2026 Volume: 02 Issue: 04 www.ijrpa.com ISSN 2456-9995 Research Article

International Journal Research Publication Analysis

Page: 01-11

STEGANOGRAPHY: HIDING SECRET MESSAGES IN IMAGES FOR DATA SECURITY

***S. Haneesh, P. Tarun, U. Sai Krishna, Soubhagya Ranjan Nayak**

GMR Institute of Technology.

Article Received: 15 March 2026
Article Revised: 05 April 2026
Published on: 25 April 2026

***Corresponding Author: S. Haneesh**
GMR Institute of Technology.

DOI: https://doi-doi.org/101555/ijarp.8016

1. ABSTRACT

This project is about using steganography to improve secure communication in the area of cybersecurity. Steganography is a technique used to hide secret information inside digital files such as images, so that no one can easily notice the hidden data. The main goal of this project is to protect confidential messages by embedding them inside images without changing the image's visible quality. This makes sure that the original image looks the same to normal users. The project uses simple and basic steganography methods to hide and retrieve secret messages when needed. Only authorized users who know the correct method can extract the hidden information. This helps prevent sensitive data from being seen or stolen by attackers. By hiding data inside normal looking images, the system allows secure communication over public or open networks without creating suspicion. Through this project, it is shown that steganography can be a useful and effective way to improve data security and privacy. It provides an extra layer of protection and helps reduce the risk of data leakage in digital communication systems.

KEYWORDS: *Steganography, Data Hiding, Secure Communication, Image Steganography, Information Security, Digital Media, Data Protection.*

2. INTRODUCTION

In today's digital world, a large amount of information is shared through the internet. People send messages, images, and important data every day. Because of this, keeping information safe has become very important. Sensitive data can be easily attacked, stolen, or accessed by unauthorized users when it is sent over open networks. Common security methods like

encryption can protect the content of the message, but they do not hide the fact that a message is being sent.

Steganography is a useful technique that helps in solving this problem. It is the process of hiding secret information inside another file, such as an image, so that no one can notice the hidden data. In this way, the communication looks normal and does not attract attention. Among different types, image steganography is widely used because digital images have enough space to store hidden data without changing their appearance.

In this project, an image steganography system is developed using the Least Significant Bit (LSB) method. In this method, the smallest bits of image pixels are modified to store secret information. These small changes do not affect the visible quality of the image, so it looks the same to normal users. A special end marker is also used to identify where the hidden message ends during decoding.

The main aim of this work is to provide a simple and secure way to hide and retrieve confidential messages using images. This method allows safe communication over public networks without creating suspicion. It also helps in improving data privacy and reduces the risk of information leakage. Therefore, steganography can be used as an additional layer of security in modern digital communication systems.

3. LITERATURE REVIEW

Several researchers have studied the importance of data security and privacy in digital communication systems and have explored different techniques to protect confidential information from unauthorized access.

The paper “Steganography and Steganalysis for Digital Image Enhanced Forensic Analysis and Recommendations” discusses how techniques for hiding and detecting secret data in images can be used to improve digital forensic investigations and provides recommendations for enhancing analysis accuracy and security. [1]

The paper “Steganography: Data Concealment in Images” explains methods of hiding secret information within digital images in a way that is not easily detectable, focusing on techniques, challenges, and their role in secure communication. [2]

The paper “The Image Steganography Using LSB and PVD Algorithms” explains how combining Least Significant Bit (LSB) and Pixel Value Differencing (PVD) techniques improves data hiding capacity and security while maintaining good image quality. [3]

The paper “An Efficient and Secure Technique for Image Steganography Using a Hash Function” describes a method where a hash function is used to randomly select pixel

positions for embedding secret data in an image, which enhances security by making the hidden data harder to detect while also maintaining good image quality and efficient data embedding. [4]

This paper focuses on improving data security in Industrial Internet of Things (IIoT) systems. In industries, many devices like sensors, machines, and controllers are connected and continuously exchange important data. Because of this, there is a high risk of cyber-attacks, data leakage, and unauthorized access. To solve this problem, the paper uses image steganography, which means hiding secret data inside images so that no one can even detect that a message exists. This adds an extra layer of security compared to normal encryption. [5]

4. METHODOLOGY

The proposed system uses an image-based steganography approach to achieve secure communication. It applies the Least Significant Bit (LSB) technique to hide confidential messages inside digital images. During the encoding process, the secret message is converted into binary form and embedded into the pixel values of the image. In the decoding process, the hidden data is extracted from the image by reading the modified pixel bits and converting them back into text. This method ensures that the message is securely hidden while maintaining the visual quality of the image.

4.1 System Initialization and Mode Selection

The proposed system begins with the initialization of the steganography module. At this stage, the user is prompted to select the operation mode, which can be either encoding or decoding. Based on the selected mode, the system directs the workflow toward the appropriate process. This step ensures a clear separation between data embedding and data extraction operations.

4.2 Encoding Phase

4.2.1 Input Carrier Image

In the encoding process, the user first selects a carrier image that will be used to hide the confidential information. The selected image is converted into RGB format so that individual pixel values can be accessed and modified. This conversion is necessary for applying the steganography technique effectively.

4.2.2 Input and Validation of Confidential Message

After selecting the image, the user provides the secret message that needs to be hidden. The system checks whether the message is empty or not. If no message is provided, the process is terminated to avoid errors. This validation step ensures that only valid input is processed further.

4.2.3 Conversion to Binary Representation

The confidential message is then converted into binary format. Each character in the message is represented using an 8-bit binary value. This binary representation is essential because the embedding process operates at the bit level within the image pixels.

4.2.4 Pixel Data Iteration and LSB Embedding

The system reads the image pixel data sequentially. Each pixel consists of three components: Red, Green, and Blue. The Least Significant Bit (LSB) of these pixel values is modified to embed the binary data. Since only the smallest bit is changed, the visual appearance of the image remains almost unchanged, making the hidden data imperceptible.

4.2.5 Insertion of End-of-Message Marker

Once all the message bits are embedded, a special end-of-message marker is inserted into the pixel data. This marker is used during the decoding process to identify where the hidden message ends. It ensures accurate and complete retrieval of the embedded information.

4.2.6 Generation of Steganographic Image

The prediction results are displayed through the web interface, allowing farmers to easily understand demand trends and recommendations. The system integrates the machine learning model with the web-based platform, ensuring smooth interaction between the frontend, backend, and database. This integration enables real-time prediction and efficient data handling.

4.3 Decoding Phase

4.3.1 Input Steganographic Image

In the decoding process, the user selects the steganographic image that contains the hidden message. The system prepares this image for data extraction by accessing its pixel values in RGB format.

4.3.2 Extraction of Pixel Data and LSB Values

The system reads the pixel data sequentially, in the same order as used during encoding. The Least Significant Bits of the pixel values are extracted, as these bits contain the hidden binary data.

4.3.3 Reconstruction of Binary Data and Text Conversion

The extracted bits are combined to reconstruct the binary data stream. This binary data is then converted back into characters, forming the original secret message. This step reverses the encoding process.

4.3.4 Detection of End of Message Marker

During the extraction process, the system continuously checks for the presence of a predefined end-of-message marker. This marker is embedded at the end of the secret data during the encoding phase. Once the marker is detected, the system understands that the complete hidden message has been retrieved and stops further data extraction. This prevents unnecessary reading of additional pixel data and ensures accurate termination of the decoding process.

4.3.5 Display of Retrieved Message

After detecting the end of message marker, the extracted binary data is fully converted back into readable text. The reconstructed message is then displayed to the user through the system interface. This step ensures that the original confidential message is presented clearly and correctly, without any extra or corrupted information.

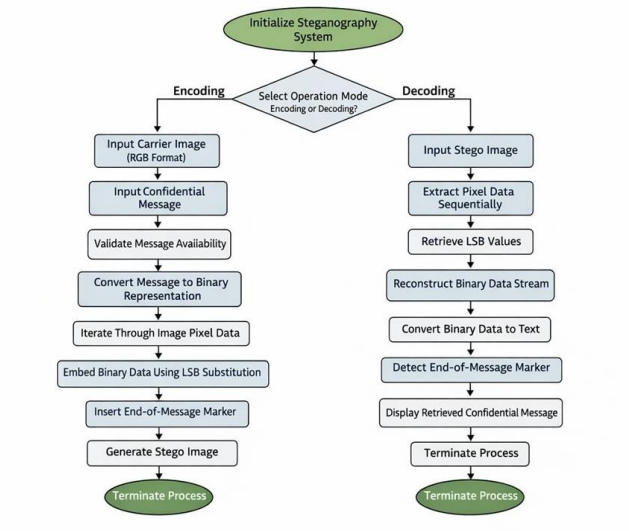

Fig 4.1: Workflow of Image based Steganographic Communication.

5. RESULTS AND DISCUSSION

5.1 Results

5.1.1 Main Interface of the System

The main interface of the StegnoVault system provides a clear and user-friendly environment for performing steganography operations. It allows the user to select between encoding and decoding modes. The layout is designed with a modern interface, making it easy to navigate. The input areas for uploading images and entering messages are clearly visible, which helps reduce user errors and improves overall usability.

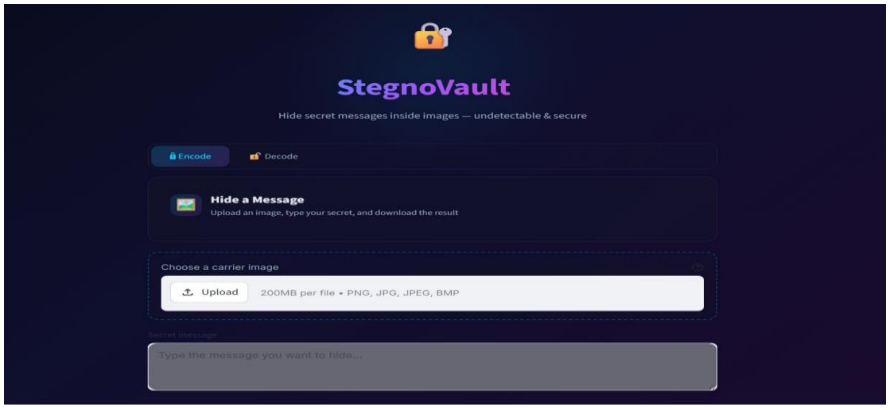

Fig 5.1: Stegno Vault System Main Interface.

5.1.2 Image Selection Process

This figure shows the process of selecting a carrier image from the system. The user can browse and choose an image file from local storage. This step is important because the selected image will be used to hide the secret message. The system supports different file formats, allowing flexibility in image selection.

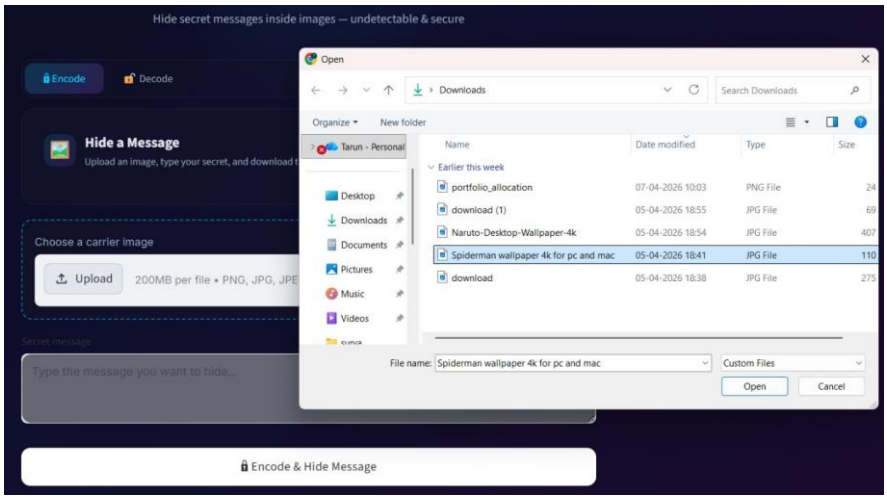

Fig 5.2: Carrier Image Selection for Encoding.

5.1.3 Encoding Interface with Image Details

This figure presents the encoding interface after selecting an image. The system displays important details such as image resolution, file size, and estimated character capacity. These details help the user understand how much data can be embedded. The user can then enter the secret message, and the system prepares the data for embedding using the LSB technique.

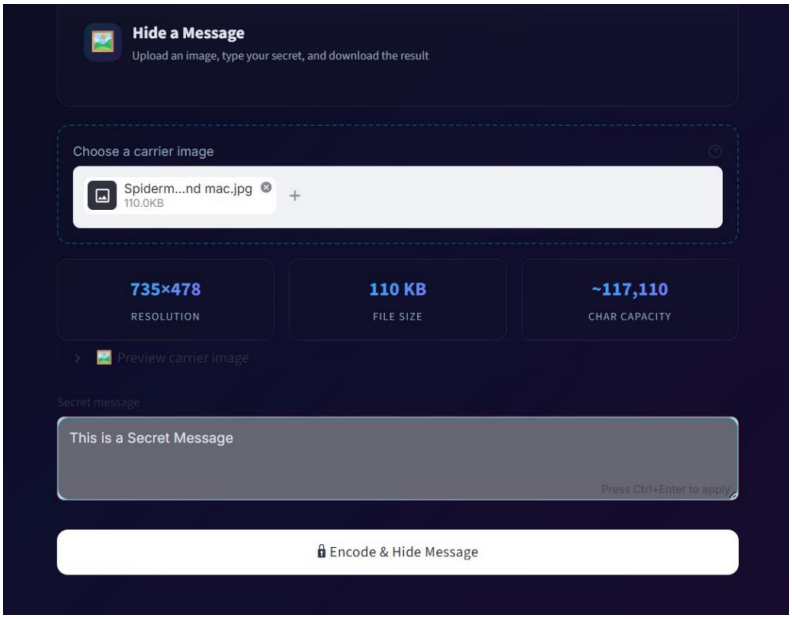

Fig 5.3: Encoding Interface with Image Properties and Message Input.

5.1.4 Decoding Interface

This figure shows the decoding interface of the system. The user uploads the steganographic image, which contains the hidden message. The system then processes the image, extracts the least significant bits, and reconstructs the original message. The interface is simple and ensures that the decoding process is easy to perform.

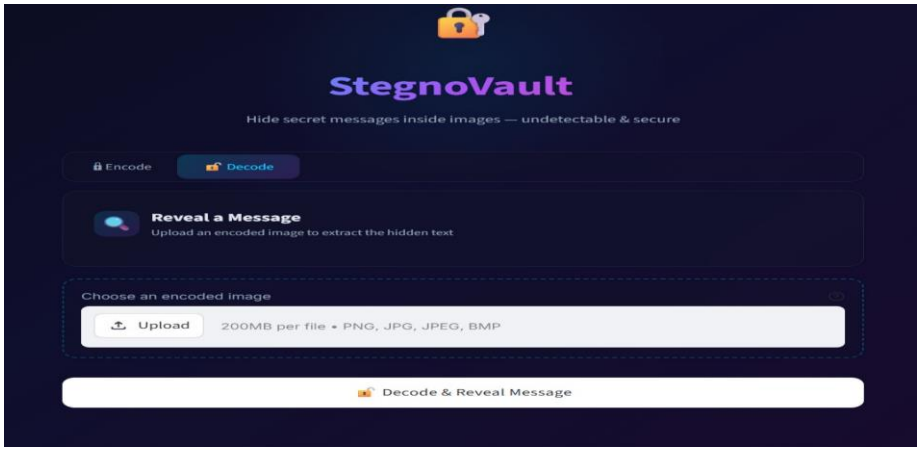

Fig 5.4: Decoding Interface for Hidden Message Extraction.

5.1.5 Selection of Encoded Image for Decoding

This figure shows the process of selecting the encoded image for decoding. The user browses and uploads the image that contains the hidden message. This step is important because the system requires the exact steganographic image generated during the encoding phase. The interface ensures easy file selection and prepares the image for the extraction process.

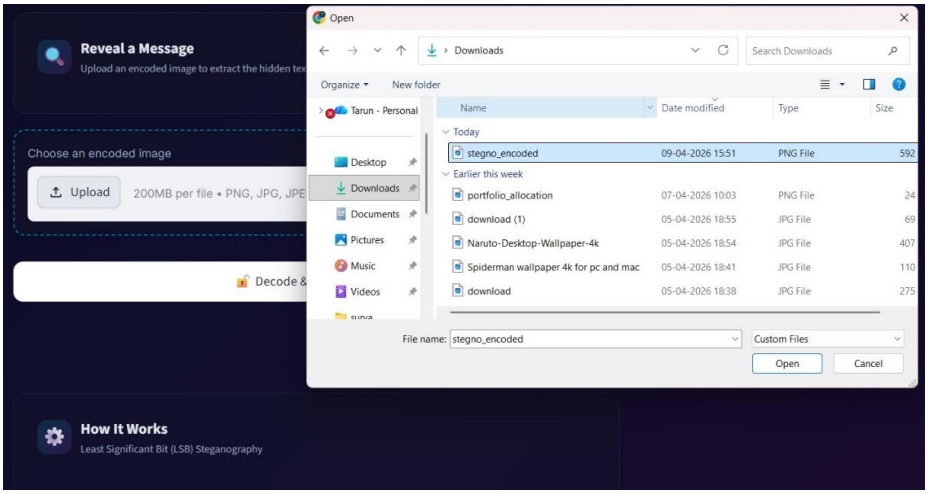

Fig 5.5: Selection of Steganographic Image for Decoding.

5.1.6 Decode and Reveal Message

This figure illustrates the final stage of the decoding process. After selecting the encoded image, the user initiates the decoding operation. The system extracts the hidden data from the image by reading the least significant bits of pixel values. The original secret message is then reconstructed and displayed to the user. This confirms the successful retrieval of the embedded information.

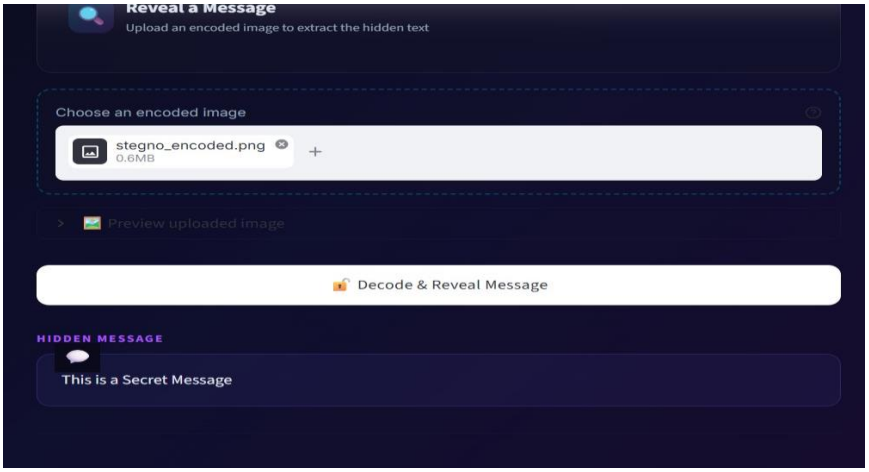

Fig 5.6: Decoding and Revealing the Hidden Message.

5.2 DISCUSSION

5.2.1 Image Quality Analysis

The quality of the steganographic image was analysed by visually comparing it with the original image. It was observed that there is no noticeable difference between the two images, which shows that the LSB technique introduces very minimal distortion. Since only the least significant bits are modified, the overall appearance of the image remains unchanged. This confirms that the method is effective for hiding data without affecting visual quality.

5.2.2 Data Capacity

The data hiding capacity of the system depends on the size and resolution of the input image. Images with higher resolution can store larger messages without degrading quality. The system also provides an estimated character capacity, which helps users avoid overloading the image. This makes the system more practical and user-friendly.

5.2.3 Security Limitation

Although the system provides an additional layer of security by hiding the message, it is not completely resistant to advanced steganalysis techniques. If an attacker suspects the presence of hidden data, they may attempt to extract it using statistical analysis. Therefore, combining steganography with encryption can further enhance the security of the system.

6. CONCLUSION

In this work, an image steganography system was developed to improve secure communication by hiding confidential messages inside digital images. The system uses the Least Significant Bit (LSB) technique to embed secret data into image pixels without affecting the visible quality of the image. The results show that the hidden messages can be accurately encoded and decoded, and the steganographic image appears almost identical to the original image.

The system is simple to use and provides a user-friendly interface for both encoding and decoding operations. It also ensures that the hidden communication does not attract attention, which adds an extra layer of security compared to traditional methods. The use of an end-of-message marker helps in correctly retrieving the embedded data without errors.

However, the method has some limitations. It is sensitive to image compression and may not work well with lossy formats like JPEG. In addition, the system may be vulnerable to

advanced detection techniques if used alone. Despite these limitations, the proposed approach is effective for basic secure communication and demonstrates the usefulness of steganography in protecting data privacy.

Overall, the project shows that image steganography is a reliable and efficient technique for hiding information and can be used as an additional security layer in modern digital communication systems.

REFERENCES

1. Kristian D. Michaylov & Dipti K. Sarmah (2024). “Steganography and steganalysis for digital image enhanced Forensic analysis and recommendations” ISSN Publication on 23 Jan 2024 DOI: 10.1080/23742917.2024.2304441.
2. Khan M. H., Agrahari H., Sharma A., Tiwari A., Sheoran S., “Steganography: Data Concealment in Images,” International Journal for Research in Applied Science & Engineering Technology (IJRASET), Volume 13, Issue V, May 2025. doi:10.22214/ijraset.2025.70300
3. Akshitha S and Aishwarya MS “The Image Steganography Using LSB and PVD Algorithms”, IJRAR May 2023, Volume 10, Issue 2, DOI: 10.1016/ijrar.2023.05.174
4. Hamid Ali, Muhammad Asif, “An efficient and secure technique for image steganography using a hash function” Published on 24 November 2022 PeerJ Comput. Sci. 8: e1157
5. M. Hassaballah and Khan Muhammad, (2021)."A Novel Image Steganography Method for Industrial Internet of Things Security “, IEEE Transactions ON Industrial Informatics, vol. 17, no. 11.
6. J Gopika Rajan and R. S. Ganesh, (2024). “Dynamic pixel shuffling and hash LSB steganography with RC4 encryption: A robust data security framework”, Except System Applications 279(2024) 127403, Doi.org/10.1016/j.eswa.2025.127403.
7. Md Amiruzzaman (2021) “A Survey on Steganography and Steganalysis Techniques in Secret Communication” Research Briefs on Information and Communication Technology Evolution, 8, 97–113. doi.org/10.56801/rebicte.v8i. 139
8. Hassan Shaban “Digital Image Steganography and Reversible Data Hiding: Algorithms, Applications and Recommendations” Published: September 16, 2025, Journal of Image and Graphics, Vol. 13, No. 1, 2025, doi: 10.18178/joig.13.1.90-114

9. Khan FarhanRafat, (2024). “Advancing Reversible LSB Steganography: Addressing Imperfections and Embracing Pioneering Techniques for Enhanced Security”, Digital Object Identifier 10.1109/access.2024.3468988.
10. Pascal Maniriho, Tohari Ahmad (2020). “Information hiding scheme for digital images using difference expansion and modulus function” Journal of King Saud University – Computer and Information Sciences 31 (2020) 335–347 doi.org/10.1016/j.jksuci.2018.01.01