Enhancing Secure Data Transfer Through Image Steganography

R.Mahashree[1], Dr.Vaidehi.V[2]
[1]Dept of Computer Applications
[2]Professor, Dept of Computer Applications
[1, 2] DR. MGR. Educational & Research Institute,Chennai-95

Abstract- *This paper explores the enhancement of secure data transfer using image steganography. Image steganography involves embedding secret information within a digital image in such a manner that its presence is concealed, thereby providing a robust method for covert communication. Various techniques for data embedding, such as Least Significant Bit (LSB) insertion, transform domain methods, and masking and filtering, are discussed. The process of embedding and extracting data, along with considerations for maintaining security, imperceptibility, and robustness, are outlined. Applications in confidential communication, digital watermarking, and covert storage are examined, along with current challenges and future directions in the field.*

Keywords- Image steganography, secure data transfer, LSB insertion, transform domain methods, digital watermarking, covert communication, data embedding, data extraction, steganalysis resistance, robust data hiding.

I. INTRODUCTION

The mentioned algorithms are studied simultaneously and in the same environment for various factors such as encoding and decoding time interval, SNR, histogram and MSE. is that the execution time of RSA is more than the other mentioned algorithms. This system explores both steganographic techniques and compression algorithm. This explains the embedding and unpacking algorithm. Here is a comparison between two different techniques. First, the LSB algorithm is used without encryption and compression. In another technique, the secret message is encrypted and the LSB is used to convert the image to the frequency domain using a DCT algorithm [1]

System work focuses on the process, application and limitations of steganography. It introduces various steganographic image file formats such as JPEG, BMP, PNG and TIFF and color models for image formats such as CMYK model, RGB model, HSL, HSV, NCS, DCT, DWT, LSB, etc.existing models undergo modified controls based on parameters such as self-image observability, technical resources and security considerations. An acidic range of PSNR readings indicates better quality of the brace image. The review shows that JPEG(DCT/DWT) algorithms are more vulnerable to attacks and very averse to stegaanalysis. BMP spatial domain techniques have higher power [2]

The system goes through various compression methods and encryption techniques. Most web applications use image or video files to send content. Due to limited bandwidth, compression methods apply and user encryption is performed. Apt's solution is a combination of encryption and compression technologies. The proposed system controls compression techniques such as Huffman coding, Run-length coding, Arithmetic coding and Lempel-Ziv-Welch compression. Lossless compression includes Huffman coding and discrete cosine transform, while lossless compression includes LZW and Run-length coding. It also explores various encryption techniques such as Caser Cipher, Data Encryption Standard and Rivest Cipher [3]

The study was conducted to test image compression and encryption algorithm, which are divided as follows: encryption followed by compression, compression followed by encryption, cooperation between encryption and compression. As a result, it was assumed that the best compression and encryption standards were achieved by encrypting the image first followed by the compression technique. The article explores the encryption techniques AES, RSA, DES, 3DES and Blowfish and the steganographic algorithm LSB. Cryptographic algorithms are Java programmers imported into the MATLAB environment image Steganography [4]

This system explores both steganographic techniques and compression algorithm. This explains the embedding and unpacking algorithm. Here is a comparison between two different techniques. First, the LSB algorithm is used without encryption and compression. In another technique, the secret message is encrypted and the LSB is used to convert the image to the frequency domain with a DCT algorithm. From the test result, we know that we have to hide the secret data while minimizing its size, which enables better security. MSE and

PSNR are used to evaluate the performance of the two approaches. The test result shows that using LSB and DCT effectively reduces the number of bytes in files, so they can be sent faster and take up less disk space [5]

II. LITERATURE SURVEY

According to**LasyaVoleti**.et al., 2021Information is processed electronically thanks to the development of the ICT industry. Therefore, privacy and security were a major concern. It can also be used to encrypt messages that are embedded in a digital host before being sent over the network so that their existence is inherently uncertain. The mechanism of hiding and encrypting sensitive data can be extended to copyright protection of interactive media, audio, video and images. It can also be used to protect the integrity of digital documents. This is the practice of hidden touch. The goal is to deliver documents and create many uses where the hidden message is encrypted with the veggie chip algorithm and stored as an image with LSB steganography [6].

According to **Rashika Joshi**.et al., 2022 Information encryption and falsification have evolved with the development of technology and data transmission. This creates a need for better and more advanced data transfer methods. Data transmission is an essential task these days, and knowing how to keep that data secure is just as important. The article uses packet steganography to ensure complete data transmission. Often the password can be used to encode the payload into the cover image. Here, data is encrypted using hashing and encryption techniques, SHA-256 and AES. The passwords used for encryption were used after the logical XOR operation. So the data is encrypted twice, using the XORed password the first time and the second input password the next time [7].

According to**Hamid Ali**.et al., 2022 Steganography is a technique where a person hides information in digital media. The message sent using this technology is so secret that other people cannot even imagine the existence of this information. This article requires the development of a mechanism to communicate with individuals hiding information from the rest of the group. Digital images, based on their availability, are the most suitable components for use as transmitters compared to other objects available on the Internet. The proposed technique encrypts the message inside the image. There are several steganographic techniques for hiding the information hidden in photos, some more complex than others, and each has its own strengths and weaknesses [8].

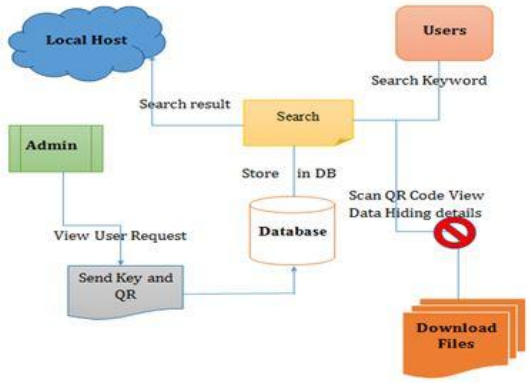
According to**S Anusooya**.et al., 2023The using encryption and decryption methods. The old technical steganography method does not improve the data hidden in the images, because the encryption and decryption uses 1-bit to 0.05-bit storage, and the shallow areas hide the information in the images, so the information is hidden by the size and scraps. of the picture. picture Hackers can easily hack information hidden in images pixel by pixel or bit by bit. So a proposed system, new technique or methods is needed. The proposed solution improves the information hidden in images by combining CNN deep learning techniques with steganography [9].

According to **Kyrylo Chernov**.et al., 2024This study explores an innovative application of direct sequence spread spectrum (DSSS) technology in the field of image steganography, known as spread spectrum image steganography (SSIS). Interpreting the cover image as noise on the communication channel, SSIS uses the anti-noise properties of broadband communication systems to effectively hide the information contained in the images. We are focused on developing new hash sequence classes with desirable entity and correlation properties that significantly impact SSIS performance. We propose an information hiding method that processes broadcast sequences directly, resulting in minimized cover image distortion and increased robustness to message detection[10].

III. PROPOSED SYSTEM

The proposed system for enhancing secure data transfer through image steganography involves a multi-step process designed to ensure both the concealment and robustness of the hidden data. The system begins with the selection of an appropriate cover image, chosen based on its size and complexity to adequately mask the secret data. The secret data is then preprocessed, which may include encryption and compression to further secure and optimize the data for embedding. Using techniques such as Least Significant Bit (LSB) insertion or transform domain methods like Discrete Cosine Transform (DCT), the data is embedded into the cover image in a manner that minimizes visible distortion. The resulting stego image, which now contains the hidden data, is then ready for transmission over secure or insecure channels. On the receiving end, the system reverses the process, extracting the hidden data from the stego image using the same algorithmic approach and decryption keys if necessary. This system emphasizes maintaining the balance between data capacity, imperceptibility, and resistance to detection and attacks, ensuring that the secret data remains confidential and intact throughout the transmission process.

ARCHITECTURE DIAGRAM:



Explanation:

1.User Interface Layer: This is where users interact with the system, upload images, and input the data they wish to hide.
2.Processing Layer: This layer handles the core functionality of steganography – embedding and extracting data within images.
3.Security Layer: This ensures the data is encrypted before embedding to provide an extra layer of security.
4.Storage Layer: This manages the storage of images with hidden data, including databases or cloud storage.
5.Transmission Layer: This handles the secure transmission of steganographic images over the network.

IV. RESULT AND DISCUSSION

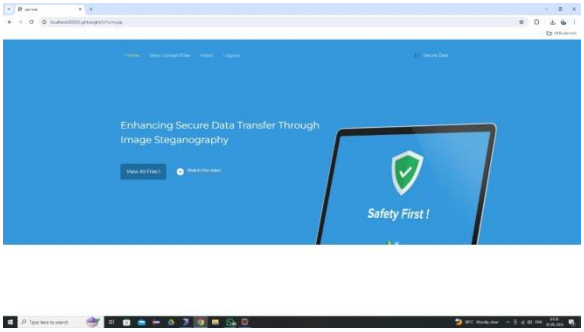


FIG.1 HOME PAGE

'The home page serves as the initial interface for users interacting with the system. It provides an overview of the system's functionality and allows users to navigate to different sections such as user sign-in, file upload, and file request information. The layout is designed for ease of use, ensuring that users can quickly access the features they need. The home page also includes links to relevant resources and support.

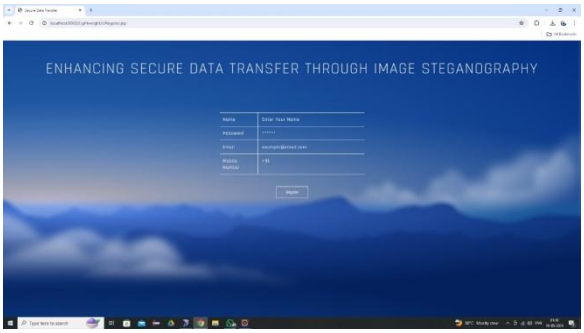


FIG.2 USER SIGNIN

The user sign-in page is where users authenticate their identity to access the system's features. This page includes fields for entering a username and password, ensuring that only authorized users can upload or request files. Upon successful authentication, users are redirected to the main interface, where they can perform secure data transfer operations. The sign-in process is protected with encryption to safeguard user credentials.

FIG.3 FILE UPLOAD STATUS

The file upload status page provides real-time feedback to users on the progress of their file uploads. This page displays information such as the file name, size, upload progress (in percentage), and any error messages if the upload fails. This feature ensures that users are informed about the status of their files and can take appropriate actions if needed. The system confirms when a file has been successfully uploaded and embedded with secret data.

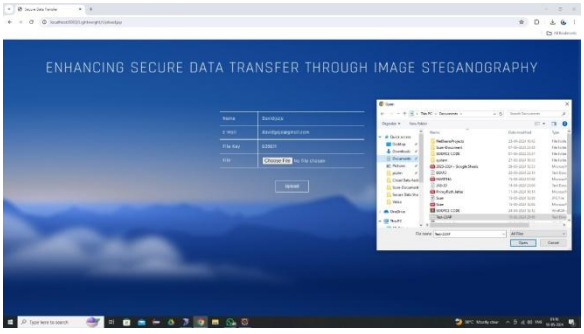


FIG.4 UPLOAD FILES

The upload files page is where users select and upload files to be embedded with secret data. This page includes a simple interface for choosing files from the local storage and specifying any additional options, such as encryption settings for the secret data. Once the files are selected, the system processes the data embedding using the chosen steganographic method. The page also provides an option to preview the stego image before finalizing the upload.

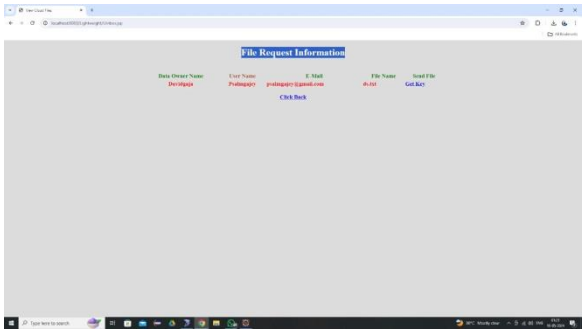


FIG.5 FILE REQUEST INFORMATON

The file request information page allows users to request access to files that have been embedded with secret data. Users can enter specific information or criteria to locate the desired file, such as file name, upload date, or unique identifiers. This page also provides details about the file, including its current status, availability, and any required decryption keys. The system ensures that only authorized users can retrieve the embedded data, maintaining the security and integrity of the information.

V. CONCLUSION

In conclusion, image steganography presents a viable solution for secure data transfer by embedding secret information within digital images in a way that is not detectable to the human eye or standard analysis techniques. By utilizing methods such as LSB insertion and transform domain techniques, it is possible to achieve a high degree of data concealment while maintaining the visual integrity of the cover image. The proposed system demonstrates a comprehensive approach to embedding and extracting data, emphasizing security, robustness, and imperceptibility. While challenges such as enhancing detection resistance and increasing embedding capacity remain, ongoing research and development in this field hold promise for increasingly sophisticated and secure steganographic methods. Ultimately, image steganography can significantly contribute to secure communication and data protection in various applications.

REFERENCES

[1] Alenezi, M. N., Alabdulrazzaq, H., & Mohammad, N. Q. (2020). Symmetric encryption algorithms: Review and evaluation study. International Journal of Communication Networks and Information Security, 12(2), 256–272

[2] Abkenar, S. B., Kashani, M. H., Mahdipour, E., &Jameii, S. M. (2021). Big data analytics meets social media: A systematic review of techniques, open issues, and future directions. Telematics and Informatics, 57, 101517

[3] Ahmad, I., & Shin, S. (2021). A novel hybrid image encryption–compression scheme by combining chaos theory and number theory. Signal Processing: Image Communication, 98, 116418.

[4] Grewal, D., Herhausen, D., Ludwig, S., &Ordenes, F. V. (2022). The future of digital communication research: Considering dynamics and multimodality. Journal of Retailing, 98(2), 224–240.

[5] Karsa, A. H. A. N., Wahyuningsih, O., Jannah, R., &Saebah, N. (2024). Web-Based Car Rental Information System At Cv. Mandarental Cirebon. Asian Journal of Engineering, Social and Health, 3(2), 374–380.

[6] LasyaVoleti, RM Balajee, Siva KoteswararaoVallepu, KarthikBayoju, Devireddy Srinivas 2021, A secure image steganography using improved LSB technique and Vigenere cipher algorithm2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), 1005-1010, 2021.

[7] Rashika Joshi, Amit Kumar Bairwa, VineetaSoni, Sandeep Joshi 2022 ,Data security using multiple image steganography and hybrid data encryption techniques,2022 International Conference for Advancement in Technology (ICONAT), 1-7, 2022

[8] Zahid Iqbal Nezami, Hamid Ali, Muhammad Asif, HananAljuaid, Isma Hamid, Zulfiqar Ali 2022, An efficient and secure technique for image steganography using a hash function PeerJ Computer Science 8, e1157, 2022

[9] R Prabhu, P Archana, S Anusooya, P Anuradha 2023, Improved Steganography for IoT Network Node Data Security Promoting Secure Data Transmission using Generative Adversarial Networks,The Scientific Temper 14 (03), 938-943, 2023

[10] OleksandrKuznetsov, Emanuele Frontoni, Kyrylo Chernov2024 ,Beyond traditional steganography: enhancing security and performance with spread spectrum image steganography Applied Intelligence, 1-25, 2024.