Secure Data Encoding and Retrieval using Steganography

Mrs. Ch. Mandakini
Assistant Professor, CSE

L. Vaishnavi
G. Narayanamma Institute of Technology & Science

B. Nithya Reddy
G. Narayanamma Institute of Technology & Science

Aparna Choudhury
G. Narayanamma Institute of Technology & Science

K. Sreeja
G. Narayanamma Institute of Technology & Science

Abstract

Following the invention of data transmission over the internet, security in communication has to be maintained. Steganography and cryptography together offer security against data being compromised, upholding integrity as well as secrecy. Cryptography secures information by encrypting it into formats that cannot be read, while steganography hides information subtly within media files. This project offers a holistic steganography platform that injects and extracts hidden data within text, sound, image, and video categories securely. It allows users to encrypt messages or conceal images in other media, enabling secure and efficient communication. With robust steganographic algorithms, data encryption, and user-friendly interface, the system offers secure decryption and reliable information hiding.

Keywords: Steganographic Algorithms, Image-Based Security, Secure Decryption, Information Hiding.

1 Introduction

With all the sensitive information being sent over the internet today, safe and private communication is a stern requirement.

Though efficient, classical cryptography is at a disadvantage with suspecting evocation by encrypting information into forms that are not understandable, potentially unknowingly inviting unwanted scrutiny.

Steganography provides a less conspicuous solution in concealing data in ordinary media files such as photographs, sound, and motion pictures. Rather than encrypting messages in the open, this method places them unseen into digital content in a way that they are invisible to the naked eye. This method makes an individual private without drawing attention, which encrypted data might carry.

This project presents an adaptable steganography platform that is designed to securely embed and retrieve sensitive information in a variety of multimedia content. Hiding text within an image or concealing one image within another, the system gives a secure and simple approach to data protection. Using advanced steganographic techniques, the platform

offers efficiency, simplicity, and low computational overhead, hence becoming a mighty tool for secure communication in the modern globalized world.

2 Literature-review

Patil and Patil (2022) proposed StegoNet-22, a deep learning-based image steganography method using a CNN-LSTM hybrid and selective LSB substitution with adversarial training. While it improves undetectability by 47%, it requires high computational resources and is not open-source, limiting its accessibility and broader usage. Zhang & Wang (2022)

The 2022 book by Ravi S. and Kumar P. is an exhaustive treatment of steganalysis and watermarking with the definition of "ε-secure" systems to quantify steganographic security. It contains 23 real-world examples with protocol sketches and cryptographic details but is limited to passive adversary models without active steganalysis.

Zhang and Wang (2022) proposed a GAN-based adaptive steganography method for JPEG images, embedding data within DCT coefficients. It is very secure with texture-aware payload distribution and a 0.003% detection rate on BOSSbase. However, it is computationally expensive and is not good at low-quality compressed images.

StegaVision (2024) employs channel and spatial attention to improve steganography, with PSCA setting having high PSNR and low error rates. It is efficient on CIFAR-10 and ImageNet with adaptive payload allocation. It performs poorly with high-resolution images, is not robust against adversarial attacks, and has high computational requirements for resource-constrained devices.

Chen et al. (2023) propose an iterative neural optimizer for high visual quality and nearly zero error 3 bpp image steganography. It adaptive refinement of embeddings is based on image features. Its peak computational complexity does not allow real-time or edge deployment and its robustness to steganalysis is unknown.

3 Methodology

The methodology of the proposed steganography system follows a structured workflow to ensure secure and user-friendly message embedding across various media formats. As illustrated in fig 1.1 the process starts with the user registering or logging in to the platform. After logging in, the user is taken to the homepage, which is where the steganographic operation begins. After that, the user is asked to choose the type of media they want to use to conceal the secret message. Text, audio, video and

image formats are some of the choices one can have. The user submits the right file once he selects the media type. The system then applies the correct steganographic algorithms for the specific media type to handle the uploaded file. The algorithms are designed to efficiently hide the data without revealing it while hiding the secret message without affecting the quality and integrity of the original media. The system displays the completed results and provides feedback once the embedding process is complete. On processing, the concealed message holding file is presented for download. This method ensures a secure, efficient, and user-friendly digital steganography process.

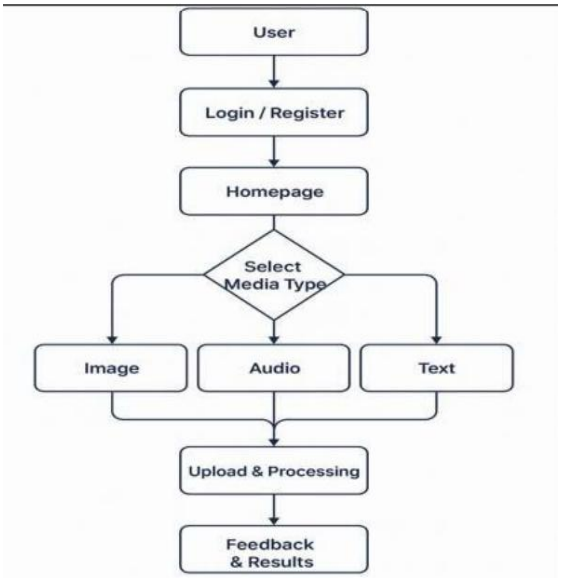

Fig 3.1 Methodology

4 Architecture

As shown in Fig 3.1, the steganographic system consists of two main parts that are the steganographic encoder and the steganographic decoder, and they are linked with a communication channel. A Cover File (X), an image, audio, or text file; a Secret Message (M) to be hidden; and a Key (K) for encryption and secure embedding are the first three inputs required. Using the key, the encoder inserts the secret message into the cover file by applying a steganographic function f(X, M, K). This ensures that the embedded message is undetectable to any observer by producing a Stego Object that closely resembles the original cover file.

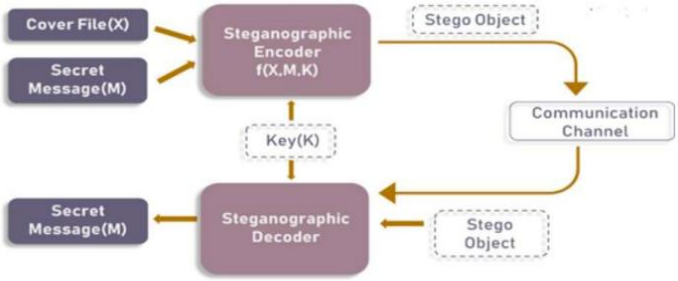

Fig 4.1 Architecture

5 Algorithms

Algorithm-1: LSB Encoding (Hiding a Message) Input: Cover media file (image/audio/video), Secret message Output: Stego media file with secret message 1. Convert the secret message into binary form (ASCII to binary). 2. Open the

cover file (image/audio/video) and read pixel or sample data. 3. Alter the least significant bit (LSB) of every pixel (for image/video) or audio sample to insert the binary message. 4. Keep inserting the message until all bits are concealed in the cover file. 5. Store the altered media file as the stego file with the secret message

Algorithm-2: LSB Decoding (Retrieving a Message) Input: Stego media file Output: Retrieved secret message 1. Open the stego media file and retrieve pixel or sample data. 2. Extract the least significant bit (LSB) of each pixel (for image/video) or audio sample. 3. Reconstruct the binary message by concatenating the extracted bits. 4. Convert the binary data back to text (binary to ASCII translation). 5. Display the extracted secret message to the user.

6 Results and Discussions

The platform includes images, audio, and video, to evaluate its capacity to securely conceal and retrieve confidential information. The trials guaranteed that the information embedded could be retrieved without triggering any noticeable alterations to the original media, which would disrupt their quality and integrity. This test verified the platform's capacity to safely embed sensitive information into diverse media types without altering their original form or audio. The results achieved across different modules were as follows:

Fig 6.1 Welcome Page

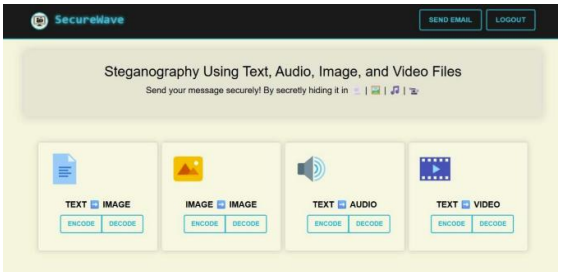

Fig 6.2 Home Page

The Fig 4 refers to the steganography tools for safely concealing messages in text, image, audio, and video files are available on the dashboard.

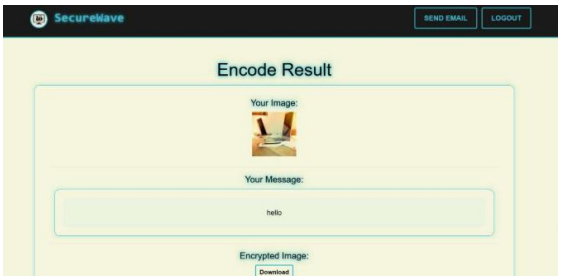

Fig 6.3 Text To Image

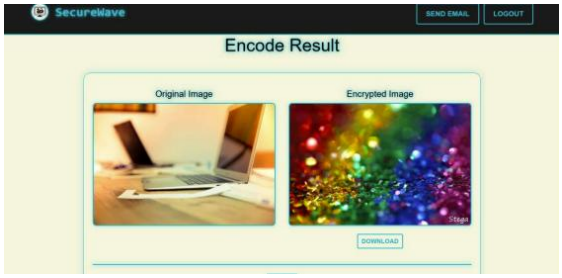

Fig 6.4 Image To Image

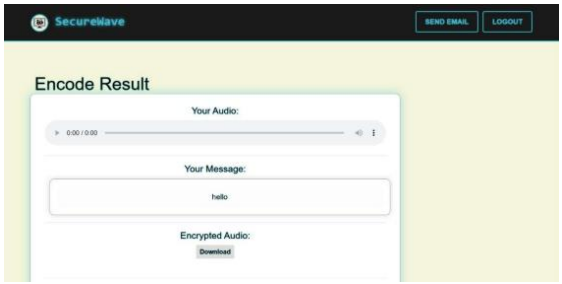

Fig 6.5 Text To Audio

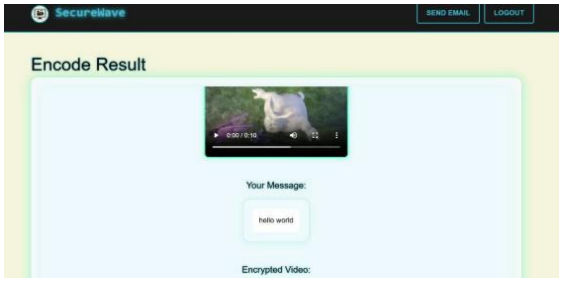

Fig 6.6 Text To Video

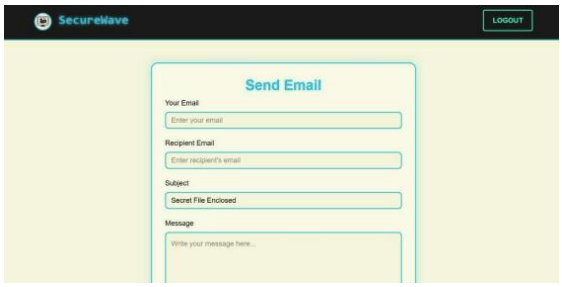

Fig Email Communication

Conclusions

This project demonstrates a secure steganography platform that allows for secure encoding and retrieval of data in various media forms—text, image, audio, and video. With the integration of cryptographic algorithms and steganographic operations, the system enhances confidentiality and data integrity without affecting the quality of the original media. The modularity of the platform, user-friendly operation, and implementation techniques like Least Significant Bit (LSB) allow for both simple and effective operation. It limits the findings in tools through capability to decode various formats as well as render uniform decoding. The tool substantially enhances the increasing requirement for safe, covert communication within today's digital age.

References

[1] Ali, S., & Ahmad, S. Enhanced LSB Steganography Technique with Adaptive Pixel Selection for Secure Data Hiding in Images. IEEE Access, 11, 45212-45225, 2023.

[2] Chen, L., & Xu, D. Secure Data Hiding in Digital Images Using LSB and Cryptographic Algorithms. IGI Global, 2023.

[3] Chen, X., Kishore, V., & Weinberger, K. Q. Learning Iterative Neural Optimizers for Image Steganography, 2023.

[4] Kaur, M., & Gupta, S. A Thorough Study on Methods of Image Steganography, 2023.

[5] Kessler, G. C. Introduction to Steganography: Methods and Applications (2nd Edition). Springer, 2023.

[6] Kumar, A., Singla, P., & Yadav, A. StegaVision: Enhancing Steganography with Attention Mechanism. arXiv preprint arXiv:2411.05838, 2024.

[7] Patil, P., & Patil, S. A Novel Approach to Image Steganography Using Deep Learning and LSB Techniques. International Journal of Computer Applications, 975, 8887, 2022.

[8] Rana, N., & Sharma, M. Steganography Based on LSB with Error Correction Mechanisms in Lossless Image Formats. Journal of Information Security and Applications, 68, 103453, 2023.

[9] Ravi, S., & Kumar, P. Data Hiding Techniques: Fundamentals and Advances in Steganography and Watermarking. CRC Press, 2022.

[10] Zhang, Y., & Wang, L. Neural Network-Based Adaptive Steganography for JPEG Images, 2022.