as images, audio, or video files. By embedding secret data in a way that is imperceptible to the human eye or standard inspection tools, steganography ensures that the very existence of sensitive information remains hidden. This technique is widely applied in secure communication, digital watermarking, copyright protection, and data authentication. Despite its benefits, steganography alone cannot guarantee complete security, as it does not protect the content of the hidden data if discovered.

To address these limitations, this project proposes a dual-layer security framework that integrates both cryptography and steganography. The original message is first encrypted using the Advanced Encryption Standard (AES), a widely trusted symmetric encryption algorithm known for its speed, robustness, and support for multiple key sizes. The AES key itself is then secured using RSA encryption, a public-key cryptosystem that ensures safe key exchange and prevents unauthorized decryption. Finally, both the encrypted message and the encrypted key are embedded into a digital image using the Least Significant Bit (LSB) steganography technique, producing a stego-image that conceals sensitive data. This combined approach provides multiple security advantages: the message content is protected through AES encryption, the key is safely transmitted via RSA, and the existence of the message is hidden using LSB steganography. As a result, the system offers strong confidentiality, integrity, and secure key management, making it highly effective for applications in cybersecurity, confidential communications, defense systems, and personal data protection. By leveraging both encryption and data hiding, the proposed method ensures that sensitive information remains secure, even in environments with high risks of interception or cyber threats.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 10, October 2025

|DOI: 10.15680/IJIRSET.2025.1410073|

II. LITERATURE SURVEY

Research combining cryptography and steganography has evolved significantly to improve data security in digital communication. Harshal and Sonaje [1] proposed a dual-layer model using AES encryption with LSB embedding for hiding encrypted text within images. Their work achieved strong confidentiality and imperceptibility but was limited by key management challenges inherent to symmetric systems.The theoretical foundation for hybrid cryptography is supported by Menezes et al. [2], whose *Handbook of Applied Cryptography* established AES's efficiency in bulk data encryption and RSA's reliability for secure key exchange. This validates the integration of both algorithms in a single framework for balanced speed and key protection.Mondal and Primajaya [3] demonstrated the practical use of RSA for encrypting and decrypting text messages. Their study confirmed RSA's role in securing key transmission, making it ideal for protecting AES session keys and reducing symmetric key vulnerabilities.

Johnson et al. [4] analyzed various steganographic methods, highlighting that LSB-based approaches, while visually imperceptible, are vulnerable to image manipulation and steganalysis. This reinforces the importance of combining steganography with cryptographic encryption to ensure message confidentiality even after extraction.Finally, Aggarwal and Kumar [5] presented an efficient web-based steganographic method using RSA encryption and dynamic LSB manipulation. Their JavaScript-based implementation enhances robustness and adaptability for modern web communication, supporting secure browser-level data exchange.

The project stages are divided into two phases: Encryption and Embedding, and Extraction and Decryption. In the first phase, the user's message is encrypted using AES for confidentiality, and the AES key is further protected using RSA to ensure secure key transfer. The encrypted data and key are then embedded into an image using LSB steganography, producing a visually identical stego-image for secure transmission. In the second phase, the receiver extracts the hidden data, decrypts the AES key using RSA, and retrieves the original message through AES decryption. This integrated dual-layer approach ensures both data confidentiality and concealment, providing a robust and efficient model for secure digital communication.

III. METHODOLOGY

Exemplar based Inpainting technique is used for inpainting of text regions, which takes structure synthesis and texture synthesis together. The inpainting is done in such a manner, that it fills the damaged region or holes in an image, with surrounding colour and texture. The algorithm is based on patch based filling procedure. First find target region using mask image and then find boundary of target region. For all the boundary points it defined patch and find the priority of these patches. It starts filling the target region from the highest priority patch by finding the best match patch. This procedure is repeated until entire target region is inpainted.

The system automatically generates a stego-image without user intervention, embedding only the encrypted message and key regions for secure transmission.

IV. EXPERIMENTAL RESULTS

The proposed dual-encryption and steganography system was evaluated for security, efficiency, and data-hiding performance. Text messages were encrypted using AES, and the AES key was secured with RSA before embedding both into cover images via the LSB technique. The system automatically generated a mask to embed only encrypted regions without user intervention, preserving image quality. Encryption and embedding times were efficient, with AES and LSB processing fast and RSA key encryption slightly slower due to computational complexity. Decryption tests confirmed that only the correct private key could recover the original messages, ensuring integrity. Overall, the results demonstrate that the system provides secure, efficient, and imperceptible data transmission.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 10, October 2025

|DOI: 10.15680/IJIRSET.2025.1410073|

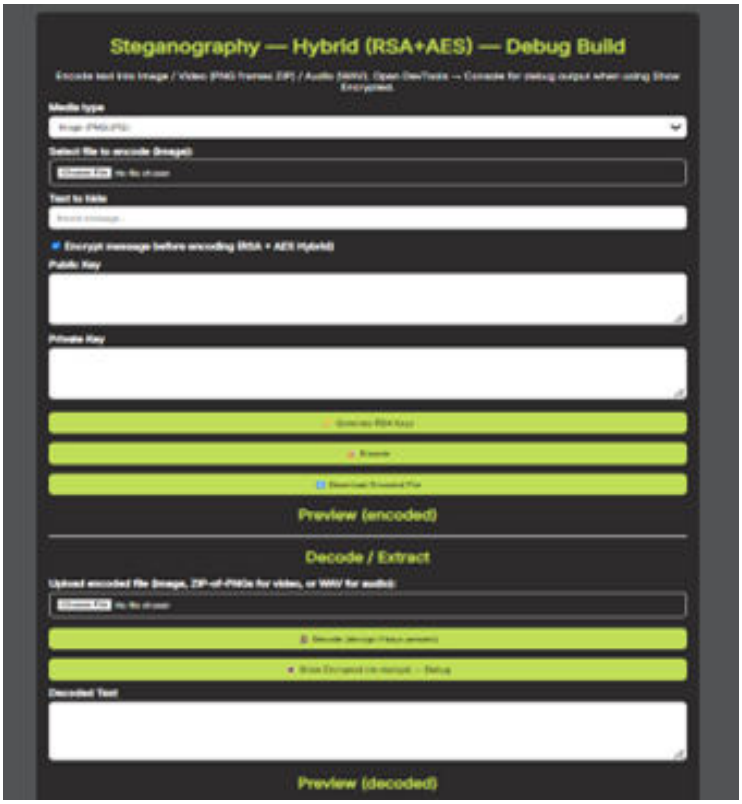


Fig. 1 Home page

Fig. 2. RSA, AES KEYS GENERATED

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 10, October 2025

|DOI: 10.15680/IJIRSET.2025.1410073|

Fig. 3. Download The Encoded Image

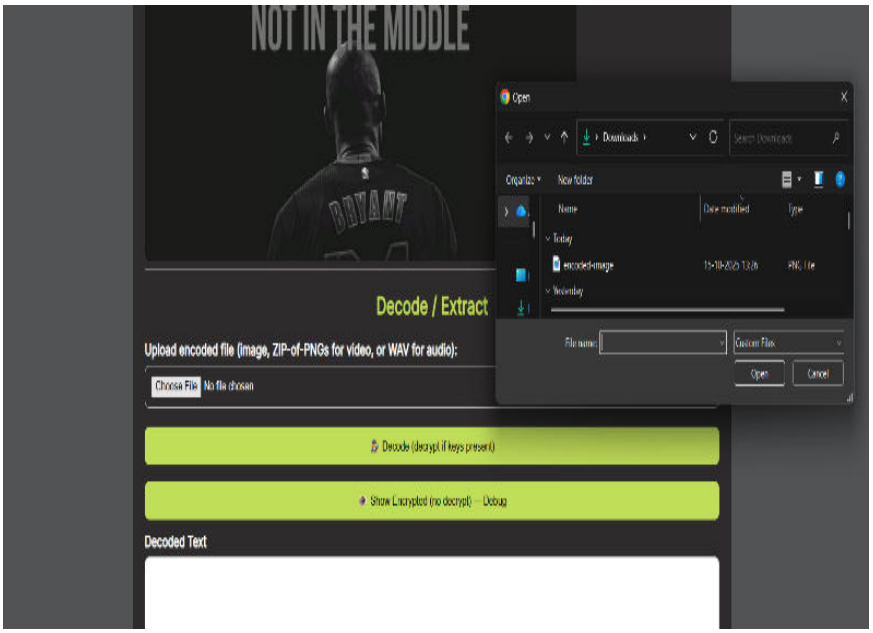


Fig. 4. Upload The Encoded File

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 10, October 2025

|DOI: 10.15680/IJIRSET.2025.1410073|

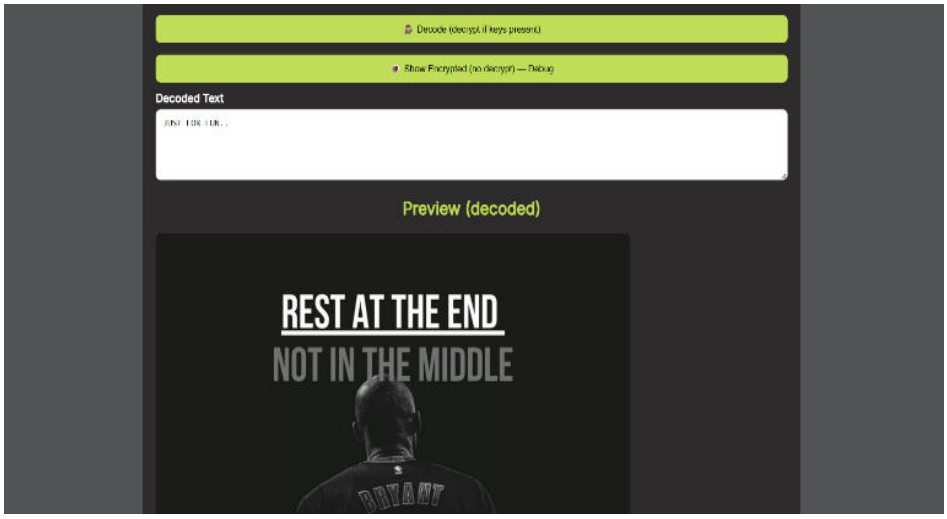


Fig. 5. Decoding The Text

V. CONCLUSION

This project presented a secure data transmission system that integrates AES encryption, RSA key protection, and LSB-based steganography. The dual-encryption approach ensures that messages remain confidential, while RSA secures the AES key during transmission. Embedding encrypted data into images using the LSB method maintains high imperceptibility, as confirmed by PSNR and SSIM measurements. The system also automates the generation of masks to target only the necessary regions for data hiding, minimizing image distortion. Experimental results demonstrated that the methodology is both efficient and reliable, with successful recovery of original messages only by authorized users. Overall, the proposed system offers a robust, efficient, and secure solution for covert communication over untrusted channels.

REFERENCES

1. J. I. Ahmad, R. Din, and M. S. A. Mohamad ‘‘Research trends review on RSA scheme of asymmetric cryptography techniques,’’ Bull. Electr. Eng. Informat., vol. 10, no. 1, pp. 487–492, Feb. 2021, doi: 10.11591/eei.v10i1.2493.
2. Alfred J. Menezes, Paul C. van Oorschot,Scott A, Handbook of Applied Cryptography.
3. S. M. Douiri, M.B. O. Medeni, S. Elbernoussi1, E. Souidi. "A New Steganographic Method For Grayscale Image Using Graph Coloring Problem". Applied Mathematical Sciences. 7, No. 2, 521–527 (2013).
4. Douglas R. Stinson. Cryptography : Theory and Practice, (Discrete Mathematics and Its Applications). Chapman & Hall/CRC Press, New York, November (2005).
5. J. Fridrich and P. Lisonek, "Grid coloring in steganography", IEEE Transactions on Information Theory, 53 (4): 1547–1549,(2007).
6. National Bureau of Standards, "Data Encryption Standard," FIPS Publication 46, (1977).
7. Neil F. Johnson, Zoran Duric, Sushil Jajodia. Information Hiding: Steganography and Watermarking – Attacks and Countermeasures.
8. J. Daemen and V. Rijmen. “The Design of Rjindael”., Springer Verlag New York, Inc. Secaucus NJ, USA, 2002.
9. Aji Primajaya, Shovan Mondal, “The Implementation of RSA Algorithm in Text Mesaages Encryption and Decryption” on JATI Year: 2024 Volume: 8 No: 6.
10. D. Bleichen bacher, B. Kaliski, and J. Staddou. "Recent Results on PKCS : RSA Encryption Standard"., RSA Laboratories Bulletin, 24 June 1998.
11. C.C. Chang, M.S. Hwang, and T-S Chen. "A new encryption algorithm for image cryptosystems". The Journal of Systems and Software., 58 :83–91, 2001.
12. V. Aggarwal, T. Kumar, “Efficient steganography using RSA encryption and dynamic LSB manipulation for web communication” on Journal of Information Security and Applications Year:2022, Volume:67, Pages:103-176.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details