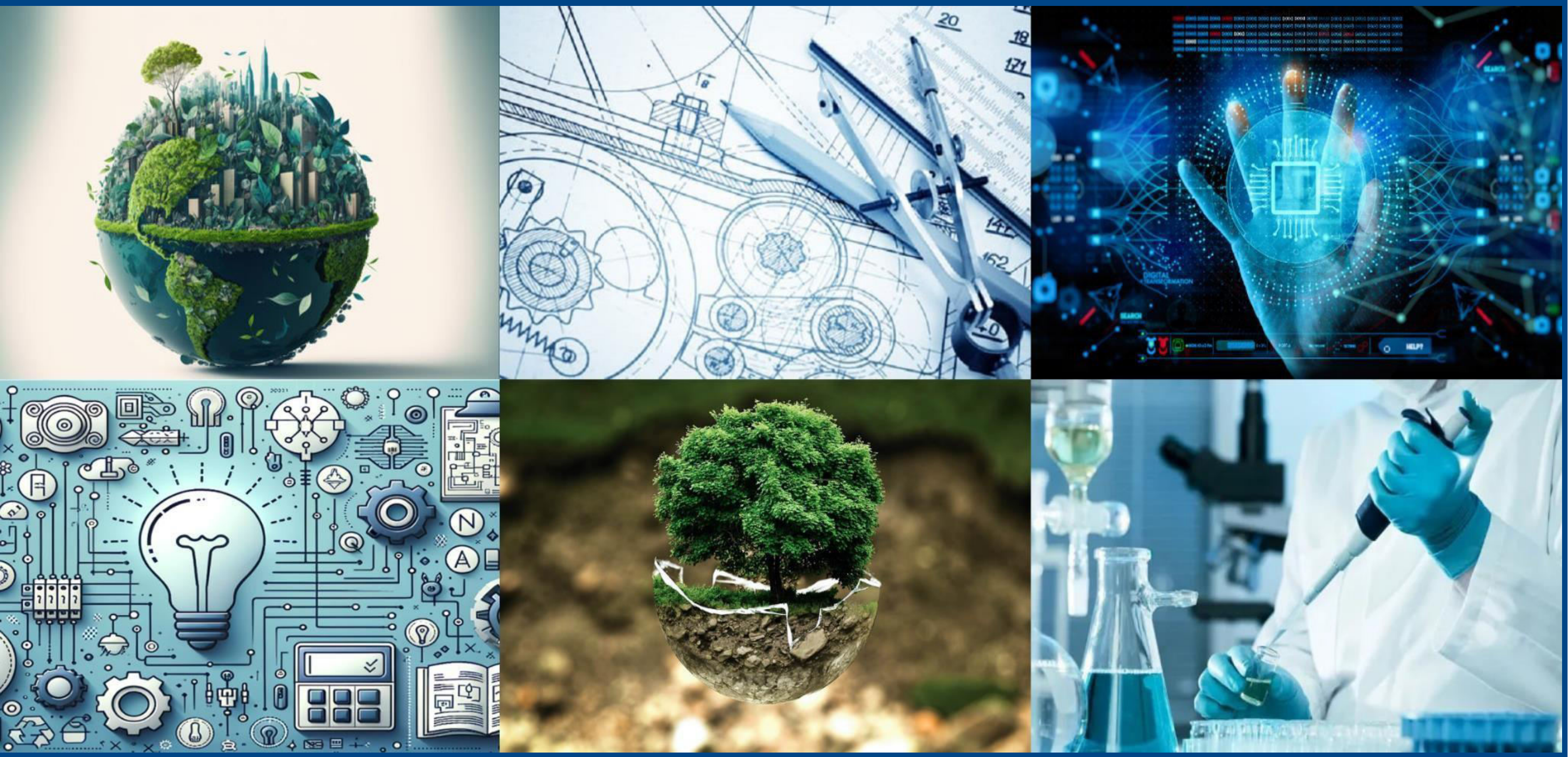
ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

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



Impact Factor: 8.206

Volume 8, Issue 12, December 2025

www.ijmrset.com ijmrset@gmail.com +91 6381 907 438 +91 63819 07438

Adaptive Steganography Technique

Dileep G N, Akash J, Ansh Gupta, Abhilash K A, Mr. Nandish M

Department of Computer Science and Engineering, JNNCE, Shivamogga, Karnataka, India

ABSTRACT: The increase of data communication globally requires secure exchange of private information. Steganography is a common form of information hiding from an unauthorized access. Secret messages can be in different ways and file formats such as: images, texts, audios, and videos. Transmitting secret messages is important for trading private information between different countries without hacking. Adaptive Steganography enables hiding data with variable numbers of bits based on the size of the secret message and the cover image. This paper proposes a new data hiding approach for image steganography based on the human visual properties using adaptive Least Significant Bits (LSB). Two different methodologies are applied; firstly, the human eye has different sensitivity to RGB color channels which permits different number of bits for every color channel. Secondly, photos focus normally on their middle zone which permits hiding the secret message using a spiral way starting from the images' edges towards its center. Both methods are used to enhance the visual appearance of the stego image using the simple LSB replacement approach. This approach enables hiding bigger secret message with less real visual effect/distortion. Experiments are implemented using the common image processing photos dataset. We applied the traditional LSB Steganography with our approach using different performance metrics criteria. Our approach presented better results when compared to traditional LSB approach and when compared with similar recent researches.

I. INTRODUCTION

In today's digital world, secure communication is very important because large amounts of sensitive data such as personal, financial, and business information are transmitted over public networks. While cryptography protects data by encrypting it, it does not hide the existence of the communication, which may attract attackers. Therefore, there is a need for techniques that can both secure the data and hide its presence during transmission. Steganography is an information hiding technique that embeds secret data inside digital media such as images, audio, or videos. Image steganography is widely used because digital images have high data capacity and redundancy. The Least Significant Bit (LSB) method is a popular technique where secret data is hidden in the least significant bits of pixel values, causing minimal visual changes. However, traditional LSB methods can reduce image quality and are vulnerable to detection and attacks. To overcome these limitations, adaptive steganography techniques are used. Adaptive methods consider image characteristics and human visual sensitivity, embedding more data in complex or less noticeable regions of the image. This improves imperceptibility, increases data capacity, and provides better resistance to steganalysis, compression, and noise. In this project, steganography is combined with cryptography to provide an additional layer of security. Encryption algorithms like DES and AES are used to encrypt the secret message before embedding it into the image. The proposed adaptive steganography system uses adaptive LSB embedding, randomized placement, and encryption, along with a user-friendly Python-based GUI. This approach ensures secure, efficient, and imperceptible data hiding for modern communication needs.

II. LITERATURE REVIEW

Ashraf AbdelRaouf **[1]** proposed an adaptive image steganography technique based on human visual color sensitivity. The method uses spiral embedding from image edges to the center and adaptive LSB modification across color channels. By exploiting areas less noticeable to the human eye, the approach improves imperceptibility and robustness of hidden data. Cong Xie and Jun Yu **[2]** presented a survey on the role of deep learning in modern steganography. The paper reviews neural networks such as autoencoders and GANs for data embedding and detection. It highlights improved security and efficiency while discussing challenges like robustness and large dataset requirements. Chunhua Zhang and Ming Zhang **[3]** introduced a robust image steganography method using deep neural networks. Their approach enhances resistance against distortion and steganalysis attacks. Experimental results show improved security and reliability, making the method suitable for sensitive communication. Jiawei Zhang and Sudeep Pasricha **[4]** reviewed recent advancements in audio steganography. The paper discusses traditional and machine learning–based techniques for embedding data in audio files. It emphasizes challenges such as preserving audio quality while maintaining security and robustness. Weiwei Zhang and Shengli Xie **[5]** proposed an end-to-end deep learning framework for image steganography. The model integrates encoding and decoding into a single system to balance payload capacity and imperceptibility. Results show high image quality even with large embedded data. Javed Iqbal and Saba Shams **[6]** provided a comprehensive review of steganography techniques for audio and video files. The paper analyzes various embedding methods, their limitations, and robustness issues. It also discusses applications in secure communication and digital rights management. Shiqi Wang et al. **[7]** introduced "Deeps Tego," a generative deep learning–based steganography approach. The method uses neural networks to optimize data embedding while increasing resistance to steganalysis. Results show better performance compared to traditional techniques. Mohd Khalid and Zubair Baig **[8]** presented a survey on image steganography and steganalysis techniques. The paper categorizes existing methods and discusses security vulnerabilities and countermeasures. It also highlights the growing role of deep learning in both data hiding and detection Mohamed Abdo and Khaled AlSharif **[9]** proposed an adaptive steganography technique using Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT). Data is embedded in low-frequency regions to minimize visual distortion. The method achieves high PSNR, SSIM, and improved robustness. Rasha M. Ali and Hossam M. Zawa **[10]** introduced an adaptive image steganography approach using Integer Wavelet Transform (IWT) and Genetic Algorithms. The genetic algorithm optimizes embedding locations to maximize payload while minimizing distortion. Experimental results show improved image quality and resistance to attacks. Hiroaki Kikuchi and Shigeo Watanabe **[11]** proposed a robust adaptive steganography technique designed to withstand JPEG re-compression. The method embeds secret data using dither modulation in low-frequency DCT coefficients and simulates re-compression during the embedding process. Additionally, error correction codes are applied to ensure reliable data extraction. This approach significantly improves robustness against compression, format conversion, and lossy transmission, making it suitable for real-world steganographic applications

III. SYSTEM ARCHITECTURE

The system architecture is designed to securely hide confidential information within ordinary digital media using steganography. It starts with **cover data**, such as an image, audio file, or text document, along with the **secret data** that needs to be concealed. During the **embedding process**, a steganographic algorithm carefully modifies the cover data in a subtle manner so that the secret message is inserted without noticeably affecting the appearance or quality of the original media. The result of this process is known as **stego data**, which appears the same as the original cover data to an untrained observer.

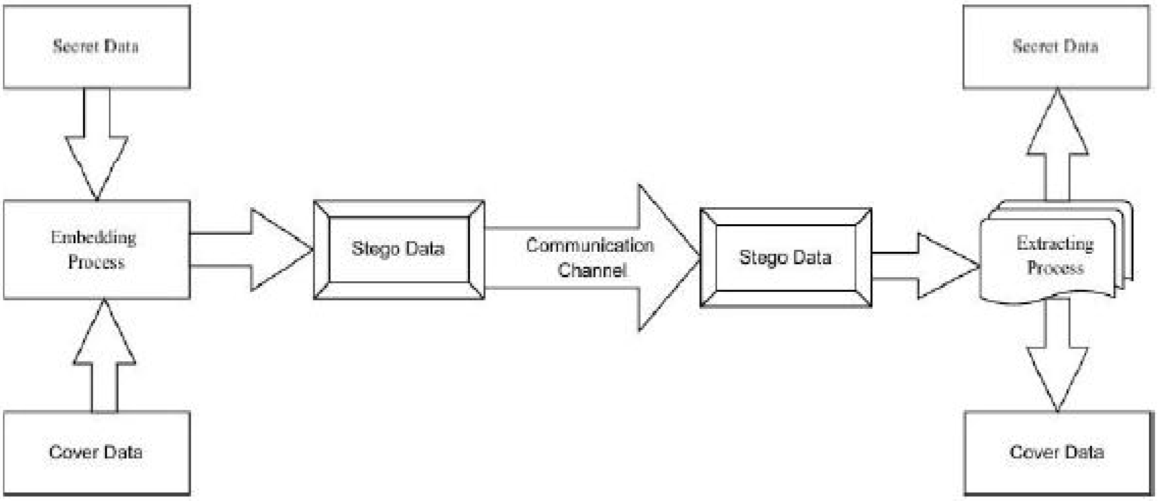


Figure 1: System Architecture of Adaptive Steganography Technique

The stego data is transmitted through a **communication channel** such as the internet, email, or social media platforms. At the receiver's end, an **extracting process** is used to retrieve the hidden secret information from the stego data using a specific algorithm. Once the secret message is successfully extracted, the original cover data is no longer needed and is typically discarded. This architecture ensures secure, hidden, and reliable communication between the sender and receiver.

IV. FLOWCHART

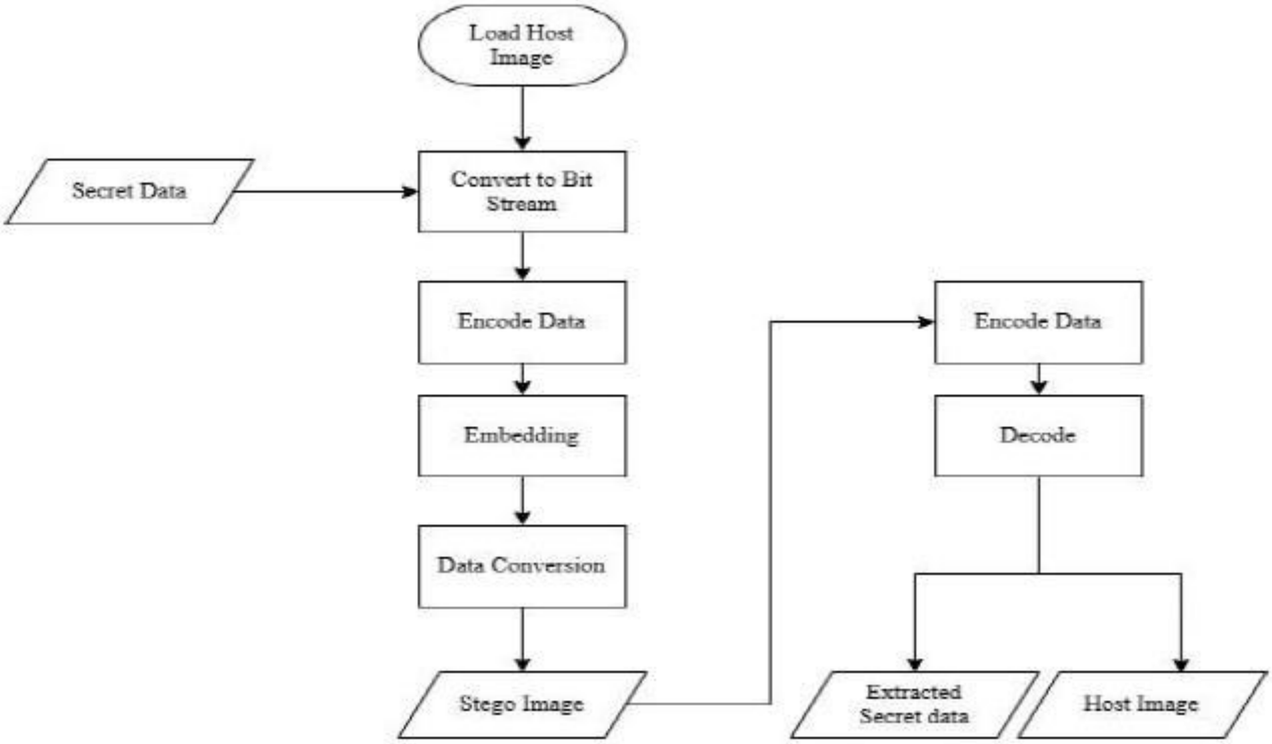


Figure 2: Flowchart of Adaptive Stenography Technique

V. OBJECTIVE

Steganography enhances **security and privacy** by embedding confidential information within images in a way that prevents unauthorized detection and access. The technique also focuses on **optimizing data capacity**, allowing a maximum amount of information to be hidden without degrading image quality by using efficient encoding methods. Additionally, the embedding process is designed to **minimize distortion** in the host image, ensuring that visual quality remains unchanged and the presence of hidden data is imperceptible. Finally, the system emphasizes **robustness**, protecting the concealed data against common image manipulations such as compression, resizing, or noise.

.

VI. SCOPE

Steganography involves concealing secret information within non-suspicious digital media such as images, audio, video, or text so that the hidden message remains undetectable. The scope of a steganography project is wide and includes image, audio, and video-based data hiding using techniques like LSB, DCT, and DWT, along with the integration of cryptographic algorithms such as AES and DES for enhanced security. It also covers robustness against image processing attacks, performance evaluation in terms of capacity and imperceptibility, and security analysis against steganalysis. Additionally, steganography finds applications in secure communication, digital watermarking, copyright protection, authentication, and privacy preservation, making it an important area in modern information security.

VII. APPLICATIONS OF SYSTEM

The combination of steganography and cryptography in this system opens up a range of practical applications

Secure Communication: The primary use case for this system is secure communication. By embedding encrypted messages into images, users can send confidential information through channels that might otherwise be insecure, such as email or social media, without raising suspicion. Even if an attacker intercepts the image, the hidden message will be difficult to extract due to both the encryption and the steganographic techniques.

Digital Watermarking: Steganography can be used to embed watermarks into digital media, such as images or videos. These watermarks can be used for copyright protection, ensuring that the original creator’s information is embedded into the content in a way that cannot easily be removed.

Privacy Protection: Individuals seeking to protect their privacy can use this system to hide personal information within images. This is particularly useful for protecting sensitive personal data in situations where conventional encryption might draw attention.

Digital Forensics: Forensics experts can use this system to detect and extract hidden data in digital media during investigations. Understanding how steganography works and being able to detect hidden messages is a crucial skill in digital forensics.

Data Integrity: The hidden messages can also serve to verify the integrity of digital content. For example, one could embed a checksum or a hash of the content within the image itself, allowing for verification of its authenticity later.

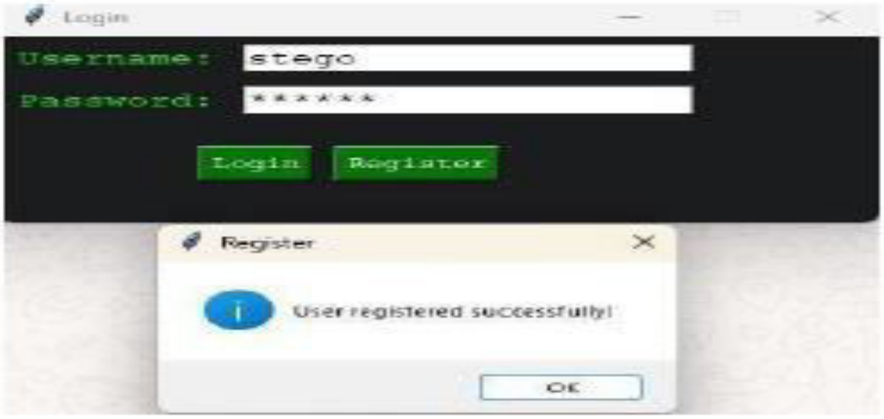
VIII. RESULT

In this chapter, the focus shifts towards showcasing the outcomes and practical demonstrations of the steganographic techniques employed in the project. This chapter provides an in-depth analysis of how the implemented methods perform in terms of embedding and extracting hidden data. By presenting key results, practical examples, this section aims to illustrate the effectiveness, efficiency, and robustness of the steganographic solutions developed throughout the project. These results will not only validate the proposed methods but also highlight their potential applications, limitations, and areas for future improvement.

IX. SYSTEM DESIGN

The project focuses on developing a steganography-based application that enables secure and hidden message embedding within images using various encoding techniques. The application utilizes multiple methods such as Adaptive LSB (Least Significant Bit), DES (Data Encryption Standard), AES (Advanced Encryption Standard), and Randomized LSB for encrypting and concealing messages within the pixel data of images. It provides users with the ability to encode and decode hidden messages securely, ensuring data confidentiality and integrity. Additionally, the project features an intuitive graphical user interface (GUI) for easy interaction, allowing users to manage their encrypted data and perform steganographic operations efficiently.

X. SNAPSHOTS



Username: stego

Password: ******

User registered successfully!

Fig 3: Login Page

Figure 4.1 shows a simple login interface with a username and password field. The user has entered "stego" as the username. The password field is masked with asterisks for security. The interface also includes "Login" and "Register" buttons. A message box appears, indicating that a user has been successfully registered. This suggests a basic authentication system for accessing the steganography application.

XI. GRAPHICAL USER INTERFACE (GUI)

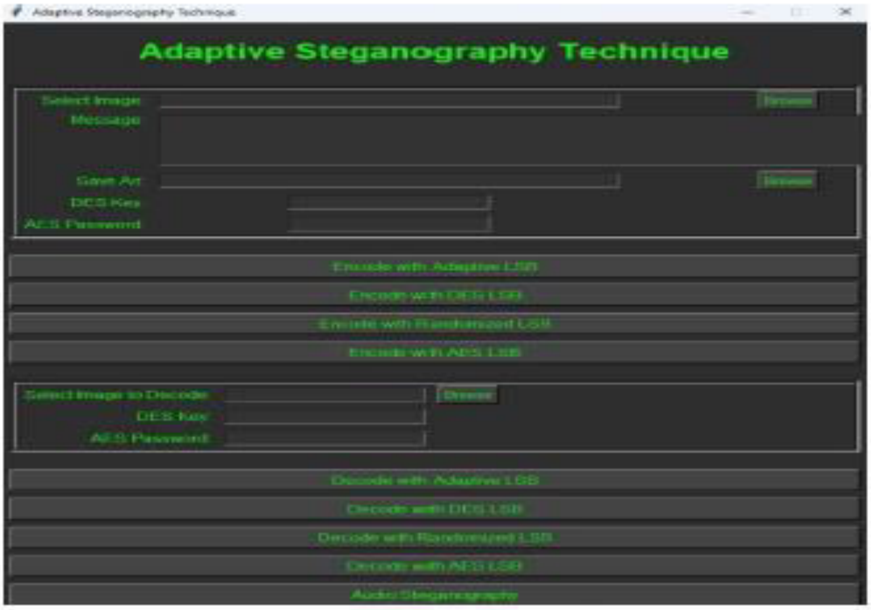


Figure 4: Graphical User Interface

GUI is designed for implementing adaptive steganography techniques. Users can select a host image and enter a secret message. They can then choose from various embedding methods, including adaptive LSB, DES LSB, AES LSB, audio steganography and randomized LSB. The GUI also allows for data encryption using DES or AES for enhanced security. Once the encoding parameters are set, the user can embed the secret message into the host image. The decoding section enables users to select the stego image and the appropriate decoding method to extract the hidden message.

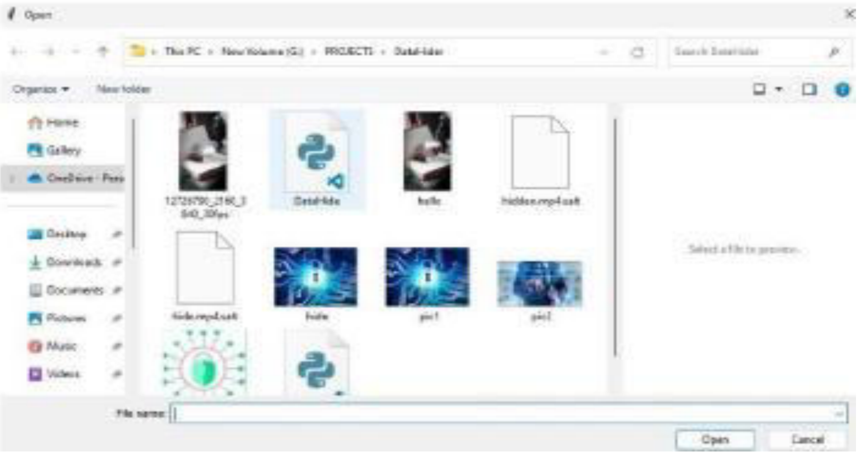


Figure 5: Image Selection

XII. FUTURE ENHANCEMENT

Steganalysis Resistance: Explore and implement techniques to improve the robustness of the system against steganalysis attacks, which aim to detect the presence of hidden data.

Image Quality Assessment: Incorporate metrics to assess the impact of data embedding on image quality and optimize the embedding process to minimize visual artifacts.

Adaptive Embedding: Implement more sophisticated adaptive embedding algorithms that dynamically adjust the embedding process based on the characteristics of the host image and the desired level of security.

Data Compression: Integrate data compression techniques to increase the amount of data that can be hidden within a given image.

Audio/Video Steganography: Extend the project to support data hiding in audio and video files. This project provides a foundation for further research and development in the field of steganography. By addressing the limitations and exploring advanced techniques, we can create more secure and efficient methods for covert communication and data protection.

XIII. CONCLUSION

Our steganography project effectively combines image processing, encryption, and data embedding techniques to securely hide and retrieve messages within images. By utilizing various encoding methods, such as Adaptive Least Significant Bit (LSB) encoding, Randomized LSB encoding, and cryptographic techniques using DES and AES encryption, the system ensures both data concealment and message security. The LSB method hides messages in the least significant bits of image pixels, while the randomized LSB adds an extra layer of security by selecting random pixel positions for embedding. The use of DES and AES encryption further secures the message, making it unreadable without the correct decryption key or password. The project provides a user-friendly graphical user interface (GUI) built using Tkinter, allowing users to easily load images, input messages, and select from various encoding and encryption methods. This makes it accessible to users without requiring in-depth technical knowledge. The system is designed to handle both encoding and decoding tasks, making it a versatile tool for secure communication. Users can encode messages in images and then decode them with the appropriate keys, ensuring confidentiality and privacy. While the project offers a range of encoding techniques, there are areas for improvement. For instance, the system may

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)
(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

encounter limitations when dealing with larger messages due to the pixel constraints of the images. Additionally, more advanced error handling mechanisms could be implemented to address edge cases and improve the user experience. Future enhancements could also include message compression before embedding to optimize space usage and allow larger payloads. Overall, this steganography project provides a solid foundation for secure communication using images, highlighting the importance of combining encryption and data embedding for protecting sensitive information in digital form. It is a practical tool for those interested in secure messaging, digital watermarking, and data protection.

REFERENCES

[1] A. AbdelRaouf, “A new data hiding approach for image steganography based on visual color sensitivity,” Journal of Visual Communication and Image Representation, vol. 90, 2023.

[2] C. Xie, J. Yu, et al., “Steganography in the Era of Deep Learning: A Survey,” IEEE Access, vol. 9, pp. 97066–97095,2021.

[3] C. Zhang, M. Zhang, et al., “A Robust and Secure Image Steganography Method Using Neural Networks,” Journal of Information Security and Applications, vol. 64, p. 103110, 2022.

[4] J. Zhang and S. Pasricha, “Advances in Audio Steganography: Techniques, Applications, and Challenges,” IEEE Transactions on Multimedia, vol. 25, pp. 2757 2772, 2023.

[5] W. Zhang and S. Xie, “End-to-End Optimized Image Steganography Using Deep Learning Models,” Neural Processing Letters, vol. 55, pp. 1083–1100, 2023.

[6] J. Iqbal, S. Shams, et al., “Steganography for Audio and Video: A Review of Techniques, Applications and Challenges,” Multimedia Tools and Applications, vol. 79, no. 39–40, pp. 29143–29180, 2020.

[7] S. Wang, J. Luo, M. Wang, et al., “Deeps Tego: A Generative Approach for Steganography Using Deep Learning,” IEEE Transactions on Information Forensics and Security, vol. 16, pp. 3235–3250, 2021.

[8] M. Khalid, Z. Baig, et al., “A Survey on Image Steganography and Steganalysis Techniques,” Journal of King Saud University - Computer and Information Sciences, vol. 33, no. 5, pp. 505–519, 2021.

[9] C. Xie, J. Yu, et al., “Steganography in the Era of Deep Learning: A Survey,” IEEE Access, vol. 9, pp. 97066–97095,2021.

[10] M. Abdo and K. AlSharif, “Adaptive Steganography Using Wavelet and Cosine Transforms,” Journal of Electrical and Applied Systems, Springer Open, vol. 12, 2023.

[11] R. M. Ali and H. M. Zaw baa, “Integer Wavelet Transform and Genetic Algorithm Based Steganography,” Multimedia Tools and Applications, Springer, vol. 82, pp. 34211– 34235, 2023.

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com