International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 03 | March – 2025 DOI: 10.55041/ISJEM02520
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

Robust Data Security through Hybrid AES-RSA and LSB Steganography Techniques

M. Venkat Dass[1], L Raghavendar Raju[2]
[1]CSE, University college of Engineering, Osmania University
[2]CSE, Matrusri Engineering, Hyderabad

Abstract

In today's interconnected digital landscape, exchanging information and data has become integral to our daily lives. Steganography offers a unique approach to secure data communication by concealing sensitive information within seemingly innocuous digital content. However, traditional steganography methods also have their disadvantages. They can be susceptible to detection by advanced steganalysis techniques, and their compatibility with specific file formats can be limiting. This paper proposes Hybrid AES-RSA encrypted LSB, a two-layered approach to address the shortcomings of conventional steganography. This approach ensures that the information is well-hidden within digital content, while encryption provides an additional layer of protection to prevent unauthorized access. Our proposed method, Hybrid AES-RSA Encrypted LSB, achieves an SSIM (Structural Similarity Index Measure) index of 0.99 for images, The achieved accuracy of 97% is 13.25% higher than the traditional LSB method, underlining the effectiveness of our proposed hybrid technique.

Keywords*: Steganography, AES-RSA, LSB, SSIM, RMSE, MSE*

1. Introduction

Steganography dates back to ancient times when people used various methods to hide secret messages, such as invisible inks or messages within wax tablets. In the digital age, steganography techniques have evolved to exploit the characteristics of digital media. Digital steganography has gained prominence in recent decades, with the widespread use of digital media and the increased internet use for communication. The fundamental framework of steganography comprises three essential components:

1. **The Carrier Multimedia**: The carrier can take various forms, including digital images, text files, audio, or video, depending on the specific requirements and context of the steganography technique employed. It serves as the vessel for concealing the hidden message.
2. **The Message**: The secret information that needs to be concealed.
3. **The Key**: A key is employed for the purpose of decoding, deciphering, or unveiling the concealed message. This key is instrumental in the process of revealing the hidden information.

Digital files are binary data consisting of sequences of 0s and 1s. Steganographic techniques leverage the ability to subtly modify binary data in a way that does not noticeably affect the visible characteristics of the carrier media. The *Least Significant Bit (LSB)* substitution is the most popular steganographic approach. LSB refers to the lowest-order bit in a binary representation of a number. The core notion of LSB substitution entails embedding secret data in bits with the smallest weighting so that the value of the original

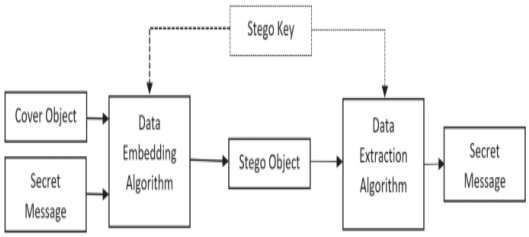

Fig. 1. Structure of Steganography system

pixel is unaffected. This subtle change is hard to detect visually but can be decoded with the right tools.

1.1 Types of Steganography

Steganography techniques can be categorized into distinct types based on the choice of cover media used to conceal the hidden data:

1. **Text Steganography**: Text is one of the oldest media choices for performing steganography. The abundance of textual information on the Internet has encouraged steganography to use this media as a carrier for hidden messages. This method primarily focuses on modifying text formatting or subtle alterations to specific attributes of textual elements, including characters and symbols.

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 03 | March – 2025 DOI: 10.55041/ISJEM02520
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

2. **Image Steganography**: In this approach, a message is concealed within an image without causing any noticeable visual changes to the image's overall appearance. Changes are typically made in pixels exhibiting significant color variations to minimize detectability.

3. **Audio Steganography**: Audio steganography involves covertly embedding digital data within audio files like MP3 or WAV.

4. **Video Steganography**: Video is a combination of pictures. Video Steganography is a technique of hiding data in a digital video file.

The selection of a steganography method depends upon the specific context and the nature of the data that needs to be concealed.
The primary objective of our proposal is to create a robust and secure solution for data communication by combining the approaches of encryption and the traditional LSB steganography algorithm. The hybrid AES-RSA encryption algorithm combines the strengths of both AES (Advanced Encryption Standard) and RSA (Rivest–Shamir–Adleman) encryption to achieve secure data communication. In this approach, AES is used for efficient bulk data encryption, making it well-suited for quickly encrypting large amounts of data. On the other hand, RSA is employed for secure key exchange, ensuring that the symmetric key used for AES encryption is safely distributed to the intended recipient. The hybrid AES-RSA encryption algorithm offers a practical and effective solution for data confidentiality and secure communication between parties.

2. Related Works

There are many advancements in the field of steganography, such as Samir Kumar et al. [14], who proposed a methodology for LSB modification and phase encoding techniques in audio steganography. The methodology involves segmentation of the original audio signal into smaller segments and applying *Discrete Fourier Transforms (DFT)* to each segment to obtain the phase spectrum. The secret message is then inserted into the *phase vector* of the first segment. The modified phase matrices are used to reconstruct the sound signal by applying inverse DFT and concatenating the segments with the original header.

Shilpa Gupta et al. [4] introduced the Enhanced LSB Algorithm for image steganography. This algorithm operates in the spatial domain, explicitly focusing on concealing information within the blue color component of the carrier image to minimize distortion and ensure imperceptibility to the human eye.

Pooja Yadav et al. [13] proposed a video steganography method that combines cryptography and steganography to hide a secret video stream within a cover video stream. The method involves encrypting each frame of the secret video using symmetric encryption. After encryption, sequential encoding is applied to embed the encrypted frames into the cover video.

Cheng Zeng, Jingbing, et al. [1] introduced a CNN-based color image steganography technique to conceal a secret image within a cover image of matching dimensions. This steganographic approach comprises two main components: the hiding network and the revealing network.

3. Hybrid AES-RSA Encrypted LSB

The entire process of Hybrid AES-RSA Encrypted LSB (Least Significant Bit) is shown in Fig 2. Steganography is a method used for hiding information within digital images while providing high security through encryption shown in Algorithm 1 and 2.

3.1 Encryption

The sender chooses the secret information that must be protected and transmitted securely.

1. **AES Encryption**: The sender generates a random symmetric AES key, and it is used to encrypt the secret information. AES encryption is efficient for encrypting large amounts of data.

2. **RSA Encryption**: The symmetric key is encrypted using the recipient's RSA public key.

The combination of these encryption algorithms ensures that the secret information is secure, as shown in Algorithm 1.

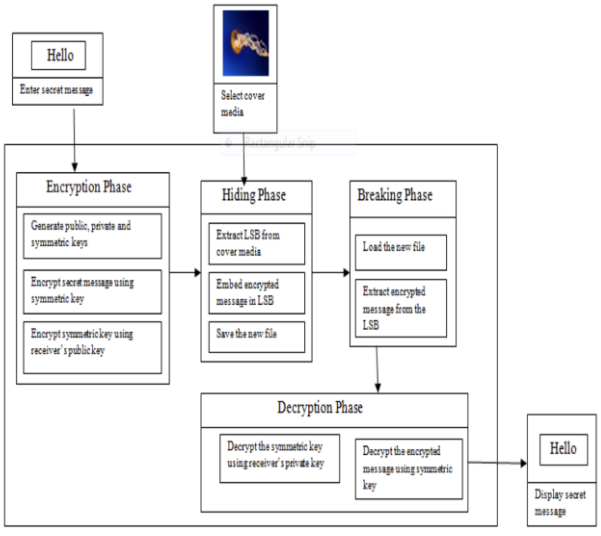

Fig. 2. System Architecture for Hybrid AES-RSA Encrypted LSB Steganography

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 03 | March – 2025 DOI: 10.55041/ISJEM02520
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

Algorithm 1. ***Hybrid AES-RSA Encryption***

Input: *Plain text, AES Symmetric key, RSA Public key*
Output: *Encrypted symmetric key, Cipher text*
Begin
def hybridEncrypt(data, symmetricKey, rsaPublicKey):
encryptedData = aesEncrypt(data, symmetricKey)
//Encrypt the original data using AES encryption
encryptedSymmetricKey = rsaEncrypt(symmetricKey, rsaPublicKey)
//Encrypt the symmetric key using RSA public key23
return(encryptedSymmetricKey, encryptedData)
// Return the encrypted symmetric key and the encrypted data
End Function

3.2 LSB Steganography

LSB refers to a technique where secret information is concealed by replacing the least significant bits of a carrier file with the bits of the hidden message. LSB steganography is a commonly used method for hiding data within digital media.

The sender selects an appropriate carrier file, which can be a text, image, audio, or video file. The carrier file acts as the container to hide the encrypted secret information. The selection of the carrier file dictates the category of steganography.

3.2.1 Image Steganography

Image steganography is a method that discreetly embeds data within images by manipulating the least significant bits (LSBs) of pixel channels. It involves sequentially altering the LSBs of the Red, Green, and Blue channels in an image with corresponding bits from an encrypted text message and adding a delimiter at the end of the message.

3.2.2 Text Steganography

Text steganography employs Zero Width Characters (ZWCs), specifically U+200B, to covertly conceal data within text files. ASCII values are modified during encoding, and binary representations are generated, allowing messages to be embedded using ZWCs.

3.3 Decryption and Extraction

The recipient receives the carrier file and performs the following steps to extract and decrypt the hidden message:

1. The receiver enters a combination of username and password, validated against the ones in the database. If they match, then the encrypted symmetric, public, and private keys are fetched from the database.

2. **RSA Decryption**: The recipient uses their private RSA key to decrypt the symmetric key, revealing the original one.

3. **Extraction of Hidden Data**: The recipient extracts the least significant bits from the carrier file to retrieve the encrypted secret information.

4. **AES Decryption**: The recipient uses the decrypted AES symmetric key to decrypt the encrypted secret information.

The decryption process is shown in Algorithm 2.

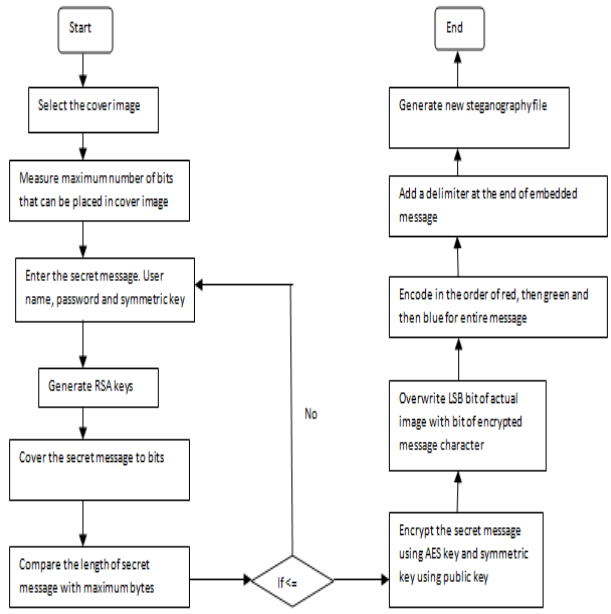

Fig. 3. Flowchart for Image Steganography

Algorithm 2. ***Hybrid AES-RSA Decryption***

Input*: Encrypted AES Symmetric Key, RSA Private Key, Cipher text*
Output*: Plain text*
Begin
defhybridDecrypt(encryptedSymmetricKey, rsaPrivateKey, encryptedData):
decryptedSymmetricKey = rsaDecrypt(encryptedSymmetricKey, rsaPrivateKey)
// Decrypt the encrypted symmetric key using RSA private key
decryptedData = aesDecrypt(encryptedData, decryptedSymmetricKey)
//Decrypt the cipher text using decrypted symmetric key
return decryptedData
// Return the decrypted data as the final result.
End

---

4. Empirical Assessment

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 03 | March – 2025 DOI: 10.55041/ISJEM02520
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

In evaluating the proposed model's performance, objective metrics such as PSNR (Peak Signal-to-Noise Ratio), MSE (Mean Square Error), SSIM (Structural Similarity Index), and RMSE (Root Mean Square Error) are employed. These objective metrics quantitatively measure the differences between the original and stego multimedia. They help assess the steganographic techniques' effectiveness in concealing information while minimizing the impact on the data's quality.

4.1 Experimental Setup

The chosen IDE for implementing AES-RSA Hybrid Encrypted LSB Steganography is PyCharm. It offers a conducive environment for developing and testing the steganographic system, allowing for efficient code development and debugging.

4.2 Results Analysis

This research implements the Least Significant Bit (LSB) steganography method for four types of multimedia files: text, images, audio, and video.

4.2.1 Image Steganography

The proposed approach guarantees both high embedding rates and robust security measures. Following the LSB method insertion, the stego image exhibits minimal perceptible differences from the original image. The size of the stego image remains unchanged, and the message extraction process is highly successful.

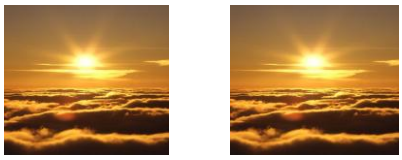

Fig. 3. Sun (a) Cover Image (b) Stego Image

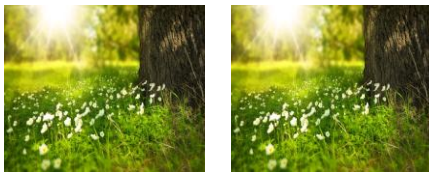

Fig. 4. Flowers (a) cover image
(b) stego image

Table 1 MSE, PSNR and SSIM values for the Original and Stego images

Cover image	Stego image	MSE (%)	PSNR (dB)	SSIM
Sun	Steg Sun	0.424	51.857	0.999
Flower	Steg Flower	0.431	51.689	0.997

In general, as the amount of data (payload) being embedded into an image increases, the Mean Squared Error between the original and modified image also tends to increase. This increase in MSE negatively impacts the Peak signal-to-noise ratio (PSNR), often expressed in logarithmic decibels (dB). Lower PSNR values, typically below 30 dB, indicate lower image quality, where distortions caused by the embedding process can be visibly apparent. Conversely, in the context of a high-quality stego-image, achieving a PSNR of 40 dB or higher is desirable.

Our research findings support that the embedding process introduces minimal perceptual distortion, leading to higher PSNR values. To quantify the distortion introduced during data embedding into the cover image, we measured the Peak signal-to-noise ratio (PSNR) for several images. We consistently observed PSNR values exceeding 51 dB, as shown in Table 2. This suggests that the quality degradations introduced by the embedding process are virtually imperceptible to the human eye[17].

In addition to PSNR, the Structural Similarity Index (SSIM) is a valuable metric for assessing image quality. High SSIM scores indicate a high degree of similarity between images and can further validate the minimal perceptual distortion observed in our results.

4.2.2 Text Steganography

Levenshtein distance is employed to assess the degree of similarity between two text documents. For the cover text file and generated stego file, the Levenshtein distance is 0 which indicates high similarity.

5. Discussions

5.1 Results Interpretation

Figure 5 and Table 2 compare the accuracy percentages achieved by traditional LSB and our proposed methodology. For Text data, the AES-RSA encrypted hybrid LSB method achieves an accuracy improvement of 5% to 9% compared to Traditional LSB.

Table 4 Result of Simulations

Methods	Accuracy			
	Text	Image	Audio	Video
Traditional LSB	90%-95%	80%-85%	70%-75%	75%-80%
AES-RSA encrypted hybrid LSB	95%-99%	96%-99%	90%-95%	90%-95%

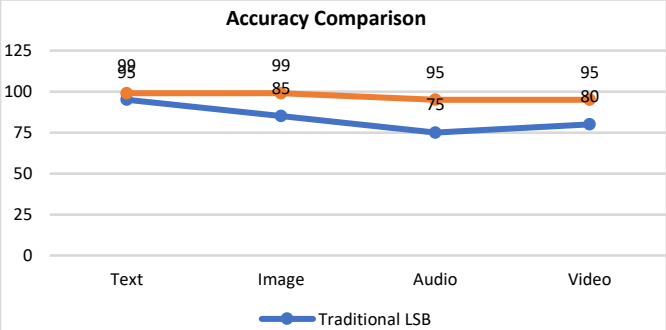

Fig. 5. Accuracy Comparison

Similarly, for Image data, the improvement is even more significant, with the hybrid approach showing an accuracy boost of 16% to 19% over Traditional LSB. The increase in accuracy for the AES-RSA encrypted hybrid LSB technique can be attributed to encryption and a hybrid approach.

6. Conclusion

Steganography is a powerful tool to secure data hiding and can be applied in various contexts. The proposed hybrid AES-RSA encrypted LSB steganography system represents a significant advancement in data security and covert communication. This innovative approach overcomes the limitations of traditional steganography methods and offers a robust solution for protecting sensitive information. Our proposed method, Hybrid AES-RSA Encrypted LSB, achieves an *SSIM (Structural Similarity Index Measure) index* of *0.9997* for images, *0.9973* for videos, and an *RMSE (Root Mean Square Error)* value of *0.000179* for audio files. The achieved accuracy of *97%* is 13.25% higher than that of the traditional LSB method, underlining the effectiveness of our proposed hybrid technique. By mitigating the constraints of conventional steganography and fortifying it with advanced encryption, this approach caters to the escalating demand for confidential and surreptitious data transmission within our progressively digitalized world.

References

[1] Cheng Zeng, Jingbing Li, Jingjun Zhou, and Saqib Ali Nawaz, "Color Image Steganography Scheme Based on Convolutional Neural Network", Advances in Artificial Intelligence and Security. ICAIS 2021.
[2] E. Abdelfattah, R. J. Mstafa, and K. M. Elleithy, "A robust and secure video steganography method in DWT-DCT domains based on multiple object tracking and ECC," IEEE Access, vol. 5, pp. 5354-5365, 2017.
[3] G. Fu, H. Shi, S. Wang, X.-Y. Zhang, and J. Tang, "Synchronized detection and recovery of steganographic messages with adversarial learning," Proc. Int. Conf. Comput. Sci, pp. 31-43, 2019.
[4] G. Gujral, S. Gupta, and N. Aggarwal, "Enhanced least significant bit algorithm for image steganography," Proc. Int. J. Comput. Eng. Manage., vol. 15, no. 4, pp. 40-42, 2012.
[5] I. Aljazaery, and M. Aziz, "Combination of hiding and encryption for data security," hj,hk., vol. 10, no. 15, pp. 10-20, 2020.
[6] Huwaida T. Elshoush, Mahmoud M.& Abdelrahman Atigani, ""A new high capacity and secure image realization steganography based on ASCII code matching., 2022.
[7] Khare, P., Singh, J. and Tiwari, "Digital Image Steganography", Journal of Engineering Research and Studies, Vol. II, Issue III, pp. 101-104, 2011.
[8] K. Ibrahim Mohammad Abuzanouneh and M. Hadwan' Multi-Stage Protection using Pixel Selection Technique for Enhancing Steganography', International Journal of Communication Networks and Information Security (IJCNIS), 2021
[9] Laskar, S.A. and Hemachandran, "An Analysis of Steganography and Steganalysis Techniques", Assam University Journal of Science and Technology, Vol.9, No.II, pp.83-103, 2012.
[10] M. H. Abd, "Dynamic Data Replication for Higher Availability and Security," Wasit Journal of Computer and Mathematics Sciences, pp. 31-42, 2021.
[11] N. F. Hordri, S. S. Yuhaniz, and S. M. Shamsuddin, "Deep learning and its applications: A review," Proc. Conf. Postgraduate Annu. Res. Informat. Seminar, pp. 1-6, 2016.
[12] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," Computer, vol. 31, no. 2, pp. 26-34, Feb. 1998.
[13] Petitcolas, F.A.P., Anderson, R. J. and Kuhn, M.G. (1999) "Information Hiding -A Survey", Proceedings of the IEEE, Special issue on Protection of Multimedia Content, vol. 87, no. 7, pp.1062- 1078.
[14] Pooja Yadav, Nishchol Mishra, Sanjeev Sharma, "A secure video steganography with encryption based on LSB technique", IEEE, 2013.
[15] Samir Kumar, BandyopadhyayBarnali, Gupta Banik, "LSB Modification and Phase Encoding Technique of Audio Steganography Revisited", IJARCCE, 2012.
[16] Sokouti, M., Sokouti, and Pashazadeh, "An approach in improving transposition cipher system", Indian Journal of Science and Technology, Vol.2 No. 8, pp. 9-15, 2009.
[17] Stuti Goel, Arun Rana & Manpreet Kaur., "A Review of Comparison Techniques of Image Steganography", IJCTT, 2013, Vol. 13(4).
[18] Ulutas and Nabiyev, "Distortion free geometry based secret image sharing", Elsevier Inc, Procedia Computer Science 3, pp.721--726, 2011.
[19] Zhou, X., Gong, W., Fu, W., & Jin, L. "An improved method for LSB based color image steganography combined with cryptography", IEEE, 2016.