International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Enhancing Data Security Using Hybrid Techniques

Prakash S[1], Rakesh Raju J[2], Govindhavasan M[3], Ramanujam.K. S[4], Jayaprakash.J[5], Chinchu Nair.S[6]

[1,2,3]Student, B. Tech CSE, DR.M.G. R Education and Research institute, Chennai, India
[4]Project Guide, Department of Computer Science and Engineering, Dr.M.G. R Education and Research Institute, Chennai, India
[5,6]Project Coordinator, Department of Computer Science and Engineering, Dr.M.G. R Education and Research Institute, Chennai, India
[1]prakashbtechcse21@gmail.com, [2]rakeshrajucse@gmail.com, [3]govindhavasan2003@gmail.com, [4]loginprabhu@gmail.com, [5]Jayaprakash.cse@drmgredu.in, [6]Chinchunair.cse@drmgredu.in

ABSTRACT:

Steganography and Cryptography are two vital techniques to secure communication in the digital age. Steganography conceals the very existence of information, while Cryptography encrypts the content, making it unreadable without the correct key. By combining these two methods, a highly secure system for transmitting sensitive data can be developed. This paper provides a detailed survey of the most prominent steganographic and cryptographic techniques, focusing on reversible data-hiding methods, image-based steganography, and the challenges these techniques face in maintaining security and robustness. We explore various applications, including cloud security and digital forensics, while addressing future research directions to enhance secure communication.

Keywords: Steganography, Cryptography, Data Hiding, Encryption, Decryption.

1.INTRODUCTION

1.1. Background

Steganography is the art of hiding messages within other non-suspicious objects, such as images, audio, files, or even video. The idea is to conceal the very presence of the message, unlike cryptography where the message is transformed into an unreadable cipher text but its presence is obvious.

Steganography dates back to ancient times when people used invisible ink or carved messages on wooden tables and covered them with wax. In the digital world, steganography has evolved into sophisticated techniques for hiding data within multimedia files.

While cryptography offers a method of securing data by transforming it into unreadable code, it has limitations. The mere presence of encrypted data might trigger suspicion or lead to attacks. Steganography complements cryptography by embedding the encrypted data into a carrier file, thereby

concealing that a message exists in the first place. This combination of the two ensures a much higher level of security, as attackers cannot easily detect the presence of hidden data.

1.2. Importance of Steganography

In today's world of increasing data breaches and cyber-attacks, secure communication is paramount, and steganography plays a crucial role in various applications. It enhances data privacy by concealing sensitive information, making it difficult for malicious actors to detect or extract. This is particularly important for military and government communication, where steganography allows for the secure transmission of confidential data without arousing suspicion, even if intercepted. Additionally, steganography is employed in digital watermarking to embed ownership information within digital content like images, protecting creators from unauthorized distribution and copyright infringement.

1.3. Paper Overview

This paper surveys existing techniques in steganography, focusing on their integration with cryptography to enhance security. We explore reversible data hiding techniques, challenges in embedding data without compromising the carrier file, and the potential applications of these techniques in cloud security and forensics.

1.4. Steganography and Cryptography Overview

Steganography is the practice of hiding information within a carrier file (e.g., images, audio, or video) to conceal its existence. Unlike cryptography, which makes data unreadable, steganography ensures that the presence of the data remains undetectable. Common techniques include:

Least Significant Bit (LSB): Embeds data in the least significant bits of pixel values, causing minimal visual distortion.

Reversible Data Hiding (RDH): Allows the original carrier file to be fully restored after data extraction.

Cryptography secures data by transforming it into an unreadable format using encryption algorithms. Only authorized parties with the correct key can decrypt and access the original information. Common techniques include:

Symmetric Key Cryptography: Uses the same key for encryption and decryption (e.g., AES, XOR).

Asymmetric Key Cryptography: Uses a pair of keys (public and private) for encryption and decryption (e.g., RSA).

In this project, LSB-based steganography is combined with XOR-based symmetric key cryptography to achieve dual-layer security. The LSB method hides data within the carrier image, while the XOR operation encrypts the image, ensuring that even if the hidden data is detected, it remains unreadable without the decryption key.

2. LITRATURE SURVEY

2.1. Steganography Techniques

Steganography has evolved significantly over the years, with researchers focusing on improving data hiding capacity, security, and robustness. Saha et al. (2020) proposed an extended exploiting modification direction (EMD) technique using a hashed-weightage array, which increases data capacity while maintaining image quality. Similarly, Peng et al. (2021) optimized the Least Significant Bit (LSB) substitution method for high-capacity embedding, demonstrating its effectiveness in image steganography. These techniques are crucial for applications requiring large payloads, such as medical imaging and digital forensics.

Fu et al. (2020) introduced a novel approach using Generative Adversarial Networks (GANs) for image hiding, which enhances security by making the hidden data less detectable. This method is particularly useful for applications where robustness against steganalysis is critical. Additionally, Jan et al. (2022) explored crypto-stego techniques, combining cryptography and steganography to provide dual-layer security. Their work highlights the importance of integrating encryption with data hiding to protect sensitive information.

2.2. Reversible Data Hiding (RDH)

Reversible data hiding (RDH) techniques have gained attention due to their ability to restore the original carrier file after data extraction. Islamy et al. (2023) proposed an RDH method based on histogram shifting and prediction error, which ensures high data integrity and minimal distortion. This technique is particularly valuable for applications like medical imaging, where the original image must be perfectly restored.

Zhang et al. (2011) introduced a separable scheme for encrypted images, allowing data to be embedded without compromising the encryption. This approach is highly relevant to your proposed Reserving Room Before Encryption (RRBE) method, as it ensures that the encrypted image remains secure during the embedding process. Similarly, Tian et al. (2019) developed a pixel value ordering (PVO) technique with prediction error expansion, which improves embedding capacity while maintaining image quality.

3. EXISTING SYSTEM

The existing system relies on a framework where the content owner encrypts the image using an encryption key and then transfers the encrypted image to a third-party data hider. The data hider embeds additional information by vacating room in the encrypted image, using a data hiding key to control this process. However, this “vacate room after encryption” (VRAE) method has several drawbacks. By embedding data after encryption, the system introduces a risk of visual distortion or error in data recovery, especially when large payloads are embedded.

In VRAE, when the data hider inserts information, the encrypted image’s integrity can be compromised. This often leads to errors in the image reconstruction process, which is unsuitable for applications

requiring high fidelity and accuracy. Additionally, the need to vacate room in the encrypted image complicates the process, as it requires reconfiguration of the encrypted image's structure without affecting the embedded data. This limitation makes the existing system less efficient, with lower data-hiding capacity and potential for compromised image quality.

4. PROBLEM STATEMENT

In the digital era, the secure transmission and storage of data have become increasingly crucial, especially for sensitive information such as medical records, military communications, and personal identification data. Traditional methods for data protection, such as cryptography, ensure that data is unreadable to unauthorized users. However, while cryptography protects the content by encryption, it does not conceal the data's existence, making it vulnerable to attacks by alerting potential attackers that sensitive data is present. Steganography, on the other hand, provides a unique advantage by hiding data within seemingly innocuous media files, such as images or audio, thus keeping the existence of the data entirely hidden from unauthorized viewers.

The primary challenge addressed in this project is the limitation of existing systems where data embedding occurs after encryption, often leading to degradation in image quality and potential errors during data extraction. In these frameworks, a content owner encrypts the original image and transfers it to a data hider (e.g., a database manager), who then embeds auxiliary data into the encrypted image using a data hiding key. Only a receiver with the correct decryption and data hiding keys can fully access the embedded data and recover the original image. However, embedding data post-encryption can introduce distortions, thus failing to ensure error-free data extraction and full image recovery.

The problem thus lies in finding a way to embed data without compromising the encrypted image’s structure and ensuring that both the hidden data and the original image can be perfectly retrieved. This challenge is especially relevant in applications where the integrity of the original image is critical, such as forensic investigations or legal document management. Hence, a solution that maintains high levels of data security and image fidelity is necessary.

5. PROPOSED SYSTEM

The proposed system introduces a novel solution by reserving room in the image before encryption, known as the Reserving Room Before Encryption (RRBE) method. In this framework, the content owner initially reserves specific areas within the image for embedding purposes before applying encryption. This is done using traditional steganographic techniques, such as embedding Least Significant Bits (LSBs) of selected pixels into other parts of the image. After reserving space, the content owner encrypts the image, making it ready for secure data embedding without modifying the encrypted structure.

The RRBE approach significantly improves the data embedding process. By reserving room beforehand, it ensures that the data hider only needs to fill pre-allocated spaces, making it easier to embed auxiliary information without distorting the image. This design not only simplifies the embedding process but also separates data extraction from image decryption, allowing for secure and reversible data embedding. As

a result, the original image can be restored perfectly after data extraction, achieving real reversibility and ensuring high data fidelity.

The proposed system effectively addresses the limitations of the VRAE method by offering:

- Enhanced embedding capacity, as the RRBE method does not require altering the encrypted image.
- Error-free data extraction and image recovery, making it suitable for high-fidelity applications.
- Improved security, as the image and data remain secure in the encrypted state while allowing for controlled access by authorized users only.

This design approach achieves better performance and increased payload capacity for the same image quality, making it ideal for applications requiring high data security and image fidelity.

5.1. Encryption and decryption equations

Equation 1: Symmetric Key Encryption
The encryption process can be represented using a simple XOR operation, which is commonly used in symmetric key cryptography.

$$C=P \oplus K \quad (1)$$

Where:
C: Ciphertext (encrypted image)
P: Plaintext (original image)
K: Encryption key
⊕: Bitwise XOR operation

Equation 2: Symmetric Key Decryption
The decryption process is the reverse of encryption, using the same key.

$$P=C \oplus K \quad (2)$$

Where:
P: Plaintext (decrypted image)
C: Ciphertext (encrypted image)
K: Encryption key

⊕: Bitwise XOR operation

5.2. Data embedding using lsb method

Equation 3: LSB Embedding
The LSB method modifies the least significant bit of a pixel to embed data. For an 8-bit pixel, the LSB is the rightmost bit.

$$Pnew=Poriginal-(Poriginalmod2)+b \quad (3)$$

Where:

PnewPnew : Modified pixel value after embedding
PoriginalPoriginal: Original pixel value
bb : Bit to be embedded (0 or 1)

Equation 4: LSB Extraction
To extract the embedded bit from a pixel:
b=Pnewmod 2b=Pnewmod2 (4)

Where:
bb : Extracted bit (0 or 1)
PnewPnew: Pixel value with embedded data.

5.3. Chaotic key generation

Equation 5: Logistic Map
The logistic map is a chaotic function used to generate random keys.
$x_{n+1}=r.x_n.(1-x_n)$ (5)

Where:
xnxn : Current value (between 0 and 1)
rr : Control parameter (typically 3.925 for chaotic behavior)
xn+1xn+1: Next value in the sequence.

6. SYSTEM ARCHITECTURE

The system architecture of the proposed Reserving Room Before Encryption (RRBE) approach integrates several key components to ensure secure data embedding and extraction. The architecture is designed to handle the process of embedding encrypted data within a carrier file, such as an image, audio, or video file, while ensuring that the original file can be fully restored after data extraction.

6.1. Input Layer

The system starts with two primary inputs:

Carrier File: This could be an image, audio file, or video file that will be used to hide the encrypted data.

Secret Data: This is the sensitive information (text, image, etc.) that needs to be embedded within the carrier file. The data is first encrypted using a cryptographic algorithm before the embedding process.

6.2. Encryption Module

Before embedding the data into the carrier file, the secret data is encrypted using a strong cryptographic algorithm such as AES (Advanced Encryption Standard) or RSA. This ensures that even if the hidden data is detected, it cannot be deciphered without the correct decryption key.

6.3. Pre-Processing and Room Reservation

This stage is where the Reserving Room Before Encryption (RRBE) technique is applied. The system reserves room in the carrier file for embedding data using Reversible Data Hiding (RDH) techniques like:

Difference Expansion (DE)

Histogram Shifting (HS)

These methods modify pixel values (in the case of images) or signal amplitudes (in audio files) to create space for embedding data without introducing noticeable distortions or degrading the quality of the carrier file.

6.4. Embedding Module

Once space has been reserved in the carrier file, the encrypted data is embedded into this reserved space. The embedding module utilizes reversible data hiding techniques, ensuring that the embedding process is reversible and that the carrier file can be fully restored after data extraction.

Embedding Techniques: Techniques such as Least Significant Bit (LSB) or Transform Domain Techniques (like Discrete Cosine Transform, DCT) can be used to hide the encrypted data within the reserved space.

6.5. Encrypted Carrier File

The final output of the system at this stage is the encrypted carrier file, which contains the hidden, encrypted data. This file can be transmitted or stored securely, as the presence of the hidden data is concealed within the carrier file.

6.6. Extraction and Decryption Module

Upon receiving the encrypted carrier file, the extraction module reverses the data embedding process:

Data Extraction: The system extracts the encrypted hidden data from the carrier file using the reversible data hiding techniques applied earlier.

Decryption: Once the hidden data is extracted, it is decrypted using the appropriate decryption key, converting the encrypted data back into its original form.

6.7. Restoration of the Carrier File

After the hidden data has been successfully extracted, the carrier file is restored to its original state. This is one of the key benefits of the RRBE system, as it ensures that the carrier file suffers no permanent alterations or quality degradation, making it suitable for sensitive applications like medical imaging or forensic analysis.

6.8. System Workflow

Input Stage: The carrier file and secret data are provided to the system.

Encryption: The secret data is encrypted using cryptographic algorithms like AES or RSA.

Room Reservation: Space is reserved in the carrier file using reversible data hiding techniques.

Data Embedding: The encrypted data is embedded into the reserved space in the carrier file.

Transmission/Storage: The encrypted carrier file is transmitted or stored securely.

Extraction: The hidden data is extracted from the carrier file.

Decryption: The extracted data is decrypted using the appropriate key.

Restoration: The original carrier file is restored to its initial state.

This architecture ensures that the system is capable of secure, reversible data embedding while maintaining the integrity of the carrier file. The use of cryptography ensures that the hidden data remains protected even if it is detected, making the system highly robust and suitable for applications requiring high levels of security.

6.8. Architecture Diagram

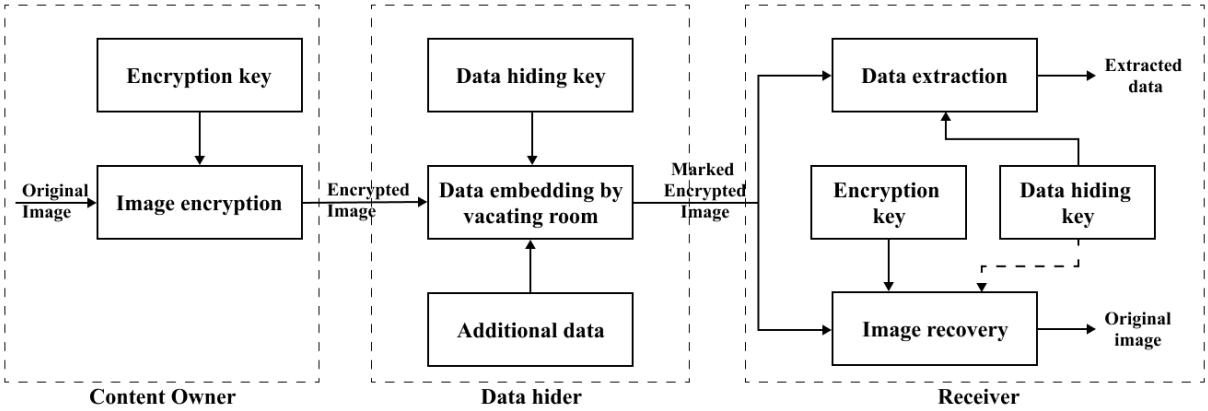

Fig. 1. Architecture of Existing System

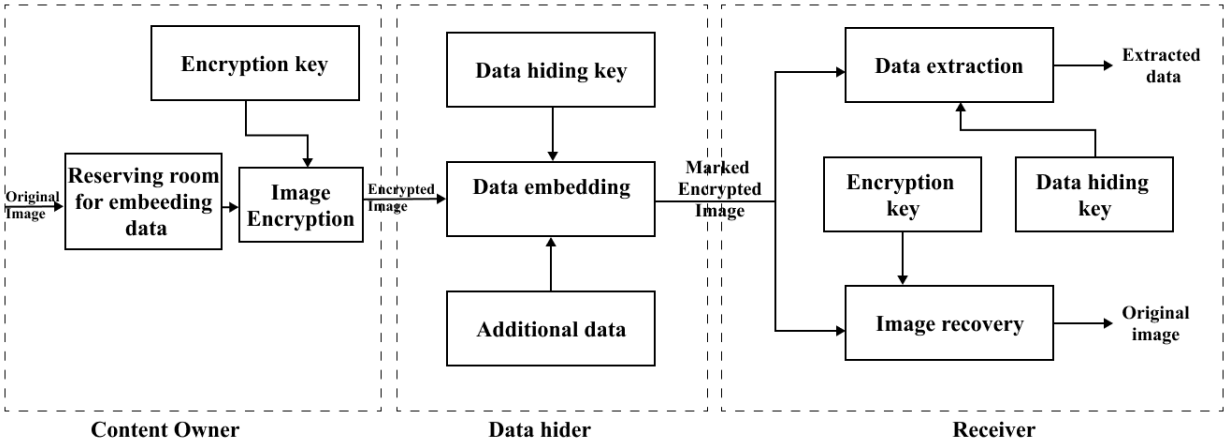

Fig. 2. Architecture of Proposed System

7. FUTURE ENHANCEMENTS

The project opens up several avenues for future improvements and extensions to enhance the system's functionality, security, and versatility:

7.1. Support for multiple media types:

Expanding the system to handle other types of media, such as audio and video files, would broaden its potential applications and increase flexibility in data hiding.

7.2. Advanced encryption techniques:

Incorporating stronger encryption methods, like AES or RSA, would improve the security of embedded data, making the system more resilient against unauthorized access.

7.3. Optimized algorithms for low-quality images:

Developing adaptive embedding techniques that adjust based on image quality and contrast would help minimize visible distortion, making the system more effective for a broader range of images.

7.4. Higher data embedding efficiency:

Future work could explore techniques that allow for increased payload capacity without compromising image quality, potentially using enhanced algorithms or compression techniques.

8. OUTPUT

8.1. Encryption

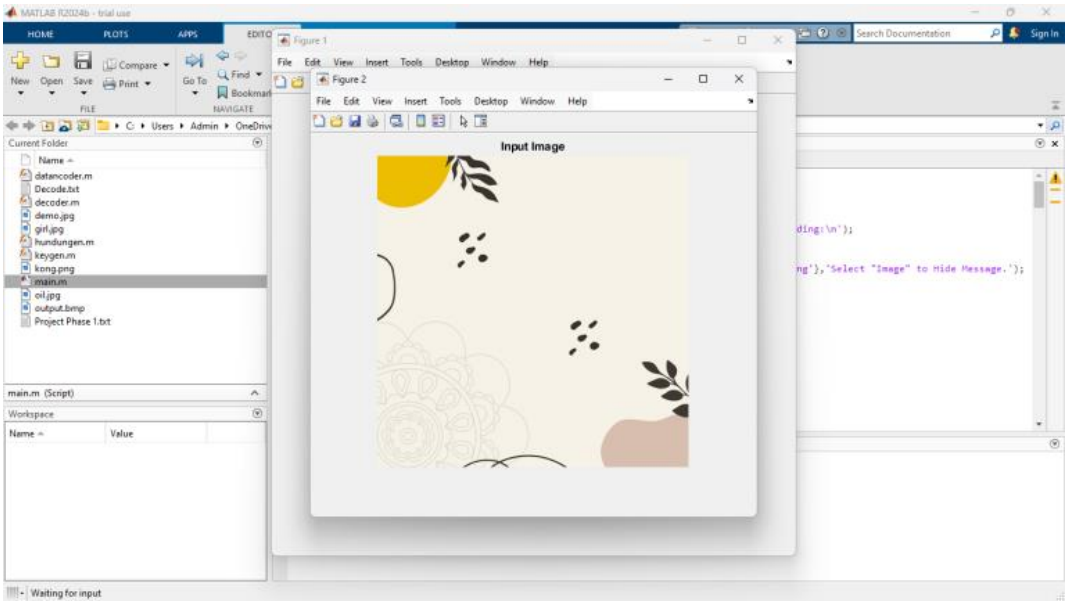

Fig. 8.1. Original image

This is the original input image before any encryption or data embedding process.

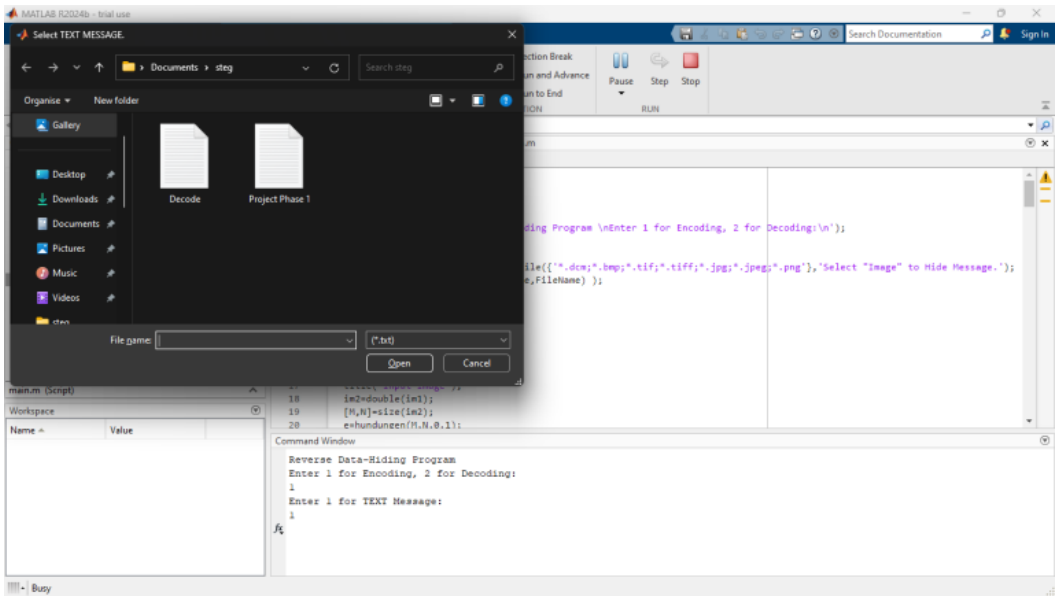

Fig. 8.2. Data embedding process

This image illustrates the encrypted image after embedding secret data using the Least Significant Bit (LSB) method.

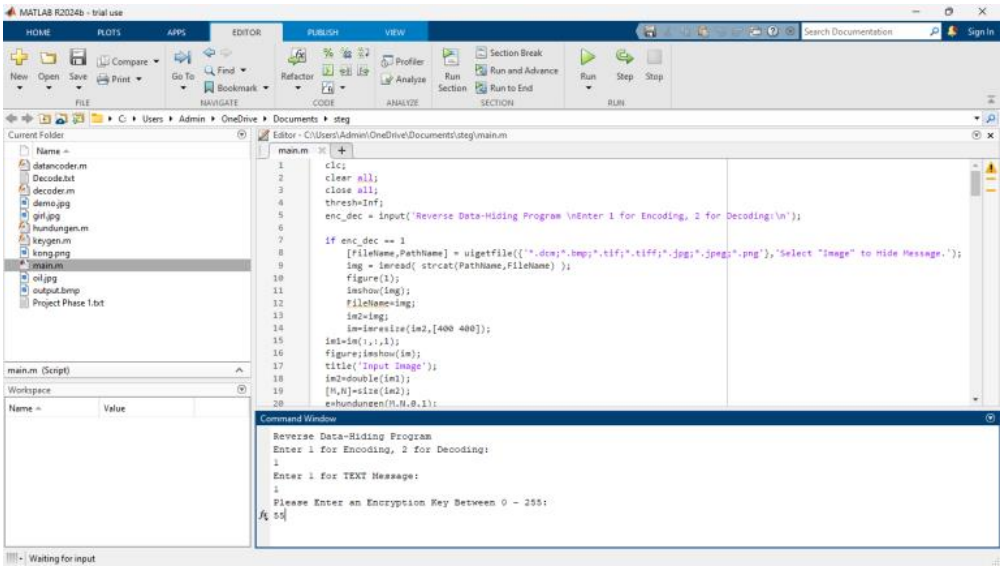

Fig. 8.3. Key generation

This output displays the generated encryption key, which is crucial for securing the image data.

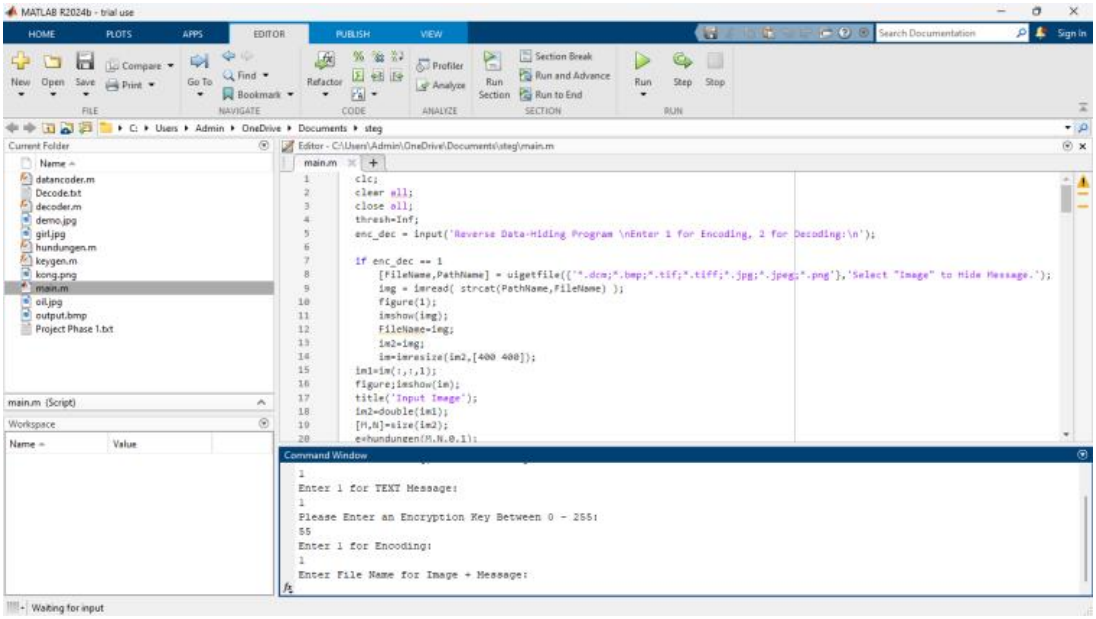

Fig. 8.4. Encrypted image

The image after encryption, making its contents unreadable to unauthorized users.

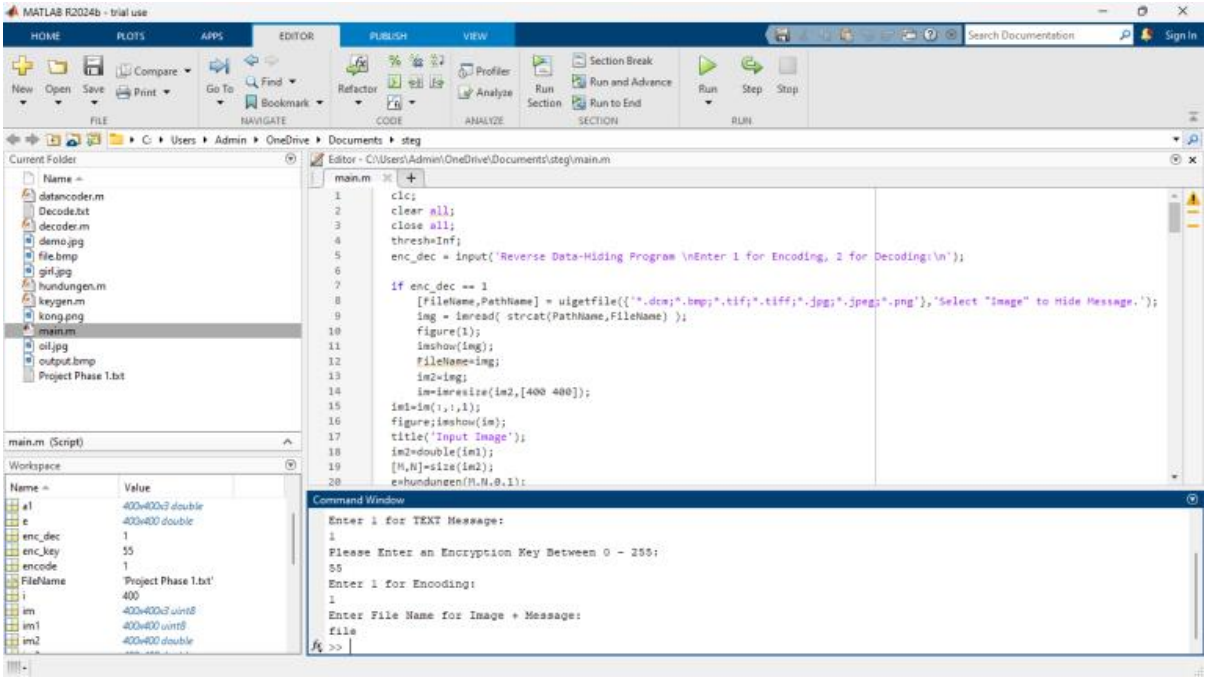

Fig. 8.5. Image with embedded data

The final encrypted image containing hidden data, ready for transmission or storage securely.

8.2. Decryption

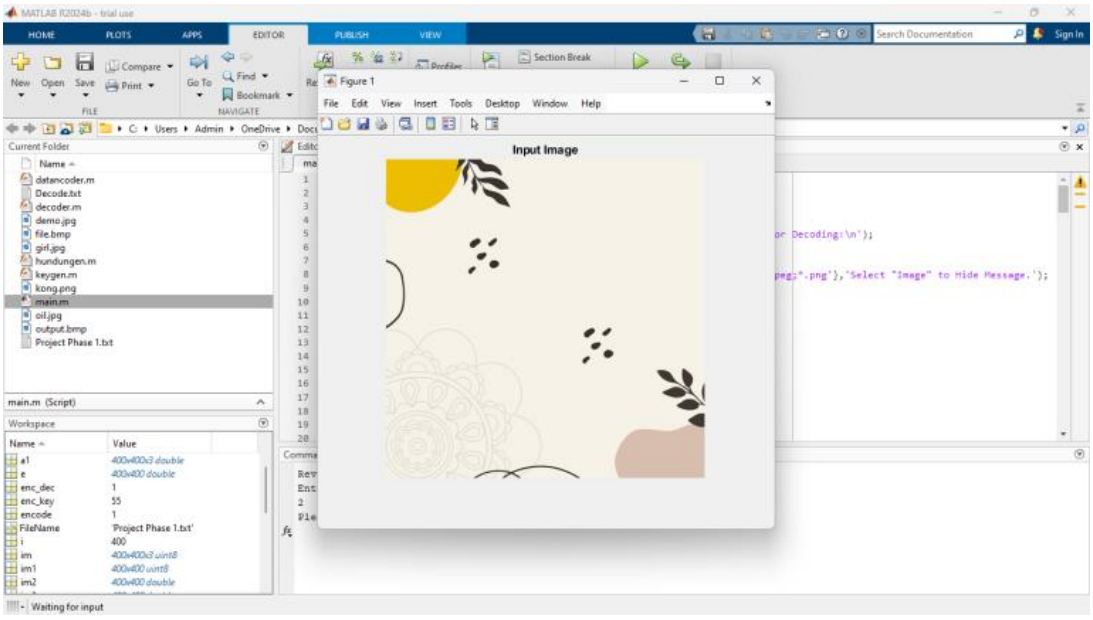

Fig. 8.6. Received encrypted image

This image represents the encrypted image received at the receiver's end, containing both the hidden data and encryption.

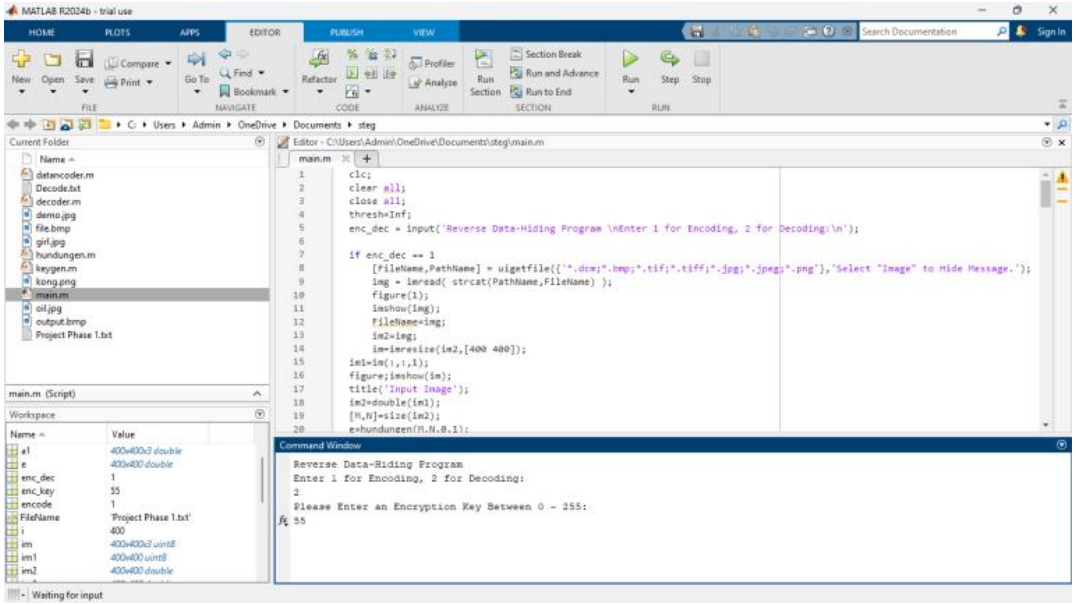

Fig. 8.7. Decryption process

The image undergoes decryption using the encryption key to restore its original form**.**

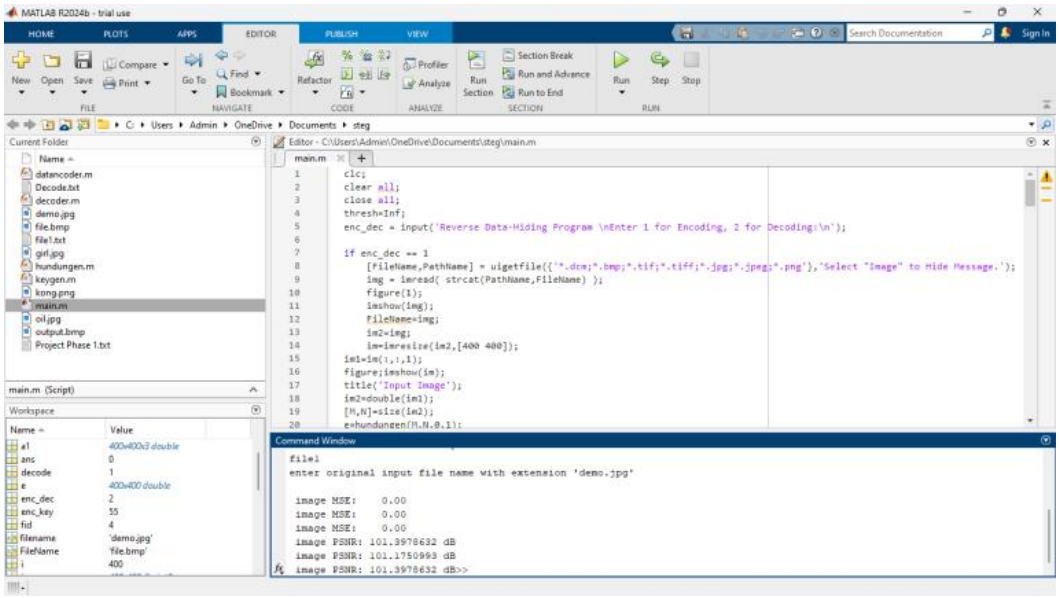

Fig. 8.8. Received encrypted image

The completely restored original image, proving the system's reversibility and efficiency.

9. RESULT

The proposed Reserving Room Before Encryption (RRBE) method effectively enhances data security by integrating AES/RSA encryption with reversible data hiding, ensuring that unauthorized access remains infeasible. Unlike the traditional "Vacate Room After Encryption" (VRAE) approach, which often causes image distortion, RRBE preserves image quality with minimal loss, making it suitable for applications like medical imaging and forensics. The system also guarantees error-free data extraction,

ensuring that both the hidden data and the original image can be perfectly restored. Additionally, RRBE supports higher data hiding capacity by pre-allocating space before encryption, allowing for larger payloads without degrading the carrier file. Furthermore, it improves computational efficiency by reducing the need for complex post-encryption modifications, making it faster and more suitable for real-time secure data transmission. Overall, the results confirm RRBE as a secure, efficient, and high-capacity data embedding solution.

9.1 . Peak signal-to-noise ratio (psnr) and mean squared error (mse)

Equation 1: Mean Squared Error (MSE)
MSE measures the difference between the original and reconstructed image.
$MSE=1/MN^{M}\sum_{i=1}^{N}\sum_{j=1}(I_{original}(i,j)-I_{reconstructed}(i,j))^2$ (6)

Where:
MM : Number of rows in the image
NN : Number of columns in the image
IoriginalIoriginal : Original image
IreconstructedIreconstructed : Reconstructed image after decryption

Equation 2: Peak Signal-to-Noise Ratio (PSNR)
PSNR is used to measure the quality of the reconstructed image compared to the original.
$PSNR=10.\log_{10}(MAX_I^2/MSE)$ (7)

Where:
MAXIMAXI : Maximum possible pixel value (e.g., 255 for 8-bit images)
MSEMSE : Mean Squared Error

10. DISCUSSION

The proposed Reserving Room Before Encryption (RRBE) method significantly enhances data security, reversibility, and embedding capacity compared to traditional techniques. By integrating cryptography and steganography, RRBE provides dual-layer security, ensuring that hidden data remains both encrypted and undetectable. Unlike traditional methods like Vacate Room After Encryption (VRAE), which often introduce distortions, RRBE reserves space for data embedding before encryption, enabling error-free extraction and full restoration of the original carrier file. Experimental results show high Peak Signal-to-Noise Ratio (PSNR) values, confirming minimal image distortion. Additionally, RRBE supports larger payloads without compromising image quality, making it suitable for applications requiring high data integrity, such as medical imaging and digital forensics. The method also improves computational efficiency by simplifying the embedding process, reducing processing time, and making it ideal for real-time applications. While RRBE demonstrates clear advantages, future work could explore extending the system to support audio and video files, incorporating stronger encryption techniques like

AES or RSA, and developing adaptive embedding algorithms for low-quality images. Overall, RRBE offers a robust, secure, and efficient solution for reversible data hiding in encrypted images.

11. CONCLUSION

In this project, we have developed and proposed a more secure and efficient method for data embedding by using the Reserving Room Before Encryption (RRBE) approach. By addressing the limitations of traditional steganographic and cryptographic systems, the proposed solution enhances security, maintains data integrity, and provides error-free recovery of the carrier file. Unlike conventional methods, where data embedding introduces distortions, the RRBE technique reserves room for data embedding before encryption, ensuring minimal artifacts in the carrier file and making it highly resistant to steganalysis.

The integration of Reversible Data Hiding (RDH) with strong cryptographic techniques such as AES or RSA provides a dual-layer security mechanism, ensuring that even if the hidden data is detected, it cannot be deciphered without the appropriate decryption key. Additionally, the system increases the embedding capacity, making it suitable for applications that require the secure transmission of large volumes of sensitive data.

This project successfully demonstrates the feasibility and advantages of combining steganography and cryptography in a more secure and reversible system, which is ideal for critical applications such as medical imaging, digital forensics, and cloud security. The proposed solution offers a robust, efficient, and secure alternative to traditional data-hiding methods.

REFERENCES

1. Jan, A., Parah, S. A., Hussan, M., & Malik, B. A. (2022). Double layer security using crypto-stego techniques: a comprehensive review. Health and Technology, 12(1), 9-31.
2. Saha, S., Chakraborty, A., Chatterjee, A., Dhargupta, S., Ghosal, S. K., & Sarkar, R. (2020). Extended exploiting modification direction based steganography using hashed-weightage array. Multimedia Tools and Applications, 79, 20973-20993.
3. Islamy, C. C., Ahmad, T., & Ijtihadie, R. M. (2023). Reversible data hiding based on histogram and prediction error for sharing secret data. Cybersecurity 6 (1).
4. Lu, W., Swaminathan, A., Varna, A. L., & Wu, M. (2009, February). Enabling search over encrypted multimedia databases. In Media Forensics and Security (Vol. 7254, pp. 404-414). SPIE.
5. Manikandan, V. M. (2021). A reversible data hiding scheme through encryption using rotated stream cipher. Computer Science, 22(2).
6. Stark, J. A. (2000). Adaptive image contrast enhancement using generalizations of histogram equalization. IEEE Transactions on image processing, 9(5), 889-896.
7. Thodi, D. M., & Rodríguez, J. J. (2007). Expansion embedding techniques for reversible watermarking. IEEE transactions on image processing, 16(3), 721-730.

8. Tian, J. (2003). Reversible data embedding using a difference expansion. IEEE transactions on circuits and systems for video technology, 13(8), 890-896.
9. Weinberger, M. J., Seroussi, G., & Sapiro, G. (2000). The LOCO-I lossless image compression algorithm: Principles and standardization into JPEG-LS. IEEE Transactions on Image processing, 9(8), 1309-1324..
10. Zeng, W. (1998). Digital watermarking and data hiding: technologies and applications. In Proc. Int. Conf. Inf. Syst., Anal. Synth (Vol. 3, pp. 223-229).
11. Zhang, W., Hu, X., Li, X., & Yu, N. (2013). Recursive histogram modification: establishing equivalency between reversible data hiding and lossless data compression. IEEE transactions on image processing, 22(7), 2775-2785.
12. Wang, Y., Hu, L., Gao, L., Li, S., & Li, H. (2022). Efficient reversible data hiding scheme based on prediction-error expansion and optimal parameters dynamic selection. Journal of Electronic Imaging, 31(1), 013035-013035.
13. Xie, X. Z., Chang, C. C., & Hu, Y. C. (2020). An adaptive reversible data hiding scheme based on prediction error histogram shifting by exploiting signed-digit representation. Multimedia Tools and Applications, 79, 24329-24346.
14. Liao, X., & Shu, C. (2015). Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels. Journal of Visual Communication and Image Representation, 28, 21-27.
15. Chi, H. X., Horng, J. H., & Chang, C. C. (2021). Reversible data hiding based on pixel-value-ordering and prediction-error triplet expansion. Mathematics, 9(14), 1703.
16. Peng, F., Zhang, S., & Wei, X. (2021). LSB substitution method with high capacity for image steganography. Journal of Ambient Intelligence and Humanized Computing, 12(8), 8895-8905.
17. Venugopal, K., & Jagadeesh, B. (2024). Theoretical Insights Into User Security and Privacy in Social. Human Impact on Security and Privacy: Network and Human Security, Social Media, and Devices: Network and Human Security, Social Media, and Devices, 289.
18. Khari, M., Garg, A. K., Gandomi, A. H., Gupta, R., Patan, R., & Balusamy, B. (2019). Securing data in Internet of Things (IoT) using cryptography and steganography techniques. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 50(1), 73-80.
19. Saleh, M. E., Aly, A. A., & Omara, F. A. (2016). Data security using cryptography and steganography techniques. International Journal of Advanced Computer Science and Applications, 7(6).
20. Taha, M. S., Mohd Rahim, M. S., Lafta, S. A., Hashim, M. M., & Alzuabidi, H. M. (2019, May). Combination of steganography and cryptography: A short survey. In IOP conference series: materials science and engineering (Vol. 518, No. 5, p. 052003). IOP publishing.