International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 05 Issue: 03 | Mar – 2026 DOI: 10.55041/ISJEM05769
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

Secure Text Embedding in Images via Pixel-Level Steganography

M.Sai Prasad[1], B. Muktheeshwar[2], K.Rasagnya[3], D.Niharika[4], N.Harshith[5]

1Assistant Professor, Department of CSE, Jyothishmathi Institute of Technology and Science, Telangana, India,

2Student, Department of CSE(AI&ML), Jyothishmathi Institute of Technology and Science, Telangana, India, muktheeshwarbukka@gmail.com

3Student, Department of CSE(AI&ML), Jyothishmathi Institute of Technology and Science, Telangana, India, kodurirasagnya26@gmail.com

4Student, Department of CSE(AI&ML), Jyothishmathi Institute of Technology and Science, Telangana, India, dommatiniharika@gmail.com

5Student, Department of CSE(AI&ML), Jyothishmathi Institute of Technology and Science, Telangana, India, harshithnarsingoju14@gmail.com

***Abstract*— Secure transmission of sensitive information has become increasingly important due to the rapid growth of digital communication systems. This project proposes a secure data communication approach that combines cryptography and steganography to enhance information protection. In the proposed system, the secret text message is first encrypted using the Advanced Encryption Standard (AES) algorithm to ensure confidentiality. The encryption key is further protected using the RSA public key cryptographic technique to enable secure key exchange between sender and receiver. After encryption, the ciphertext is embedded into a digital image using the Least Significant Bit (LSB) steganography method, allowing the message to remain hidden without significantly altering the visual quality of the image. At the receiver side, the hidden data is extracted from the stego image, the AES key is recovered using RSA decryption, and the original message is reconstructed through AES decryption. By integrating encryption with image-based data hiding, the proposed system provides multiple layers of security, ensuring confidentiality, integrity, and secure communication over open networks.**

***Index Terms*— Steganography, AES Encryption, RSA Cryptography, LSB Technique, Image Security, Data Hiding, Secure Communication**

1. INTRODUCTION

The continuous growth of digital communication technologies has made the exchange of information faster and more convenient than ever before. However, this rapid advancement has also increased the risk of security threats such as data interception, unauthorized access, and cyber attacks. Sensitive information including personal messages, financial details, and confidential documents is frequently transmitted across public networks, making it vulnerable to malicious activities. Traditional security mechanisms mainly rely on cryptography to protect data by converting readable information into an unreadable format using encryption algorithms. Although encryption ensures the confidentiality of the message content, the presence of encrypted data can still draw attention from attackers. This situation may encourage attempts to break the encryption using different analytical techniques. As a result, relying solely on encryption may not always provide complete security for highly sensitive information. To overcome this limitation, additional techniques that can hide the existence of the message itself are required to enhance the overall security of communication systems.

Steganography provides a solution by concealing secret information within digital media such as images, audio, or video files, making the communication less noticeable. Among these mediums, digital images are widely used because they contain a large number of pixels that can store hidden information without significantly altering the visual quality of the image. One commonly used method is the Least Significant Bit (LSB) technique, which embeds secret data into the least significant bits of image pixels while maintaining the original appearance of the image. However, if hidden data is discovered, it may still be vulnerable if it is not encrypted. Therefore, combining steganography with cryptography creates a multi-layered security approach. In the proposed system, the secret text message is first encrypted using the Advanced Encryption Standard (AES), which provides strong and efficient protection for digital information.

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 05 Issue: 03 | Mar – 2026 DOI: 10.55041/ISJEM05769
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

2. BODY OF THE PAPER

2.1 RELATED WORK

Researchers have proposed various techniques to improve the security of digital communication using cryptography and steganography. Image steganography has been widely used to conceal confidential information within digital images, where methods such as Least Significant Bit (LSB) embedding allow data to be hidden without causing visible changes to the image. At the same time, encryption algorithms like the Advanced Encryption Standard (AES) are commonly applied to protect the content of the message by converting it into ciphertext. However, encryption alone does not hide the existence of the message. To overcome this limitation, recent approaches combine encryption with steganography, where the message is first encrypted and then embedded into an image. In addition, asymmetric encryption techniques such as RSA are used to securely transmit encryption keys between the sender and receiver. These hybrid approaches provide multiple layers of security by ensuring both confidentiality and concealment of the information, which forms the basis of the proposed system.

In recent developments, researchers have focused on improving the robustness and efficiency of steganographic techniques by optimizing embedding methods to reduce distortion in images. Some approaches aim to increase the data hiding capacity while maintaining image quality, ensuring that larger amounts of information can be embedded without detection. Other studies have explored adaptive steganography methods that select suitable pixel regions based on image characteristics to improve security. Additionally, combining advanced encryption algorithms with steganography has been shown to significantly reduce the risk of unauthorized access, even if the hidden data is detected. Researchers have also examined the use of secure key management techniques to prevent key exposure during communication. The integration of these methods enhances the reliability of secure communication systems. These findings highlight the importance of using hybrid security approaches that combine encryption, key protection, and data hiding techniques to achieve stronger protection against modern cyber threats.

2.2 SYSTEM DESIGN

The system is organized into a few core modules that work together to secure and hide sensitive information within images. Each module performs a specific task to ensure safe data transmission and accurate recovery.

• Input and User Interface Module:

This module allows the user to enter the secret message and choose the cover image. It acts as the starting point of the system and provides an easy way to interact with the application.

• AES Encryption Module:

The entered message is encrypted using the AES algorithm. This step converts readable text into protected ciphertext, ensuring that the data cannot be understood by unauthorized users.

• RSA Key Protection Module:

The AES encryption key is further secured using RSA encryption. This adds an extra layer of protection, making key exchange safe and reliable.

• Steganography Module (Embedding & Extraction):

The encrypted message is hidden inside the image using the LSB technique. At the receiver side, the same module extracts the hidden data from the image.

• Decryption Module:

The system first decrypts the AES key using RSA, and then uses the recovered key to decrypt the ciphertext. This process restores the original message accurately.

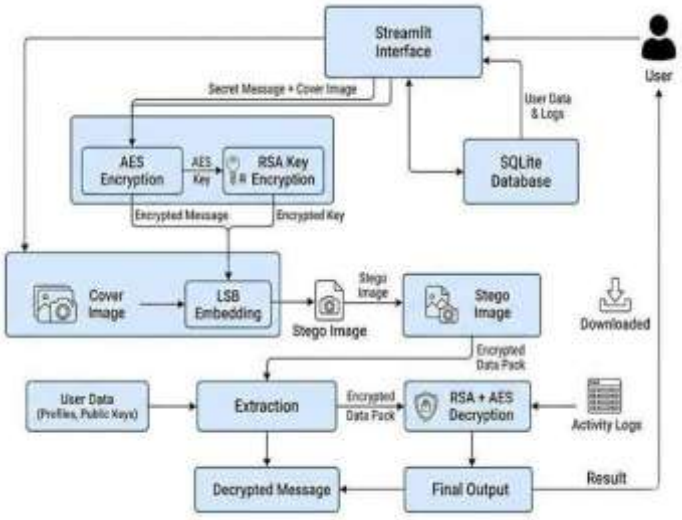

FIG.1. ARCHITECTURE DIAGRAM

Workflow :

1. The user enters a secret message and selects a cover image.The system prepares the input for further processing.

2. The message is encrypted using the AES algorithm.This converts the readable text into protected ciphertext.

3. A unique AES key is generated during encryption.This key is essential for later decryption.

4. The AES key is secured using RSA encryption.This ensures safe transmission of the key.

5. A suitable image is chosen as the carrier medium.It will be used to hide the encrypted data.

6. The encrypted message is embedded using LSB technique.The data is hidden inside image pixels without visible changes.

7. A stego image is created after embedding.It looks similar to the original image but contains hidden data.

8. The stego image is sent to the receiver.It can be shared through normal communication channels.

9. The receiver extracts the hidden encrypted data.The system retrieves the data using LSB extraction.

10. The message is decrypted using the AES key after RSA recovery.The original secret message is obtained successfully.

2.3 IMPLEMENTATION

The implementation of the proposed system focuses on securely hiding secret text inside digital images by combining encryption and steganography techniques. The system follows a structured process in which the message is first encrypted, then embedded into an image, and finally recovered at the receiver side. This approach ensures that the information remains confidential and concealed during transmission. The implementation is divided into the following stage.

A. User Input Module

The system begins by collecting the secret message and the cover image from the user.This module ensures that the input data is ready for secure

B. AES Encryption Module

The message is encrypted using the AES algorithm to convert into ciphertext.This protects the data from being understood by unauthorized users.

C. AES Key Generation.

During the encryption process, a unique secret key is generated automatically. This key is essential for both encryption and decryption, making it a critical part of the system.

D. RSA Key Protection Module

The generated AES key is secured using RSA encryption with the receiver's public key. This ensures that the key can only be accessed by the intended receiver using their private key.

E. Image Preparation Module

The selected cover image is processed to make it suitable for embedding. The system ensures that the image quality is preserved during the embedding operation.

F. LSB Embedding Module

The encrypted message is embedded into the image using the Least Significant Bit technique. This method hides the data within pixel values while keeping the image visually unchanged.

G. Stego Image Generation

After embedding, a new image is created that contains the hidden encrypted data. This stego image appears similar to the original image, making the hidden information difficult to detect.

H. Transmission Module

The stego image is transmitted to the receiver through normal communication channels. Since the image looks unchanged, it does not reveal the presence of hidden data.

I. Data Extraction Module

At the receiver side, the system extracts the embedded encrypted message from the stego image. The extraction process accurately retrieves the hidden data using the same LSB technique.

J. Decryption Module

The AES key is recovered using RSA decryption, and the encrypted message is then decrypted using AES. This final step restores the original secret message for the receiver.

2.4 RESULTS AND DISCUSSIONS

The proposed system was implemented to evaluate the effectiveness of combining encryption and steganography for secure communication. The system allows a user to hide confidential text information inside digital images while maintaining the visual quality of the original image. The experimental results demonstrate that the integration of AES encryption, RSA key protection, and LSB steganography provides a reliable and secure method for protecting sensitive information during transmission.

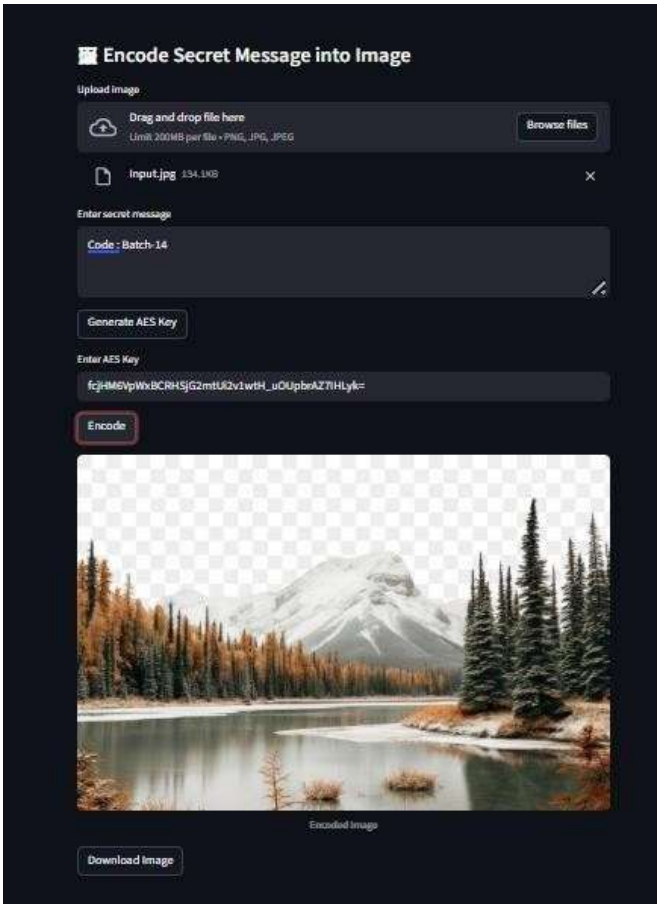

Fig.2: SECRET MESSAGE ENCODING INTERFACE

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 05 Issue: 03 | Mar – 2026 DOI: 10.55041/ISJEM05769
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

During the encoding process, the user first enters a secret message that needs to be protected. This message is encrypted using the Advanced Encryption Standard (AES) algorithm. AES converts the plaintext message into ciphertext, ensuring that the information cannot be easily understood by unauthorized users. The encryption process was tested with different text inputs, and in each case the ciphertext produced by the algorithm appeared completely unreadable without the proper key. This confirms that AES encryption successfully protects the content of the message before it is hidden.

To further enhance security, the AES key is encrypted using the RSA public key algorithm. RSA provides a secure mechanism for exchanging encryption keys between the sender and the receiver. In the implemented system, the AES key is encrypted using the receiver's public key before transmission. This ensures that only the receiver possessing the correct private key can recover the AES key. The results confirm that the RSA encryption and decryption processes function correctly and securely protect the key during communication.

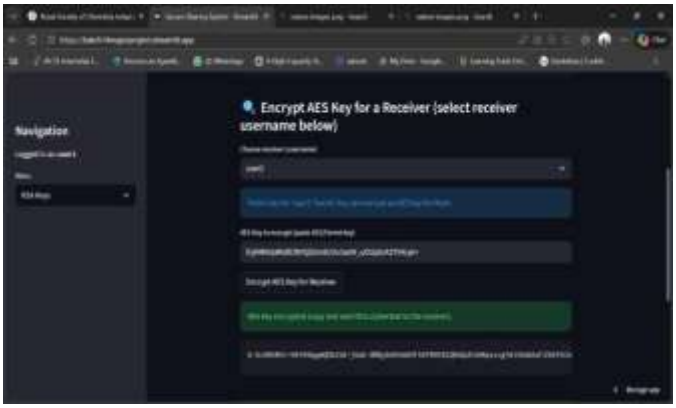

Fig.3: AES KEY ENCRYPTION INTERFACE

After encryption, the ciphertext is embedded into a digital image using the Least Significant Bit (LSB) steganography technique. This method modifies the least significant bits of the image pixels to store the encrypted data. Experimental testing shows that the embedding process does not significantly alter the appearance of the original image. The stego image produced after embedding appears visually identical to the cover image when viewed by the human eye. This indicates that the hidden data remains concealed and cannot be easily detected.

The system was tested using various image formats and different sizes of secret messages. In each case, the embedding process successfully stored the encrypted message within the image without noticeable distortion. The stego images retained their original color and structure, demonstrating that the LSB technique effectively preserves image quality while hiding data.

At the receiver side, the decoding process was performed to extract the hidden information from the stego image. The system reads the least significant bits of the image pixels and reconstructs the encrypted data. The extracted ciphertext was identical to the original encrypted message that had been embedded during the encoding process. This confirms that the LSB extraction process is reliable.

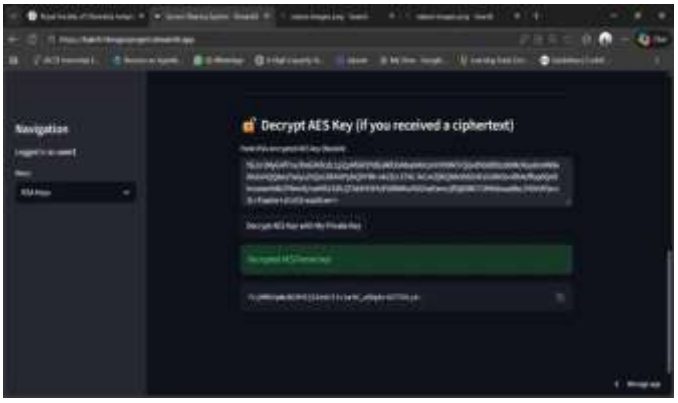

Fig.4: AES KEY DECRYPTION INTERFACE

Once the encrypted data is extracted, the receiver decrypts the AES key using the RSA private key. The successful recovery of the AES key allows the system to decrypt the ciphertext using the AES decryption algorithm. The decrypted output matches the original secret message entered by the sender. This confirms that the complete process of encryption, embedding, extraction, and decryption functions correctly without data loss.

The results demonstrate that the proposed system provides multiple layers of security. Even if an attacker suspects that data is hidden within the image, the encrypted message cannot be understood without the correct AES key. Additionally, the AES key itself is protected using RSA encryption, making unauthorized access even more difficult. This layered security approach significantly increases the protection of sensitive information.

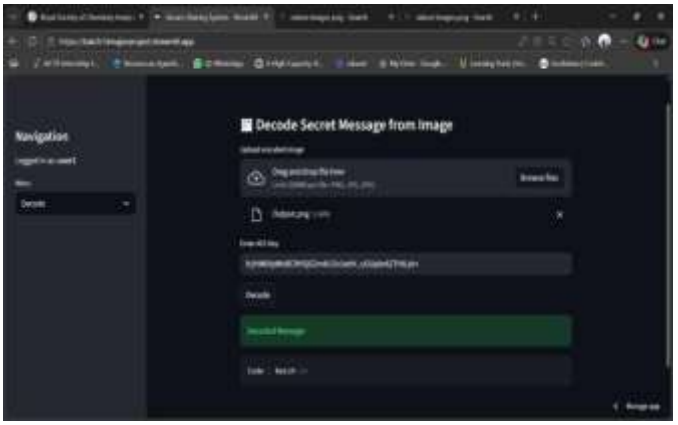

Fig.5: SECRET MESSAGE DECODING INTERFACE

Another important observation from the experimental analysis is the preservation of image quality after embedding.

Because the LSB technique modifies only the least significant bits of the image pixels, the visual difference between the cover image and the stego image is minimal. This characteristic ensures that the hidden data remains undetectable during normal viewing conditions.

The performance of the system also shows that the encryption and embedding operations can be performed efficiently without significant computational overhead. The system processes both small and moderate-sized text messages quickly, making it suitable for practical applications where secure communication is required.

Overall, the results confirm that the proposed approach successfully integrates cryptographic protection with steganographic data hiding. The combination of AES encryption, RSA key security, and LSB image steganography ensures confidentiality, secure key exchange, and concealment of information. The system demonstrates reliable performance, accurate data recovery, and effective protection of hidden communication.

The discussion of these results highlights the advantages of using a hybrid security model for protecting digital information. By combining encryption and steganography, the system ensures that the message content remains secure while also hiding its presence within an image. This approach significantly improves the overall security of digital communication systems and provides a practical solution for protecting confidential information in modern network environments.

3. CONCLUSION AND FUTURE WORK

The proposed system presents a reliable and secure approach for protecting confidential information by combining encryption and steganography techniques into a single framework. The use of AES encryption ensures that the original message is converted into a highly secure form, making it difficult for unauthorized users to interpret the data. In addition, the RSA algorithm provides a safe mechanism for protecting the encryption key, ensuring that only the intended receiver can access it. The LSB steganography method further strengthens the system by hiding the encrypted message within an image in such a way that the visual appearance remains almost unchanged. This dual protection strategy not only secures the content of the message but also conceals its existence, making it more resistant to potential attacks. The system demonstrates accurate performance in both embedding and extraction processes, ensuring that the original message is recovered without any loss of information. It also maintains a balance between security and efficiency, making it suitable for practical applications. Overall, the proposed solution offers a strong and effective method for secure communication and highlights the advantages of integrating multiple security techniques for better data protection.

In the future, the proposed system can be further enhanced by incorporating advanced techniques to improve its functionality and security. One possible improvement is the use of adaptive or intelligent steganography methods that can dynamically select optimal regions within an image for embedding data, thereby reducing the chances of detection. The system can also be strengthened by introducing more advanced encryption approaches such as multi-level or hybrid encryption to provide additional layers of protection. Future developments may include implementing dynamic key generation and secure key management systems to minimize the risk of key compromise. Expanding the system to support different types of media such as audio and video can increase its usability in a wider range of applications. Furthermore, integrating authentication mechanisms such as multi-factor verification can improve access control and prevent unauthorized use. Performance optimization can also be considered to handle larger data sizes and improve processing speed. The use of artificial intelligence techniques can be explored to enhance embedding efficiency and system intelligence. With these improvements, the system can evolve into a more advanced, flexible, and robust solution for secure data communication in modern digital environments.

REFERENCES

[1] J. Daemen and V. Rijmen, The Design of Rijndael: AES – The Advanced Encryption Standard. Springer, 2002.

[2] R. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” Communications of the ACM, vol. 21, no. 2, pp. 120–126, 1978.

[3] N. F. Johnson and S. Jajodia, “Exploring Steganography: Seeing the Unseen,” IEEE Computer, vol. 31, no. 2, pp. 26–34, 1998.

[4] N. F. Johnson, Z. Duric, and S. Jajodia, Information Hiding: Steganography and Watermarking – Attacks and Countermeasures. Kluwer Academic Publishers, 2001.

[5] J. Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge University Press, 2009.

[6] W. Stallings, Cryptography and Network Security: Principles and Practice. Pearson Education, 7th Edition, 2017.

[7] R. Chandramouli and N. Memon, “Analysis of LSB Based Image Steganography Techniques,” in Proceedings of IEEE International Conference on Image Processing, 2001.

[8] S. Katzenbeisser and F. A. P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, 2000.

[9] N. Provos and P. Honeyman, “Hide and Seek: An Introduction to Steganography,” IEEE Security & Privacy, vol. 1, no. 3, pp. 32–44, 2003.

[10] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, “Techniques for Data Hiding,” IBM Systems Journal, vol. 35, no. 3-4, pp. 313–336, 1996.

[11] J. Mielikainen, “LSB Matching Revisited,” IEEE Signal Processing Letters, vol. 13, no. 5, pp. 285–287,

2006.

[12] C. Cachin, "An Information-Theoretic Model for Steganography," in Information Hiding Workshop, Springer, 1998.

[13] K. Kaur and K. Singh, "A Study of Image Steganography Techniques," International Journal of Computer Applications, vol. 14, no. 4, pp. 1–5, 2011.

[14] A. Westfeld and A. Pfitzmann, "Attacks on Steganographic Systems," in Proceedings of the International Workshop on Information Hiding, Springer, 1999.

[15] A. Cheddad, J. Condell, K. Curran, and P. McKevitt, "Digital Image Steganography: Survey and Analysis of Current Methods," Signal Processing, vol. 90, no. 3, pp. 727–752, 2010.