AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(2026)

SECURE IMAGE -BASED DATA HIDING USING STEGANOGRAPHY TECHNIQUES

[1]Madhunika,[2]S.Sumithra,[3]N.Sahithya,[4]B.Durga bhavani siri

[1]Assistant Professor, [234]Students

Siddhartha institute of technology & sciences,narapally

kulkarnimadhunika@siddhartha.org.in, 23TQ1A6219@siddhartha.co.in.
23TQ1A6212@siddhartha.co.in, 23TQ1A6216@siddhartha.co.in

ABSTRACT

In the modern digital era, secure communication of sensitive information has become increasingly important due to the rising number of cyber threats. This project, titled "Secure Image-Based Data Hiding Using Steganography Techniques," focuses on protecting confidential data by concealing it within digital images. Steganography is a technique that hides the existence of secret information, making it less detectable compared to traditional encryption methods.The proposed system utilizes image steganography, specifically the Least Significant Bit (LSB) technique, to embed secret data into a cover image. The confidential message is first converted into binary format and then inserted into the pixel values of the image in a manner that preserves its visual quality. To further enhance security, encryption techniques can be applied to the data before embedding, ensuring that even if the hidden data is extracted, it remains unreadable without the appropriate decryption key.

This approach allows secure transmission of data over the internet without raising suspicion. The system is evaluated based on parameters such as data hiding capacity, security level, and image quality after embedding. The results demonstrate that the method effectively maintains image integrity while securely storing hidden information.Overall, this project emphasizes the significance of combining steganography and encryption techniques to ensure data privacy and secure digital communication, making it a valuable solution for protecting sensitive information from unauthorized access.

I INTRODUCTION

In the modern digital world, the transmission of information over the internet has increased rapidly. With this growth, the need to protect confidential data from unauthorized access has become highly important. Traditional security techniques such as encryption safeguard the content of a message but do not conceal its existence. This limitation may attract attackers, who can attempt to intercept and decrypt the data. To address this issue, steganography is used as an effective method for secure communication.Steganography is the process of hiding secret information within a digital medium such as an image, audio file, or video, in such a way that the presence of the hidden data is not noticeable. Among the various types of steganography, image

Received: 04-03-2026 | Accepted: 13-03-2026 | Published: 01-04-2026 | www.ajaccm.com

steganography is widely preferred because digital images contain a large amount of redundant data that can be utilized to embed information without significantly affecting visual quality.

This project focuses on secure image-based data hiding using steganographic techniques, where sensitive information is embedded into an image known as a cover image. The embedding process is typically performed using techniques such as the Least Significant Bit (LSB) method, which alters the least significant bits of image pixels to store secret data. These minor modifications are generally invisible to the human eye, ensuring that the original appearance of the image remains unchanged.

To further enhance security, encryption techniques can be applied to the secret message before embedding it into the image. This combination of steganography and encryption adds an extra layer of protection, making the hidden data more secure against unauthorized access and potential attacks.

The main objective of this project is to design a secure and efficient system for embedding confidential data within digital images while preserving image quality and maintaining data integrity. This approach can be applied in various fields such as secure communication, military data transfer, copyright protection, and digital watermarking.

II LITERATURE SURVEY

Image steganography is a technique used to hide secret information inside digital images in such a way that the existence of the message cannot be detected, making it highly suitable for secure communication over the internet. The primary objectives of steganography include imperceptibility, data capacity, and security. Various algorithms have been developed to enhance the efficiency and reliability of data hiding methods. One of the most commonly used techniques is the Least Significant Bit (LSB) method, where secret data is embedded into the least significant bits of image pixels. Since the modification occurs at the lowest bit level, the visual quality of the image remains almost unchanged, making the alterations invisible to the human eye while maintaining low computational complexity. Another widely used approach is the Pixel Value Differencing (PVD) method, which calculates the difference between adjacent pixel values to determine how many bits of secret data can be embedded. This method allows more data to be hidden in edge regions compared to smooth areas, thereby improving data capacity and maintaining better image quality, although it may still be vulnerable to certain steganalysis techniques. To further strengthen security, steganography is often combined with encryption methods, where the secret message is encrypted before being embedded into the image. This adds an additional layer of protection, making it difficult for unauthorized users to interpret the data even if it is extracted. Moreover, recent advancements in steganography focus on adaptive and intelligent techniques that utilize edge detection, image analysis, and machine learning to identify optimal embedding locations within an image. These advanced methods enhance robustness, increase embedding capacity, and reduce the chances of detection by modern steganalysis tools.

III SYSTEM ANALYSIS

System analysis is an essential phase in the development of the Secure Image-Based Data Hiding Using Steganography Techniques project, as it helps in understanding the requirements, feasibility, and overall structure of the system. The main goal of this system is to provide a secure and efficient method for hiding confidential information within digital images while ensuring data integrity and image quality.

The existing systems mainly rely on traditional encryption techniques, which protect the content of the data but do not hide its existence. This makes the data vulnerable to attacks, as unauthorized users may attempt to intercept and decrypt the information. Additionally, some basic steganography methods lack sufficient security and are prone to detection through advanced steganalysis techniques. These limitations highlight the need for a more robust and secure approach.

The proposed system addresses these issues by combining steganography with encryption techniques. In this system, the secret message is first converted into binary format and optionally encrypted for additional security. Then, using the Least Significant Bit (LSB) technique, the data is embedded into the pixel values of a cover image. The system ensures that the modifications made to the image are minimal and do not affect its visual quality. At the receiver's end, the hidden data can be extracted and decrypted using the appropriate key.

From a functional perspective, the system includes modules such as image selection, data input, encryption, embedding, extraction, and decryption. Non-functional requirements include high security, low computational complexity, good image quality, and efficient data capacity. The system is designed to be user-friendly and reliable for secure data transmission.

Existing system

The existing system for data hiding mainly uses basic image steganography techniques to embed secret information inside digital images. Commonly, methods such as the Least Significant Bit (LSB) technique are used, where secret data is inserted into the least significant bits of image pixels. This ensures that the changes made to the image are not easily visible to the human eye. These systems enable users to hide confidential information within a cover image and transmit it over the internet. At the receiver's end, the hidden data can be extracted from the stego image using appropriate extraction techniques. Image steganography is widely applied in areas such as secure communication, digital watermarking, and data protection. However, most existing systems focus only on basic embedding techniques and often lack additional security measures like strong encryption or advanced embedding strategies, making them less secure against modern attacks.

Disadvantages of Existing System

- Low Security
- Limited Data Capacity
- Image Quality Degradation

- Vulnerability

Proposed System

The proposed system aims to develop a secure and efficient method for hiding confidential information inside digital images using steganographic techniques. In this system, secret data such as text or files is embedded into a cover image using the Least Significant Bit (LSB) method while preserving the visual quality of the image. Before embedding, the secret data can be encrypted to enhance security, ensuring that even if the hidden data is detected, it cannot be understood without the correct decryption key. The encrypted data is then embedded into the pixel values of the cover image to generate a stego image. At the receiver's end, the stego image is processed using an extraction algorithm to retrieve the hidden data, and if encryption is applied, the data is decrypted using the appropriate key to obtain the original message. The proposed system offers improved security, better data protection, and minimal impact on image quality, making it suitable for secure communication, data privacy, and protection against unauthorized access.

Advantages of proposed system

- High Security
- Maintains Image Quality
- Confidential Data Transmission
- Easy Data Extraction
- Improved Privacy
- Simple and Efficient Method

IV METHODOLOGY

The methodology for the project "Secure Image-Based Data Hiding Using Steganography Techniques*"* involves a series of systematic steps to securely embed and extract confidential information within digital images. The process begins with the selection of a suitable cover image, which acts as the medium for hiding the secret data. The image is chosen in such a way that it has sufficient size and quality to accommodate the data without noticeable distortion.

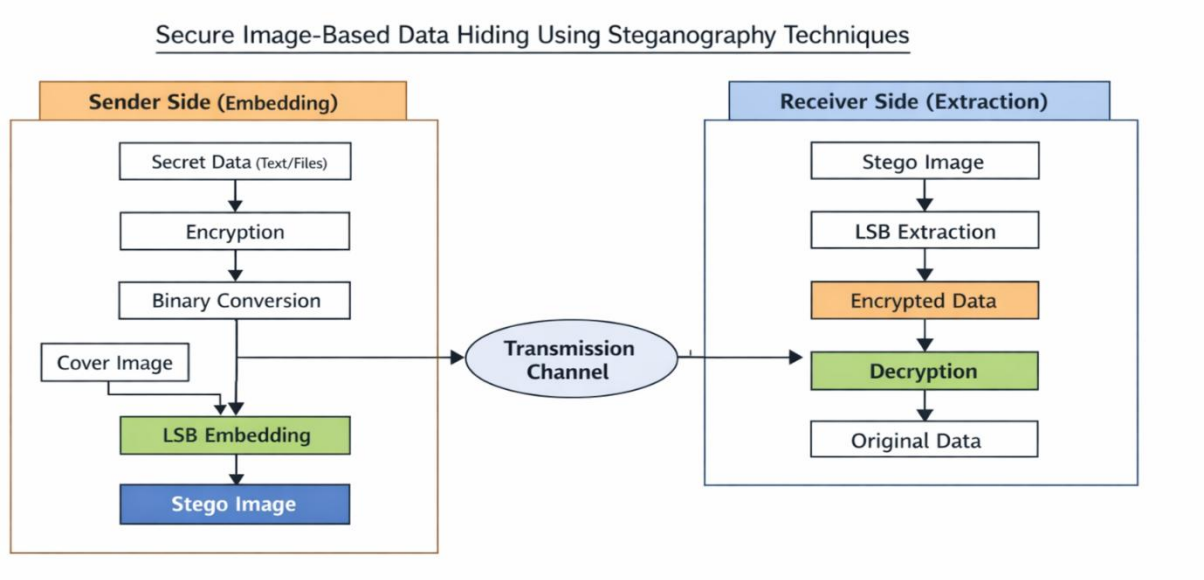
Next, the secret message or file is taken as input and converted into binary format. To enhance security, an optional encryption step is applied, where the data is encoded using an encryption algorithm and a secret key. This ensures that even if the hidden data is extracted, it cannot be understood without proper decryption.

After preprocessing, the embedding phase is performed using the Least Significant Bit (LSB) technique. In this step, the binary data is embedded into the least significant bits of the pixel values of the cover image. Since the changes occur at the smallest bit level, the visual quality of the image remains almost unchanged. The result of this process is called the stego image, which contains the hidden information.

The stego image is then transmitted to the receiver through a communication channel. At the receiver's end, the extraction process is carried out. The system reads the pixel values of the stego image and retrieves the embedded bits to reconstruct the hidden data. If encryption was applied during embedding, the extracted data is decrypted using the same key to obtain the original message.

Finally, the performance of the system is evaluated based on parameters such as image quality, data hiding capacity, and security. The methodology ensures that the hidden data remains secure, the image quality is preserved, and the system is efficient for real-time applications.

System Architecture



The system architecture for *Secure* Image-Based Data Hiding Using Steganography Techniques is designed to ensure secure transmission of confidential data by combining steganography and optional encryption. It is divided into two main phases: **Sender Side (Embedding)** and **Receiver Side (Extraction)**, connected via a **Transmission Channel**.

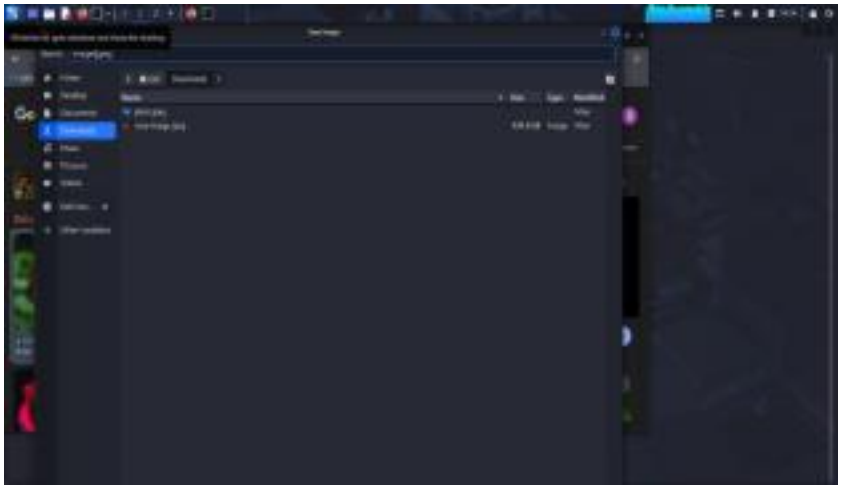
On the **Sender Side**, the process begins with the selection of a cover image, which acts as the medium for hiding information. The secret data (text or files) is first converted into binary format. For enhanced security, encryption can be applied to the data so that even if it is intercepted, it cannot be understood without the correct key. The encrypted binary data is then embedded into the least significant bits (LSB) of the cover image's pixels. Because the changes occur at the least significant bit level, the visual appearance of the image is largely preserved, producing a **Stego Image** that can be transmitted over a communication channel without attracting attention.On the **Receiver Side**, the stego image is received and processed using an LSB extraction algorithm to retrieve the embedded data. If the data was encrypted during embedding, the receiver decrypts it using the corresponding key to recover the original message.

The system architecture ensures that the secret information remains hidden, maintains the quality of the cover image, and provides strong protection against unauthorized access. By

combining steganography with encryption, the architecture provides multiple layers of security, making it robust against modern steganalysis attacks. This structure is suitable for secure communication, data privacy, digital watermarking, and other applications where confidential information must be transmitted safely.

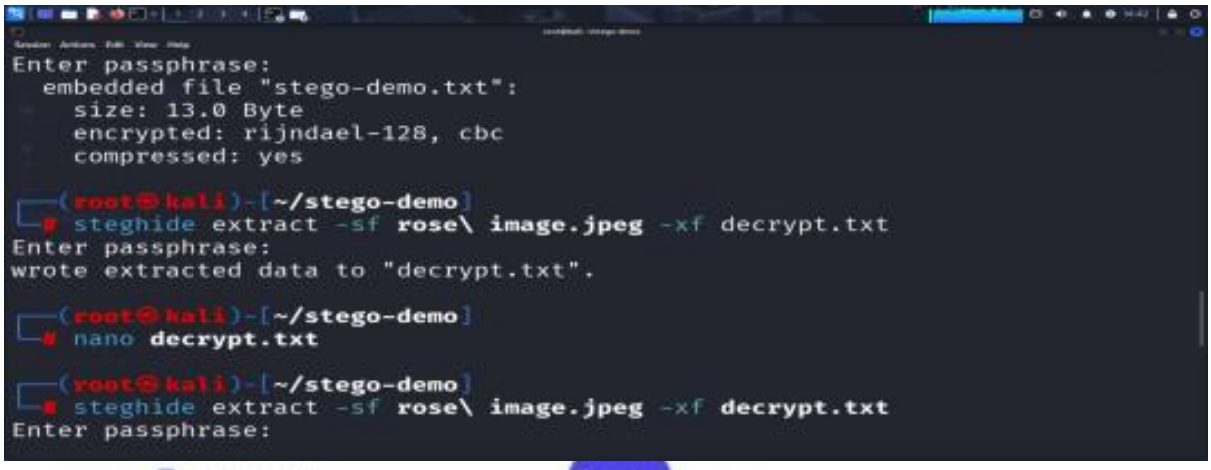
V RESULTS & OUTPUT

Steghide Installation

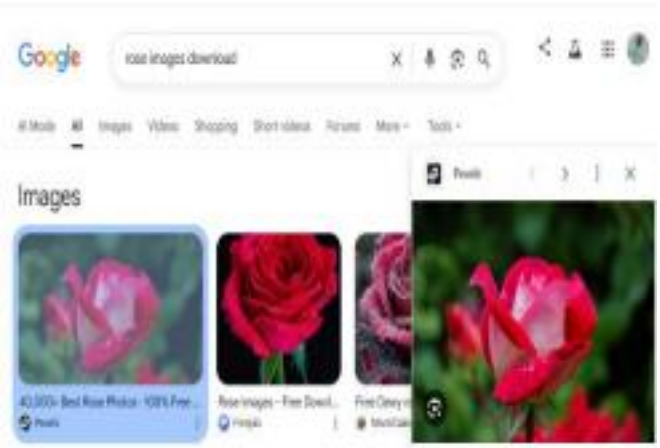


Download and Save image in Firefox [New Terminal]


(root㉿kali)-[~]
ls
cupp linux-wifi-hotspot secret.txt seeker Socialbrute stego-de
(root㉿kali)-[~]
cd stego-demo1
(root㉿kali)-[~/stego-demo1]
echo "hellohackers" > stego-demo1.txt
(root㉿kali)-[~/stego-demo1]
cp /home/kali/Downloads/rose\ image.jpeg /plain.jpeg
(root㉿kali)-[~/stego-demo1]


Enter passphrase:
embedded file "stego-demo.txt":
size: 13.0 Byte
encrypted: rijndael-128, cbc
compressed: yes
(root㉿kali)-[~/stego-demo]
steghide extract -sf rose\ image.jpeg -xf decrypt.txt
Enter passphrase:
wrote extracted data to "decrypt.txt".
(root㉿kali)-[~/stego-demo]
nano decrypt.txt
(root㉿kali)-[~/stego-demo]
steghide extract -sf rose\ image.jpeg -xf decrypt.txt
Enter passphrase:


Download
QuickStego for Windows
Editors' Review
Opera
DOWNLOAD


Google
Images

Vi CONCLSUION

In this project, a secure method for hiding confidential information inside digital images using steganographic techniques has been developed. The system uses image steganography to embed secret data within a cover image while maintaining the visual quality of the image. By using techniques such as the Least Significant Bit (LSB) method, the secret data can be hidden in a way that is not noticeable to the human eye.

The project demonstrates how steganography can be used to enhance data security and privacy in digital communication. The hidden data can be safely transmitted through images without revealing the presence of the secret message. In addition, applying encryption techniques further increases the level of security by protecting the hidden data from unauthorized access.

Overall, the proposed system provides an efficient and secure approach for data hiding while preserving image quality and ensuring reliable extraction of the hidden information. This technique can be useful in various applications such as secure communication, military data transfer, digital watermarking, and protection of sensitive information

REFERENCE

[1] Kumar, R. D., Prudhviraj, G., Vijay, K., Kumar, P. S., & Plugmann, P. (2024). Exploring COVID-19 through intensive investigation with supervised machine learning algorithm. In Handbook of Artificial Intelligence and Wearables (pp. 145-158). CRC Press.

[2] Swathi, B., Vijay, K., Sushanth Babu, M., & Dinesh Kumar, R. (2024, November). Machine Learning Techniques in Cloud Based Intrusion Detection. In The International Conference on Artificial Intelligence and Smart Environment (pp. 557-564). Cham: Springer Nature Switzerland.

[3] Sv satyakrishna, shirisha rangu ,bhargavi nalacheruve.(2024) Prospective investigation on colorectal cancer with SMOTE on machine learning Algorithm

[4] Dr.G.Vishnu Murthy, BhargaviNalacheruve 1Professor, Department of computer Science & engineering, Anurag University, TS, India. 2Student, Department of computer Science & engineering, Anurag University, TS, India.

[5] V. N. S. Manaswini, K. K, C. Nigam, S. S. Ali, R. Niranjana, and Suman, “Real-Time Object Detection in Drone Surveillance Using YOLOv5,” in Proc. 2025 3rd Int. Conf. IoT, Communication and Automation Technology (ICICAT), Gorakhpur, India, 2025, pp. 1–6, doi: 10.1109/ICICAT68430.2025.11414670.

[6] B. Soundarya, V. N. S. Manaswini, M. Ayyakrishnan, R. D. Kumar, “Contextual Analysis of Big Data Analytics in Intelligent Transportation Frameworks,” in Intersection of Artificial Intelligence, Data Science, and Cutting-Edge Technologies: From Concepts to Applications in Smart Environment, Lecture Notes in Networks and Systems, vol. 1353, Cham: Springer, 2025, doi: 10.1007/978-3-031-88304-0_79.

[7] R. D. Kumar, V. N. S.Manaswini, "Applications of blockchain in smart cities: detecting fake documents from land records using blockchain technology," in Blockchain for Smart Cities, Elsevier, 2021, pp. 105–117, doi: 10.1016/B978-0-12-824446-3.00017-X.

[8] Tejavath Veeramma, Badarla Anil, Guguloth Ravinder, "An advanced movie recommender using collaborative filtering and sentiment analysis," International Research Journal of Modernization in Engineering Technology and Science, vol. 7, no. 7, July 2025, doi: 10.56726/IRJMETS81618.

[9] Ravi Kumar Banoth, Ramana Murthy B V, "Automatic crop recommendation system using LightGBM and decision tree machine learning models," Journal of Machine and Computing, vol. 5, no. 1, pp. 343, Jan. 2025, doi: 10.53759/7669/jmc202505026.

[10] Ravi Kumar Banoth, Dr. B.V. Ramana Murthy, "Smart agriculture through IoT and machine learning for analyzing carbon footprints," in Proc. Int. Conf. Computer Science and Communication Engineering (ICCSCE), Apr. 2025.

[11] Ravi Kumar Banoth, B. V. Ramana Murthy, "Soil image classification using transfer learning approach: MobileNetV2 with CNN," SN Computer Science, vol. 5, art. no. 199, 2024, doi: 10.1007/s42979-023-02500-x.