A Mini-Project 2 Report on

Secure Data Encoding and Retrieval using Steganography

Submitted to the Department of Computer Science & Engineering, GNITS in the Partial fulfillment of the academic requirement for the award of B.Tech (CSE) Under JNTUH, Hyderabad

By

L. Vaishnavi	22251A0519
Aparna Choudhury	22251A0533
B. Nithya Reddy	22251A0535
K. Sreeja	22251A0546

Department of Computer Science & Engineering
G. Narayanamma Institute of Technology & Science
(Autonomous) (for Women)
Shaikpet, Hyderabad- 500 104.

Affiliated to
Jawaharlal Nehru Technological University Hyderabad
Hyderabad – 500 085
May, 2025

A Mini-Project 2 Report on

Secure Data Encoding and Retrieval using Steganography

Submitted to the Department of Computer Science & Engineering, GNITS in the Partial fulfillment of the academic requirement for the award of B.Tech (CSE) Under JNTUH, Hyderabad

By

L. Vaishnavi	22251A0519
Aparna Choudhury	22251A0533
B. Nithya Reddy	22251A0535
K. Sreeja	22251A0546

under the guidance of

Mrs. Ch. Mandakini
Assistant Professor, CSE

Department of Computer Science & Engineering
G. Narayanamma Institute of Technology & Science
(Autonomous) (for Women)
Shaikpet, Hyderabad- 500 104.

Affiliated to
Jawaharlal Nehru Technological University Hyderabad
Hyderabad – 500 085
May, 2025

G.Narayanamma Institute of Technology & Science

(Autonomous) **(ForWomen)**

Approved by AICTE, NewDelhi & Affiliated to JNTUH, Hyderabad
Accredited by NBA & NAAC,anISO9001:2015certifiedInstitution
Shaikpet, Hyderabd-500104

Department of Computer Science & Engineering

Certificate

This is to certify that the Mini-Project 2 report on "**Secure Data Encoding and Retrieval using Steganography**" is a bonafide work carried out by L.Vaishnavi (22251A0519), Aparna (22251A0533), B.Nithya Reddy (22251A0535),K.Sreeja (22251A0546) in the partial fulfillment for the award of B.Tech degree in Computer Science & Engineering, G.Narayanamma Institute of Technology & Science, Shaikpet, Hyderabad, affiliated to Jawaharlal Nehru Technological University, Hyderabad under our guidance and supervision.

The results embodied in the Mini-Project 2 work have not been submitted to any other University or Institute for the award of any degree or diploma.

Internal Guide
Mrs. Ch.Mandakini
Assistant Professor, CSE

Head of the Department
Dr.A.Sharada
Professor and Head, CSE

External Examiner

G. Narayanamma Institute of Technology & Science

(Autonomous) (For Women)
Shaikpet, Hyderabad – 500 104.

Department of Computer Science & Engineering

Research Center for Cloud Computing

Certificate

This is to certify that by L.Vaishnavi (22251A0519), Aparna (22251A0533), B.Nithya Reddy (22251A0535), K.Sreeja (22251A0546) III B.Tech, has successfully completed project work in **"Research Center for Cloud Computing"** CSE Department.

The project titled **"Secure Data Encoding and Retrieval using Steganography"** that is being submitted in partial fulfillment for the award of B.Tech, Computer Science and Engineering, G.Narayanamma Institute of Technology & Science affiliated to Jawaharlal Nehru Technological University is a record of bonafide work carried out by her in our guidance and supervision.

Supervisor

Mrs. Ch. Mandakini,
Assistant Professor,
Department of CSE

CoE Incharge

Dr. Rahgavender K. V,
Associate Professor,
Department of CSE.

Head of the Department
Dr. A. Sharada,
Professor and Head
Department of CSE

Acknowledgements

We would like to express our sincere thanks to **Dr. K. Ramesh Reddy, Principal, GNITS,** for providing the working facilities in the college.

Our sincere thanks and gratitude to **Dr. M. Seetha, Professor & Dean R&D, Department of CSE**, **Dr. N. Kalyani, Professor & Dean of Innovation and Incubation Department of CSE**, GNITS, for all the timely support and valuable suggestions during the period of our project.

We extend our heartfelt gratitude to **Dr. A. Sharada, Professor & Head, Department of Computer Science and Engineering**, GNITS, for unwavering support and invaluable guidance throughout our project, providing timely assistance and insightful suggestions.

We are extremely thankful to **Dr.D.V.Lalitha Parameswari, Associate Professor mini project2 coordinator, Department of CSE**, GNITS for all the valuable suggestions and guidance during the period of our project.

We are also extremely thankful to our project coordinators **Dr. G.Malini Devi, Associate Professor and Mrs. V. Divya Raj, Assistant Professor, Department of CSE**.

We are extremely thankful and indebted to our internal guide, **Mrs.Ch.Mandakini, Assistant Professor, Department of CSE,** GNITS for her constant guidance, encouragement, and moral support throughout the project.

Finally, we would also like to thank all the faculty and staff of CSE Department who helped us directly or indirectly, parents and friends for their cooperation in completing the project work.

L. Vaishnavi	22251A0519
Aparna Choudhary	22251A0533
B. Nithya	22251A0535
K. Sreeja	22251A0546

ABSTRACT

With greater internet data transmission, providing secure communication is vital. Steganography and cryptography are a solution to that by providing protection against data integrity and confidentiality breaches. Cryptography encrypts information into unintelligible formats, and steganography hides the fact of data transmission by including it within different kinds of media files. While existing cryptograms are very secure, they become apparent from visualized artifacts and are prone to suspicion. Steganography presents a quieter option with lesser mechanisms increasing the efficiency level while lessening overhead processing.

This project presents an all-encompassing steganography platform that can embed and retrieve concealed data in text, audio, image, and video files. By encrypting sensitive data into multimedia files securely, the system provides strong data security and confidentiality. Users can encrypt plaintext messages into images, audio, and videos or conceal one image in another, offering diverse solutions for secure communication. The platform also enables effective decoding to access hidden data. With an easy-to-use interface and sophisticated steganographic methods, this system caters to the increasing need for safe and hidden data transmission on various digital platforms.

Keywords: Data Encryption, Cryptographic Techniques, Steganographic Algorithms, Image-Based Security, Secure Decryption, Information Hiding

Table of Contents

List of Figures

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.

1.1 Background of the study

As ever more sensitive information is being transferred via the internet, secure communication has been made necessary. Cryptography and steganography are two essential techniques used to ensure data security. Cryptography makes information secure by encrypting it into unreadable format but its visible signs of encryption will attract interest. Steganography, though, conceals data within multimedia files like image, audio, and video, and therefore, is less suspicious.

Traditional steganographic schemes are likely to suffer from poor capacity for embedding and supercomputational complexity. In this work, there is a holistic steganography platform for the embedding and extracting of hidden data in different forms such as text, image, audio, and video. Effective encoding and decoding enable the system to facilitate both security and convenience.

An interface that is simple to use and advanced steganographic techniques make this site provide a generic and concealed avenue of secure communication to suit the growing demand of secret data transfer during the information era.

1.2 Existing System

Steganography has been widely employed for safe data transmission, and most systems employ various mechanisms for hiding secret data in media such as images. Image steganography is one of the most widely used methods, which employs methods such as Least Significant Bit (LSB) substitution, Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT) for hiding information in images without affecting visual integrity. Image-based tools such as OpenStego, StegHide, and SilentEye are supported. Camouflage but mostly can't handle more than a single medium. Steganography through audio is another most used technique of steganography, hiding data within the audio waves using methods such as phase coding, echo concealment, and spread. Audio steganography is facilitated by some software such as DeepSound and S-Tools, but most of them are functional only in pre-determined formats and cannot encode well.

Video steganography provides greater embedding capacity because of video frame redundancy, using techniques such as motion vector modification, frame differencing, and Bit Plane Complexity Segmentation (BPCS) to hide data. OpenPuff and Camouflage tools support video steganography, but some of the current solutions are computationally expensive and unsuitable for real-time applications. Text-based steganography, although less prevalent, hides data in textual information through whitespace manipulation, syntactic changes, and Unicode-based methods. Other tools such as SNOW (Steganographic Nature of Whitespace) and SteganoGraphyX are text-based hiding solutions, and the methods they use are easier to detect since text is organized.

1.3 Challenges in Existing System

1. **Limited Format Support for Media** – Most available solutions handle only one format of media (e.g., solely JPEG images or MP3 audio), making users switch between a variety of tools to support various file formats and inducing workflow inefficiencies.

2. **Insufficient Capacity of Payload** – Classic methods severely limit the amount of data that can be concealed, usually compromising host file quality while embedding amounts larger than mere tokens, which renders real-world uses ineffective.
3. **Computationally Expensive Processes** – Sophisticated steganography processes, especially for video and high-bandwidth audio files, require too much processing power and time, making them unsuitable for real-time or mobile applications.
4. **Vulnerability to Detection** – Most existing systems employ deterministic embedding routines that can be detected by current steganalysis software, undermining the confidentiality of the concealed communications.
5. **Non-Intuitive User Interfaces** – Most professional steganography software is technically demanding to use, with complicated parameter settings and command-line interfaces that pose obstacles for common users.

1.4 Problem Statement

The application is designed to create a highly intelligent and secure platform that facilitates the embedding of sensitive data in widely used media files like images, audio, and video using sophisticated steganographic methods. This is most useful in situations where data must be exchanged covertly or in areas with widespread surveillance and data interception. The platform is crafted to enable users to embed and retrieve concealed data easily, retaining the original quality, resolution, and fidelity of the host media so as not to leave behind any traces of manipulation that could be seen or heard. Through the protection of the embedded information and the integrity of the carrier file, the platform meets the growing need for secure, nonintrusive, and high-quality digital communication in a more interconnected and susceptible digital environment.

1.5 Objectives

- To design an application that leverages advanced steganographic techniques to embed and extract sensitive data within multimedia files ensuring covert, secure, and visually undetectable communication.
- To implement a Least Significant bit-based algorithm optimized for embedding and extracting data without degrading file quality.
- To develop a user-friendly platform that offers a simple, intuitive interface with a quick registration process for new users, in which user can easily upload media files to securely embed or extract hidden data and can share the files via email.

1.6 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 among the options available. The user uploads the appropriate file after choosing the media type. After that, the system uses the proper steganographic algorithms for the particular media type to process the uploaded file. These algorithms are made to effectively conceal the data while embedding the secret message while preserving the original media's quality and integrity. The system shows the finished results and offers feedback after the embedding process is finished. After processing, the hidden message-containing file is made available for download. This approach guarantees a safe, effective, and intuitive digital steganography process.

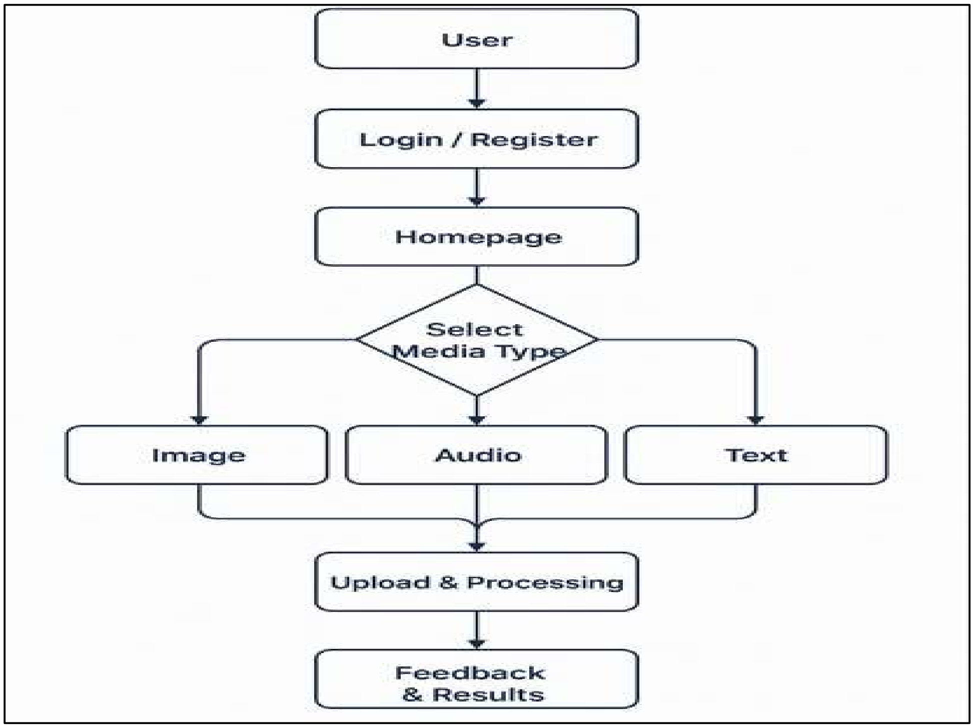


Fig 1.1: The process flow

1.7 Hardware& Software Requirements

Hardware Requirements:

- **Processor:** Intel Core i3
- **RAM:** 8GB 16GB
- **Storage:** At least 256GB SSD
- **Graphics Card:** Integrated GPU

Software Requirements:

- **Programming Languages:** Python
- **Web Framework:** Flask
- **Frontend**: HTML, CSS, JavaScript
- **Libraries & Dependencies:**
  - OpenCV
  - NumPy
  - Matplotlib
  - PIL/Pillow

  - PyAudio
  - FFmpeg
- **Development Environment:** VS Code, PyCharm, Jupyter Notebook
- **Database (if needed):** SQLite or PostgreSQL

1.8 Organization of project

The document is systematically organized into five chapters to ensure a comprehensive understanding of the work. Chapter 1 introduces the history of secure data transmission, the reasons for the study, the difficulties with current systems, and a clear definition of the problem statement and goals. It also describes the hardware and software requirements as well as the methodology used. Chapter 2 summarizes the literature survey of the various steganographic tools and techniques from earlier studies, points out the advantages and disadvantages of the current approaches, and establishes the necessity of the suggested remedy. Chapter 3 explains the system architecture thoroughly along with its functional modules, system architecture, and algorithmic techniques used for safe data encoding and retrieval. Chapter 4 concentrates on the implementation, technologies utilized, algorithms applied, and results obtained. Chapter 5 concludes the project with discusses practical implications, summarizes the key findings, and offers ideas for future improvements to increase the system's capabilities.

2. Literature Survey

A Novel Approach to Image Steganography Using Deep Learning and Least Significant bit Techniques by Patil. P., & Patil. S. in 2022 [4], created an advanced deep learning-based image steganography method called StegoNet-22, which integrates a CNN-LSTM hybrid network architecture with selective Least Significant bit replacement. The innovation is at its core adversarial training mechanism, wherein a generator network alters the cover image to embed the data and a discriminator network strives to recognize these alterations. This adversarial dynamic encourages evolutionary enhancement of both embedding and detection ability, building robustness and undetectability. The model adopts the power of deep learning to discover optimal embedding patterns instead of using fixed heuristics. Their experimentations on the BOSS base dataset reveal that the suggested method improves undetectability by 47% over conventional methods. Interestingly, the research provides detailed ablation studies that investigate the contributions of each architectural element, adding authenticity and transparency to the findings. The method, however, suffers from important limitations. The training process is computationally demanding and requires a minimum of 50,000 varied images and an 18-hour training time on a high-end RTX 3090 GPU. Such a requirement makes the approach impracticable for settings of limited computational resources. Additionally, the system suffers from a significant bias against photographic images with a 22% decrease in performance when extended to synthetic graphics. There is no open-source code has been made available by the authors, making independent verification and wider adoption by the research community difficult.

Data Hiding Techniques: Fundamentals and Advances in Steganography and Watermarking by Ravi. S., & Kumar. P. in year 2022 [6], which is a comprehensive reference text presents an in-depth overview of the data hiding landscape that covers both steganography and digital watermarking. The book presents information on different LSB variants, such as standard, randomized, and dynamic methods. Notably, Chapter 4 presents a new notion of "ε-secure" systems and offers a universal framework that defines steganographic security in terms of detectability thresholds. Such a quantitative approach allows for more scientific assessment of steganographic systems, and it represents an important theoretical breakthrough. The book also accounts for 23 implementation case studies, from medical imaging watermarking to steganographic military communications strategies. They are supported by extensive protocol diagrams, cryptographic embeddings, and security analysis, and demonstrate the real-world applicability of data hiding techniques The described evaluation framework also has limited applicability, being based on the passive attacker model and not addressing active steganalysis situations—an increasingly important factor in today's security environment.

Neural Network-Based Adaptive Steganography for JPEG Images by Zhang and Wang in 2022 introduced an adaptive steganographic approach that utilizes GANs in JPEG image embedding. The methodology is focused on the dynamic embedding of Discrete Cosine Transform (DCT) coefficients with a generator network doing the embedding and a discriminator network acting as a steganalyzer. This two-network architecture allows for a feedback loop that increases the security and adaptability of the model. It is a feature of this method and its texture-sensitive payload distribution scheme, which optimally positions more concealed data in high-frequency regions of the image—like foliage or textured regions—while minimizing changes in smooth areas like skies. When, tested against the Xu-Net steganalyzer, the system recorded an impressively low detection rate of 0.003% on the BOSSbase dataset, which highlights its strength. However, the system is not without a few caveats. Although, the training process is time-consuming and involves three individual phases: pre-training, adversarial training, and fine-tuning, each of which is computationally intensive. Furthermore, the model works very well on JPEG images with high-quality factors (over 75), its performance decreases drastically on highly compressed images with quality factors under 50.

Enhanced Least Significant Bit Steganography Technique with Adaptive Pixel Selection for Secure Data Hiding in Images by Ali, S., & Ahmad, S. in 2023, suggested a meaningful improvement over conventional Least Significant bit steganography based on an adaptive pixel selection algorithm that smartly selects embedding sites considering local image features. This selective approach enhances payload capacity but also preserves high visual fidelity with an average PSNR of 48.2 dB on several test images. The authors further propose a new distortion minimization function that minimizes embedding artifacts, especially in flat image regions, thus reinforcing the imperceptibility of embedded data. In spite of these improvements, the approach comes with a 35% computational overhead over simple Least Significant bit methods because of the extensive analysis involved in adaptive pixel selection. The algorithm has been compared mainly with simple statistical steganalysis approaches, and its performance against various sophisticated machines. In addition, the research does not consider robustness against typical image processing operations such as compression, resizing, or filtering, thus restricting its practical application in dynamic multimedia environments.

Secure Data Hiding in Digital Images Using Least Significant bit and Cryptographic Algorithms by Chen. L., & Xu. D. in 2023, suggested a hybrid security model which integrates cryptographic encryption along with LSB-based steganography. Their scheme employs a modified AES-256 algorithm, optimized for low payloads, to encrypt the cover text before hiding. Experimental benchmarks indicate the system's resistance to frequency analysis and brute-force attacks. However, this hybrid approach increases the total embedding time by a factor of 2.8 compared to conventional Least Significant bit -only methods due to the cryptographic preprocessing and randomized embedding.

Introduction to Steganography: Methods and Applications (2nd Edition) by Kessler, G. C. in 2023 established a new methodology which has a comprehensive textbook is a good introduction to study steganography for different types of media, i.e., image, audio, and video. The book defines a sound methodology of methods by classifying them according to media type and embedding domain, i.e., spatial and transform domains. The author provides mathematical models to compute embedding capacity and shows how the integration of bit-planes affects imperceptibility in the chapter dedicated to Least Significant bit methods. The book presents real-case examples that show real-world deployment, like digital watermarking systems and analysis of the SilentEye malware campaign, which used steganography for covert data exfiltration. However, the book has shortcomings, particularly in addressing recent developments. Only about 15% of the book is focused on achievements after 2018, and little is said about recent methods such as neural network-based steganography or adversarial embedding. Furthermore, although the mathematical equations are strict, they are prone to ideal assumptions, i.e., noiseless images or pixel value uniformity, which do not reflect realistic use cases. The Future Directions section is shallow and simply states future trends without real implementation examples or performance measures.

Steganography Based on Least Significant bit with Error Correction Mechanisms in Lossless Image Formats by Rana, N., & Sharma, M. in 2023, have incorporated error correction coding along with Least Significant bit steganography to increase data reliability. They use the Reed-Solomon (RS) that can correct a maximum of 16 byte-level errors per block. It is optimized for lossless image formats such as PNG, in which pixel fidelity is maintained. The system is highly robust against image distortions, with 100% message recovery even after introducing Gaussian noise (σ = 0.02) and three consecutive JPEG2000 recompressions. The authors also provide a detailed mathematical analysis of redundancy in terms of error correction vs. payload capacity and system performance, with balanced consideration to both. But in placing the RS codes, the effective payload capacity is cut down by about 12.5% since some part of the free space is taken up by redundancy. The block-based embedding approach also introduces detectable periodic patterns to the histogram of the stego-image, which could help in steganalysis. The technique is also not served well in lossy encodings such as JPEG, wherein quantization distortions contaminate embedded information outside the capabilities of the RS code to repair. Therefore, while the technique holds up very well for archive-grade or medical imaging applications, its actual utilization in day-to-day digital media contexts is severely circumscribed.

Learning Iterative Neural Optimizers for Image Steganography by Chen, X., Kishore, V., & Weinberger, K. Q. (2023) **,** paper introduces a cutting-edge deep learning approach that applies neural optimizers to iteratively refine steganographic embeddings. The authors frame the embedding task as an optimization problem and train a neural optimizer to generate low-error, high-imperceptibility encodings. Their system achieves near-zero error rates and high visual quality, even at payloads as high as 3 bits per pixel—surpassing many existing deep learning methods. The model leverages iterative refinement to adaptively adjust the embedding process based on local image features, making it suitable for a range of content types and embedding requirements. Yet, the model's strengths are counterbalanced by several practical constraints. The architecture is computationally intensive, requiring substantial memory and processing power for both training and inference. This renders it unsuitable for deployment on edge devices or in real-time applications. Its robustness against contemporary steganalysis tools remains largely unexplored, raising concerns about its vulnerability to adversarial detection methods.

A Thorough Study on Methods of Image Steganography by Kaur, M., & Gupta, S. introduced in the year 2023, has provided an extensive survey of image steganography techniques, offering a classification based on embedding domains (spatial vs. transform) and payload capacity. The paper delves into both traditional and modern approaches, comparing algorithms on the basis of imperceptibility, capacity, and computational complexity. It serves as a useful reference for researchers entering the field by outlining the core principles and evolution of steganographic strategies. The authors present a novel classification matrix that aligns algorithm choice with specific application domains, such as secure messaging or digital watermarking. However, the study has several limitations. It primarily focuses on grayscale images, thereby excluding the complexities introduced by color image steganography, which is far more relevant to real-world multimedia applications. Additionally, the review underrepresents recent developments in adaptive and deep learning-based steganography, failing to capture the rapid technological progress in these areas. The security evaluations are mostly theoretical, with no empirical testing against modern steganalysis frameworks like Ye-Net or SRNet, limiting the practical relevance of its conclusions.

StegaVision: Improving Steganography using Attention Mechanism by Kumar, A., Singla, P., & Yadav, A. in the year 2024, introduced StegaVision, an attention-enhanced steganographic framework that integrates channel and spatial attention modules into encoder-decoder architectures. The paper systematically tests various attention configurations—sequential, parallel, and hybrid—to determine the optimal balance between payload capacity, imperceptibility, and model complexity. Their results reveal that the Parallel Spatial-Channel Attention (PSCA) configuration achieves the highest PSNR (above 36 dB) and minimal bit error rates. The system is tested on CIFAR-10 and ImageNet datasets, demonstrating its adaptability and effectiveness across diverse image types. By incorporating attention mechanisms, StegaVision enables context-aware data hiding that intelligently allocates payloads based on content saliency. Despite its promise, the model is largely limited to low-resolution images (32×32 and 64×64 pixels), which may not reflect the challenges of full-resolution or real-world media. Additionally, the framework lacks integration with adversarial training or cryptographic preprocessing, potentially reducing its robustness against sophisticated steganalysis attacks. The added complexity of attention modules also increases computational burden and inference time, complicating deployment on mobile or embedded systems with limited resources.

3. Secure Data Encoding and Retrieval Model

3.1 Architecture

As depicted in Fig 3.1, the steganographic system is composed of two primary components that are the steganographic encoder and the steganographic decoder, which are connected by a communication channel. A Cover File (X), which can be an image, audio, or text file; a Secret Message (M) to be concealed; and a Key (K) for encryption and safe embedding are the first three necessary inputs. 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.

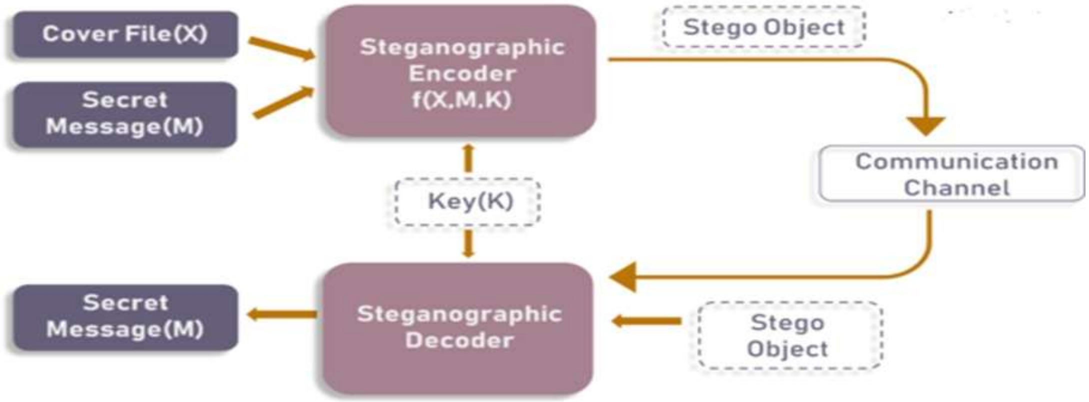


Fig 3.1: Architecture

The intended recipient then receives the stego object via the communication channel. Without sacrificing the file's quality or appearance, the Steganographic Decoder at the receiving end uses the same secret key (K) and the received stego object to extract the hidden Secret Message (M). By preserving the integrity of the cover file and preventing detection by unauthorized users, this architecture guarantees a reliable and secure method of transmitting sensitive data.

3.2 Modules

Sensitive data can be securely hidden and sent over a range of digital media, such as audio, video, and image files, using a robust multimedia steganography platform. It ensures safe file management, user authentication, and secure email transmission in addition to the steganography. Each function is logically separated into individual HTML pages, and each page corresponds to a different module performing a specific task within the system. The focus of the platform on security, simplicity, and seamless communication makes it an excellent utility for secret communication in today's digital era.

The platform consists of various modules. The modules are explained as follows:

1. The Login Module: By entering their credentials, current users can safely log in on this page. After successful authentication, access to the steganography features is granted after the username and password are checked against registered records. The goal is to safeguard the platform against unwanted access and guarantee that sensitive data can only be encoded or decoded by authorized users.

2. The Register Module: New users can create an account on the registration page by entering the required information, which includes their username, email address, and password. Users can log in to access services after successfully registering and being added to the system database. The goal is to onboard new users and keep the user environment under control for increased security and accountability.

3. Main Dashboard Module: Users are taken to the main page, which serves as a central dashboard, after logging in. Users can access various steganography options here, including: Text to Image, Image to Image, Text to Audio and Text to Video. The goal is to give users a well-structured and user-friendly interface so they can choose the steganographic operation they want.

4.Text to Image Steganography Module: With this module, users can conceal a confidential text message within an image file. To ensure that the hidden message is not visible to the naked eye, pixel manipulation techniques are employed. The platform creates a stego image with the hidden message after users upload an image and enter their secret text. The goal is to safely insert text for secret communication inside an image.

5.Image to Image Steganography Module: Users can embed a whole image inside another image using this module. To store the secret image, it slightly alters the cover image's pixel values without noticeably changing the image's appearance. Transmitting private graphical data concealed within seemingly normal images is the goal.

6.Text to Audio Steganography Module: By gently changing the audio samples, this module makes it possible to embed secret text inside an audio file. The audio sounds the same to the human ear because the changes are imperceptible. The goal is to use audio media to safely send encrypted text messages.

7.Text to Video Steganography Module: Users can incorporate text data into a video file using this module. In order to keep the hidden message hidden while the video plays normally, the text is encoded into specific frames throughout the video. The goal is to use video files to facilitate private communication.

8. The Send Email Page: This module allows users to email the stego file after the stego object (image, audio, or video) has been created. The page ensures secure end-to-end delivery of confidential data by allowing users to attach the encoded file and enter the recipient's email address. The goal is to make it easier for the stego objects to be safely transmitted via secure email channels.

4. Implementation

4.1 Technologies Used

The system is built using Python as the main programming language, which provides flexibility, strong libraries, and high support for multimedia processing. Flask is used as the web framework, which provides an easy-to-use interface for users to interact directly with the encoding and decoding operations. It supports the simple handling of HTTP requests, file uploads, and rendering of templates in order to provide a smooth user interface.

For processing image and video, the system incorporates OpenCV, a useful computer vision library, to handle frames, extract visual information, and change pixel values for steganographic embedding. NumPy is utilized for numerical computation, facilitating effective array operations necessary for multimedia file processing. Pillow (PIL) is employed for image file processing, especially for text-based steganography, where text messages are hidden within images. The Stepic library also enables encoding text messages in images by modifying pixel values.

For applying Least Significant Bit (LSB) steganography, the system uses the Stegano library, which enables messages to be concealed in images and video frames without impairing visual quality. For audio steganography, the Wave module is employed to handle WAV files, adjusting the least significant bits of audio samples to encode messages without degrading sound quality.

The system uses file-based storage to efficiently handle uploaded and processed media files. This provides seamless access to encrypted and decrypted files, making it easy to retrieve and process. Through these technologies, the system efficiently hides messages in multimedia files without compromising security, reliability, and usability.

4.2 Least Significant Bit Algorithm

Algorithm for Least Significant Bit (LSB) Steganography

The system mainly uses the Least Significant Bit (LSB) steganography method to hide and retrieve secret messages from images, videos, and audio files. Below are the algorithms for encoding and decoding messages with LSB steganography in step-by-step procedure.

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.

Explanation of the algorithm: This algorithm explains how to conceal a secret message in a cover media file, like an image, audio, or video, using the fundamental Least Significant Bit (LSB) steganography technique. Using ASCII encoding, the secret message is first converted from text to binary, with each character becoming an 8-bit binary string. The cover media then incorporates this binary data.

Each sample in audio contains amplitude values, and each pixel in images or videos contains color channel (e.g., RGB) values. Usually, these values are kept in binary format. Each pixel component or audio sample's least significant bit is changed by the algorithm; this bit change has little impact on the media's appearance or sound, making the modification nearly imperceptible to the human senses.

The algorithm works by successively substituting a bit from the binary message for each pixel's or sample's LSB. Until the complete binary message is embedded, this process keeps going. Only a tiny percentage of the media files are altered if the message is brief. The altered media file, which now includes the secret message, is saved as a stego file after embedding is finished. Because of its ease of use and minimal perceptual impact, this technique is frequently employed in watermarking and secure communication.

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

Explanation of the algorithm: This algorithm describes how to extract a hidden message from a stego media file (an image, audio, or video) using LSB steganography. The stego file's pixel or sample data's least significant bits (LSBs) are embedded with a secret message.

Opening the stego file and reading its media data—audio samples in sound files and pixels in pictures or video frames—is the first step. Binary values are stored in each of these components. In the same order as during embedding, the algorithm extracts the LSB from each pertinent value one at a time. The original binary message is then recreated by sequentially concatenating these bits.

Since each ASCII character is represented by eight bits, the binary string is separated into 8-bit chunks after it has been obtained. The original hidden message is then revealed by converting these 8-bit segments back to their corresponding ASCII characters. The user is then presented with the entire reconstructed text. Knowing when the message ends, which could be determined by a delimiter or message length—is essential to this technique. Because it is easy to use and can recover messages without significantly changing the original media, LSB extraction is frequently used in digital steganography.

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:

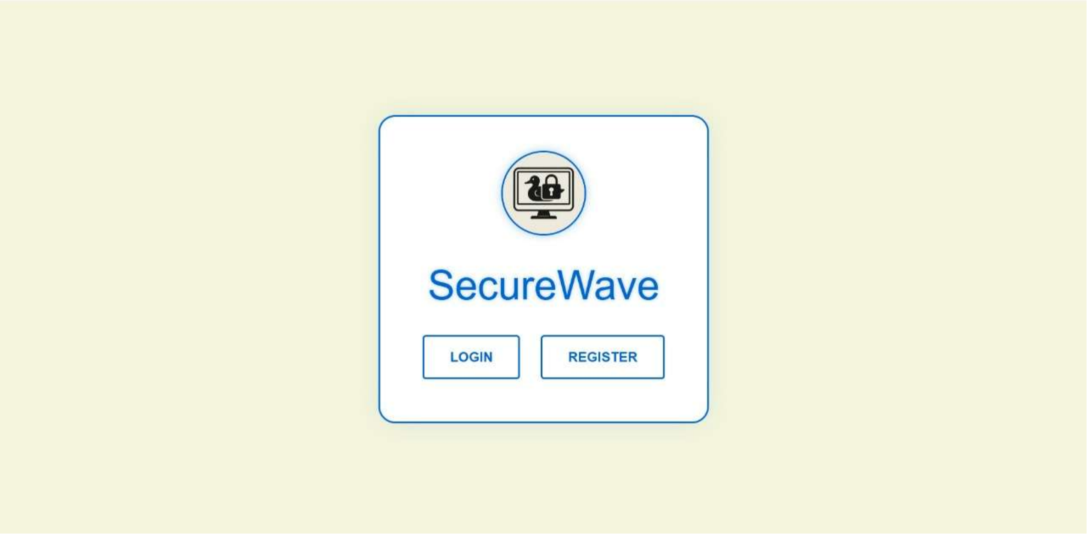
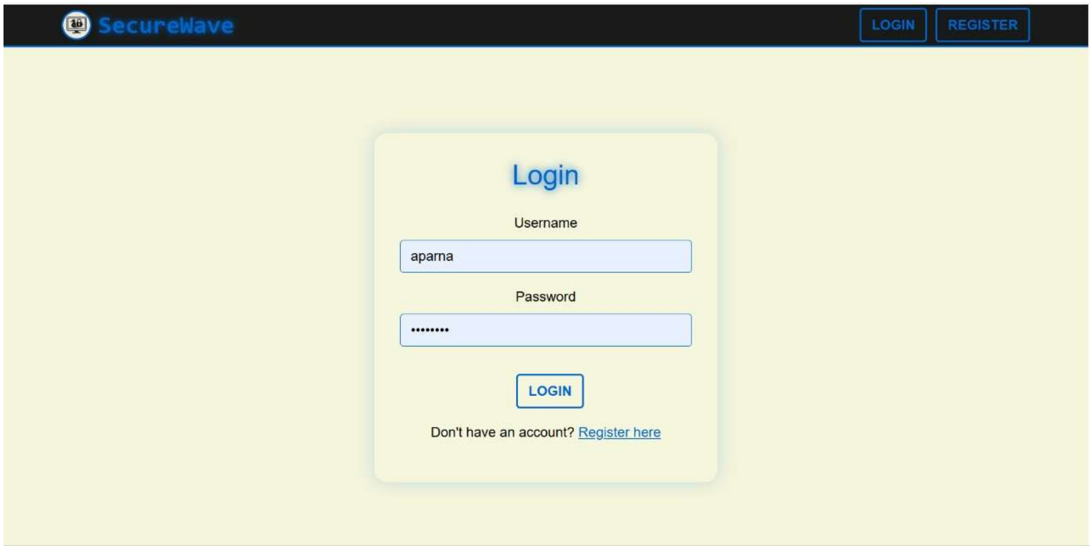


Fig 5.1 Welcome Page

The fig 5.1, explains the users about the interface that takes users through the platform's features and functionalities. It provides simple navigation to login, registration, and an outline of the platform's capabilities, making the onboarding experience seamless.



Login

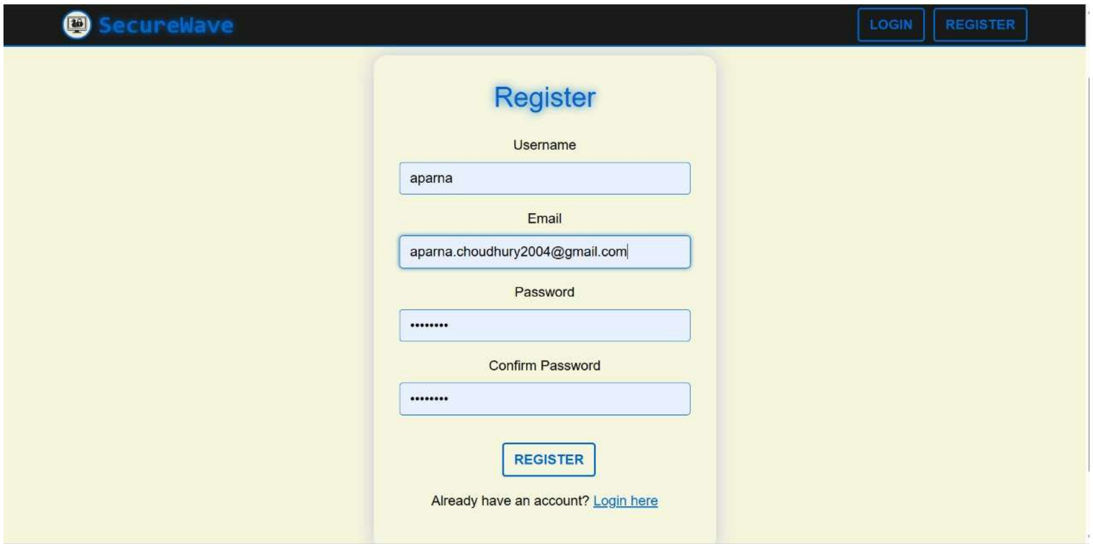
Username: aparna

Password: ••••••••

Don't have an account? Register here

Fig 5.2 Login Page

Users can safely access their accounts on the web application's login page as in fig 5.2. It has a Login button and text box for entering a username and password. To keep the interface neat and easy to use and offers a registration link for new users to register.



Register

Username: aparna

Email: aparna.choudhury2004@gmail.com

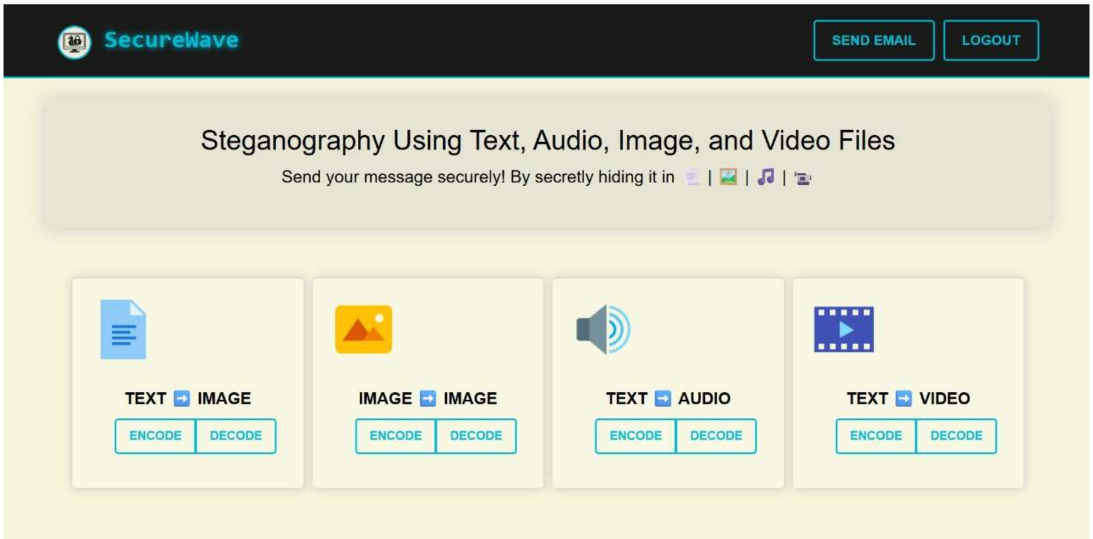
Password: ••••••••

Confirm Password: ••••••••

Already have an account? Login here

Fig 5.3 Register Page

In the fig 5.3 consists of fields such as username, email address, and password, new users can create an account. While the link below takes current users to the login page, a Register button submits the information. A seamless onboarding process is ensured by the interface's simplicity and focus on the user.



Steganography Using Text, Audio, Image, and Video Files

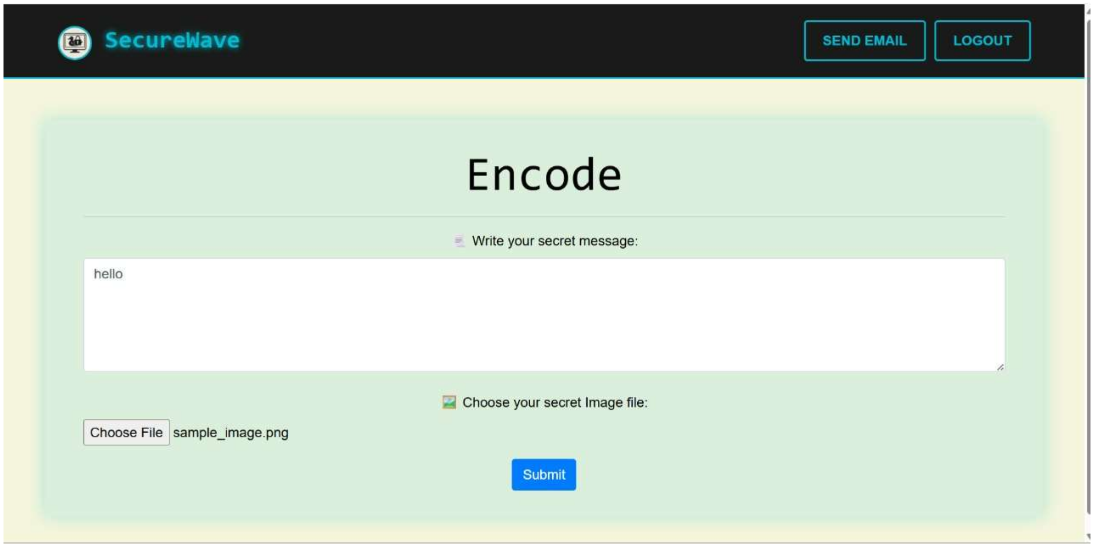
Send your message securely! By secretly hiding it in | | |

Fig 5.4 Home Page

The fig 5.4, refers to the steganography tools for safely concealing messages in text, image, audio, and video files are available on the dashboard. Text to Image, Image to Image, Text to Audio, and Text to Video are the four encoding / decoding options available to users. The user-friendly interface uses hidden data embedding to facilitate secure communication.

1. Text to Image:

Image files were successfully used to embed and retrieve the secret text. The final stego images had no discernible pixel-level distortions that could be seen with the naked eye, and their visual quality was very similar to that of the original cover images.



Encode

Write your secret message:

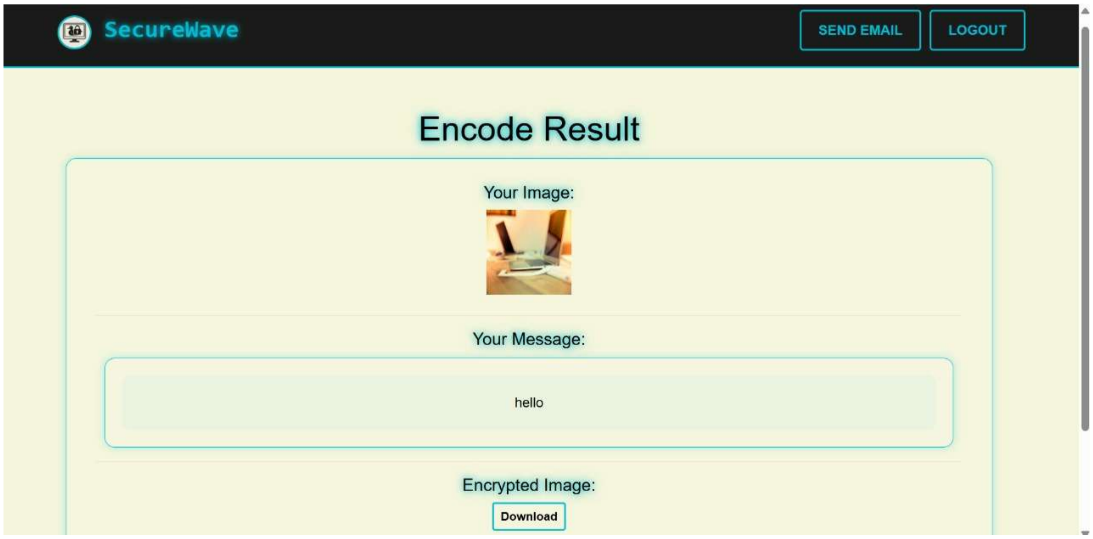
hello

Choose your secret Image file:

Choose File sample_image.png

Fig 5.5 Text to Image Encode

The fig 5.5 explains how users can insert a secret message into an image file using the encode interface. To begin encoding, users type their message into a text box, choose an image file, and press the Submit button. With the help of image-based steganography and a clear, intuitive design, this tool guarantees safe message hiding.



Encode Result

Your Image:

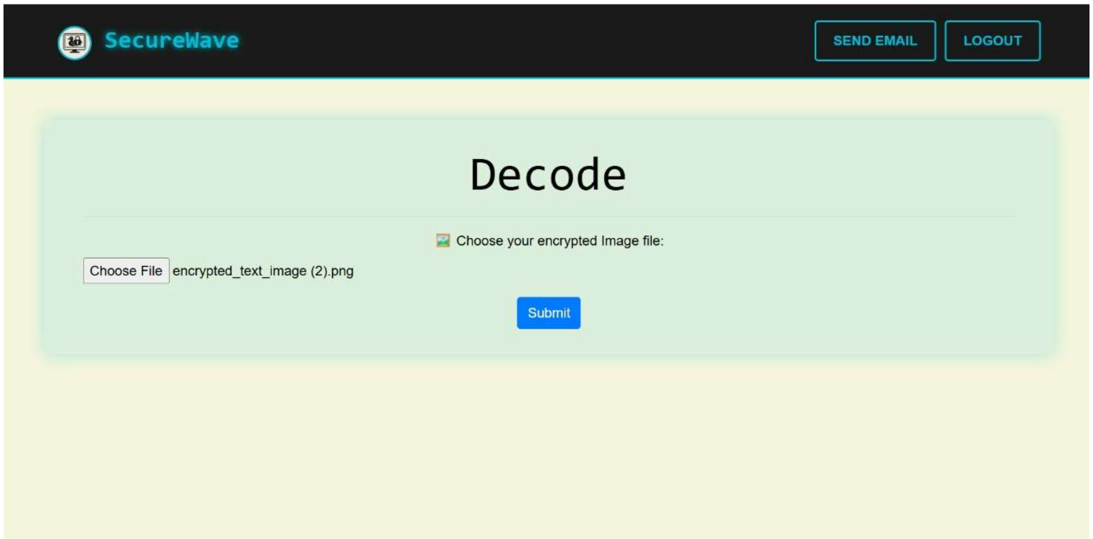
Your Message:

hello

Encrypted Image:

Fig 5.6 Text to Image Encode Result

The fig 5.6 shows how original image, the secret message that is embedded, and a button to download the encrypted image are all shown on the encode result page. Users can safely store or distribute hidden messages within picture files thanks to this confirmation of successful steganography.



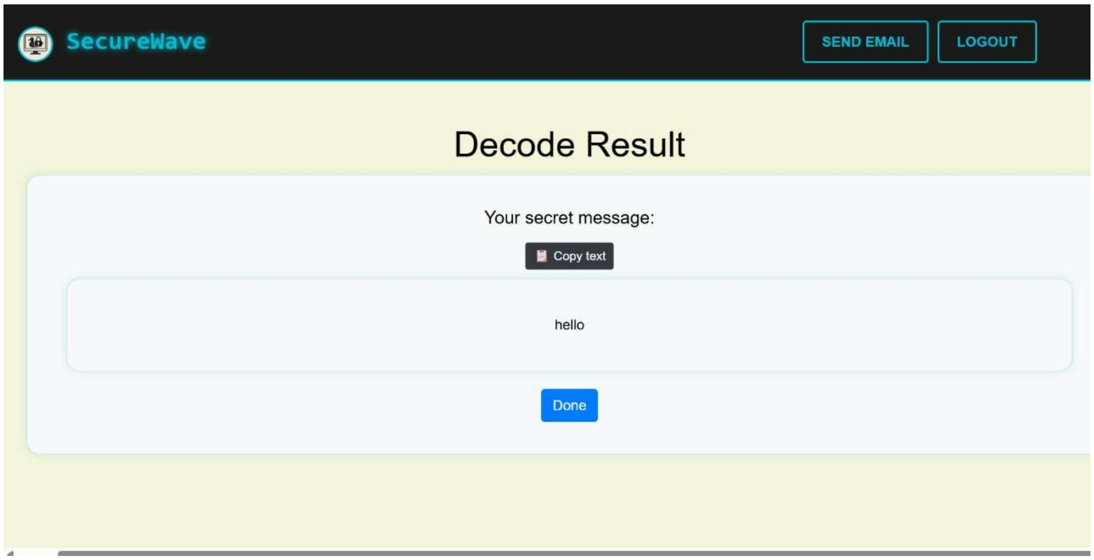
Decode

Choose your encrypted Image file:

encrypted_text_image (2).png

Fig 5.7 Text to Image Decode

The fig 5.7 explains how users can extract hidden messages from encrypted image files using the decode interface. To recover the hidden text, users use the Choose File button to upload the encoded image, then click Submit. This feature's straightforward and intuitive design facilitates secure message recovery.



Decode Result

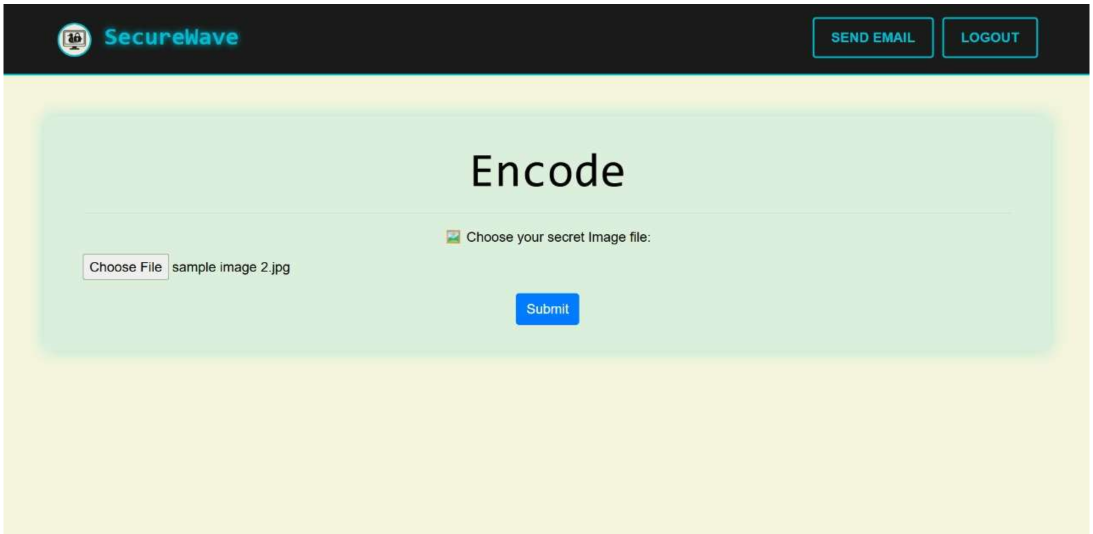
Your secret message:

hello

Fig 5.8 Text to Image Decode

2. Image To Image:

In effect, a whole image was concealed inside another image. When compared to the cover image, the resulting stego image showed very slight visual differences. During decoding, the hidden image was precisely and uncorruptedly recovered.



Encode

Choose your secret Image file:

sample image 2.jpg

Fig 5.9 Image to Image Encode

The fig 5.9 explains about a file selection field enables users to select an image to be utilized for concealing information. After selecting, a straightforward action button triggers the encoding process to prepare the file for safe conversion.

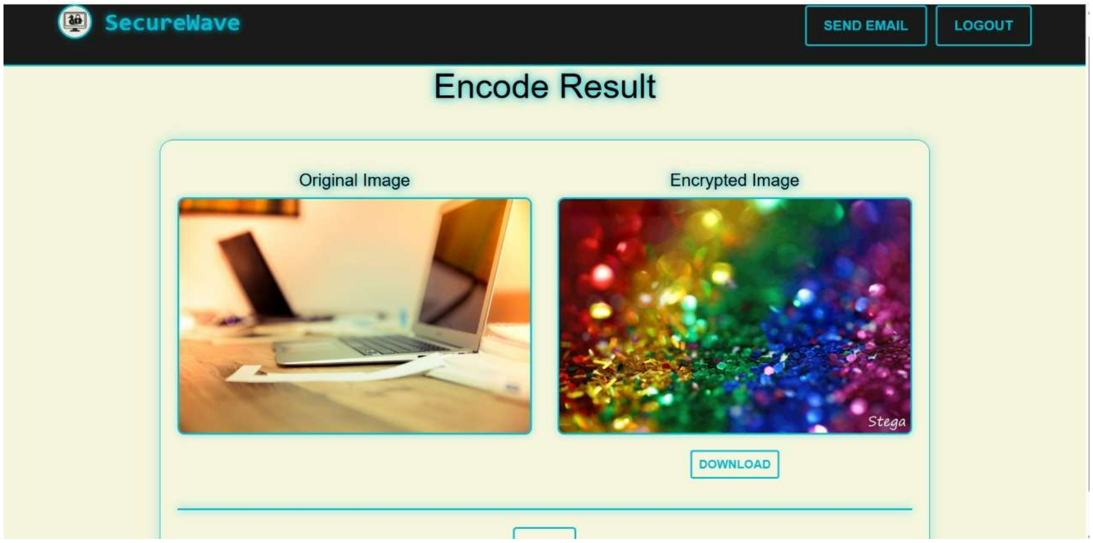


Fig 5.10 Image to Image Encode Result

The fig 5.10 explains the result, with the original image on the left and the encrypted image on the right, which includes the hidden data. A save modified option is available for saving the altered image.

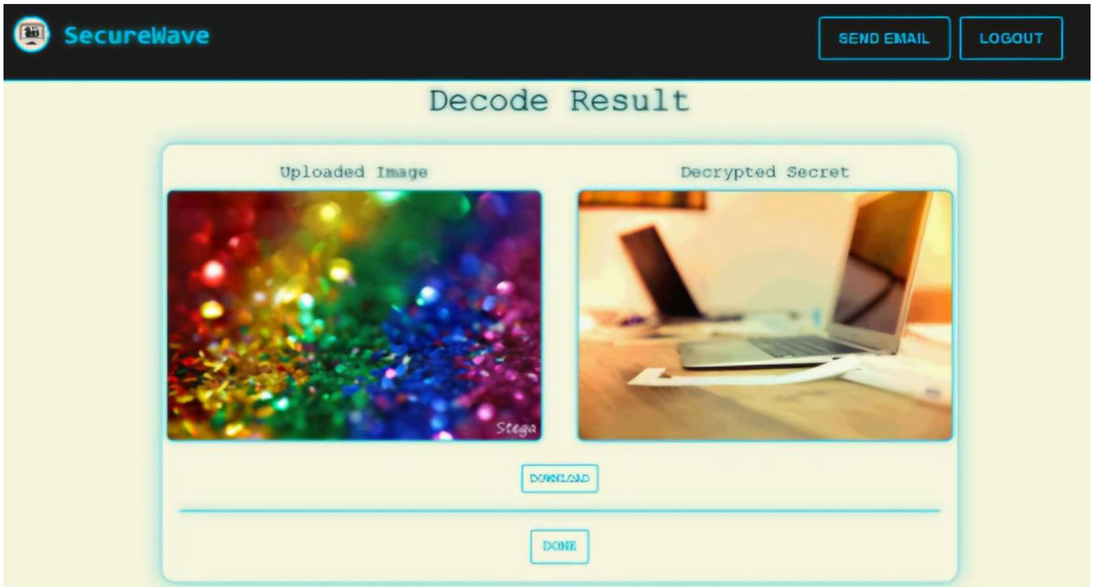
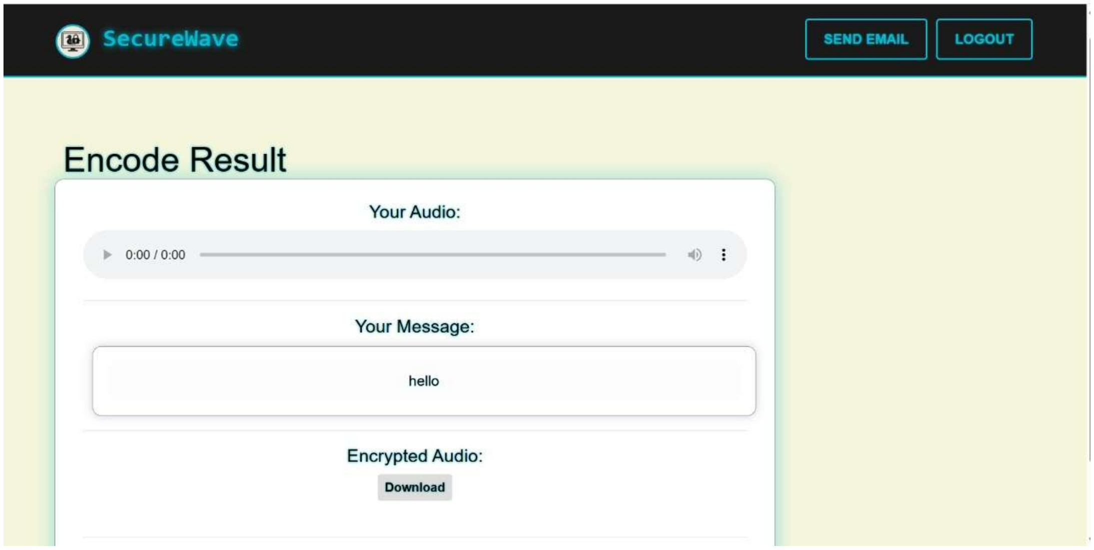


Fig 5.11 Image to Image Decode Result

The fig 5.11 shows how the concealed content is visible. The filtered image is displayed on the left, whereas the retrieved original image is shown on the right. A save feature allows users to access the unveiled content for future use.

3. Text to Audio:

Without affecting the audio files audibility, secret text was incorporated into them. Before and after the embedding procedure, the audio files were the same. Without any data loss, the concealed messages were fully decoded.



Encode Result

Your Audio:

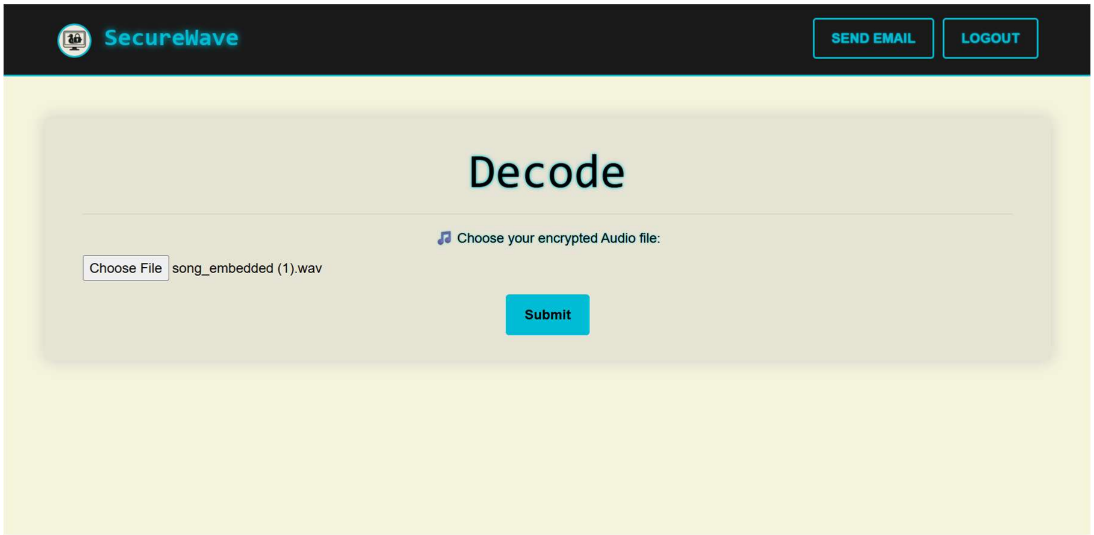
Your Message:

hello

Encrypted Audio:

Fig 5.12 Text to Audio Encode Result

The fig 5.12 shows how an audio segment plays back in conjunction with a displayable text message. The message here is "hello", which has been stored within the audio file and is presented for secure download in encrypted form.



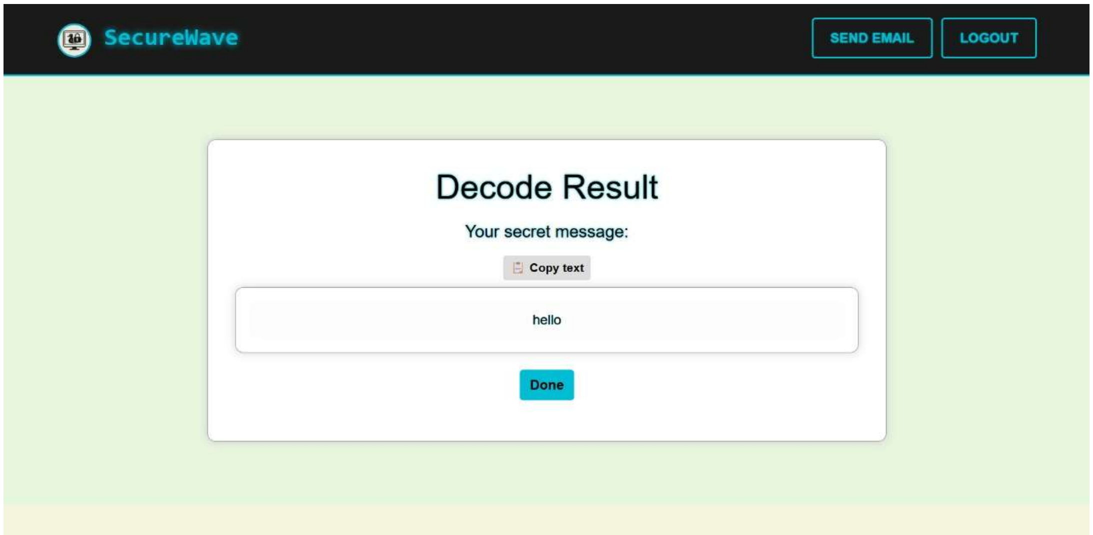
Decode

Choose your encrypted Audio file:

song_embedded (1).wav

Fig 5.13 Text to Audio Decode

A encrypted audio file is chosen to conceal information is shown the fig 5.13. When the file is selected and submitted, the decoding process extracts the stored secret.



Decode Result

Your secret message:

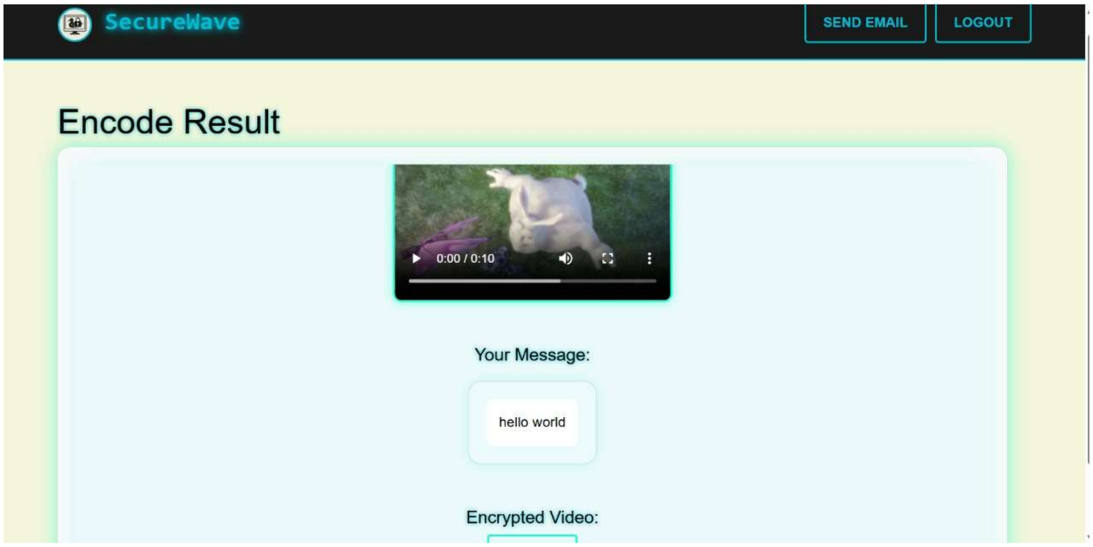
hello

Fig 5.14 Text to Audio Decode Result

The embedded message within the audio file is successfully decoded and displayed is shown in the fig 5.14. The message "hello" is displayed with a copy option, indicating the decoding was successful.

4. Text to Video:

Video frames were successfully encoded with secret text. The video continued to play smoothly and unaltered, and the decoding process successfully extracted the hidden text. The size and quality of the video files were barely affected by the embedding process. The integrity of the video and the hidden content was guaranteed since the decoded message was recovered undamaged.



Encode Result

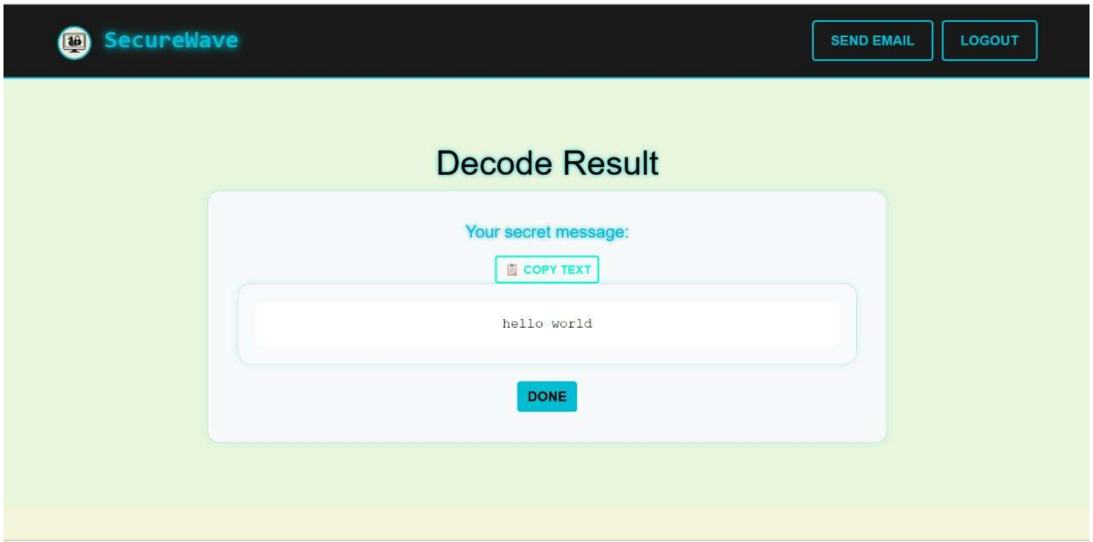
Your Message:

hello world

Encrypted Video:

Fig 5.15 Text to Video Encode Result

The fig 5.15, displays a video clip along with the message to be concealed, "hello," that has been placed within the video content. The processed video, now containing the concealed message, is ready for secure download.



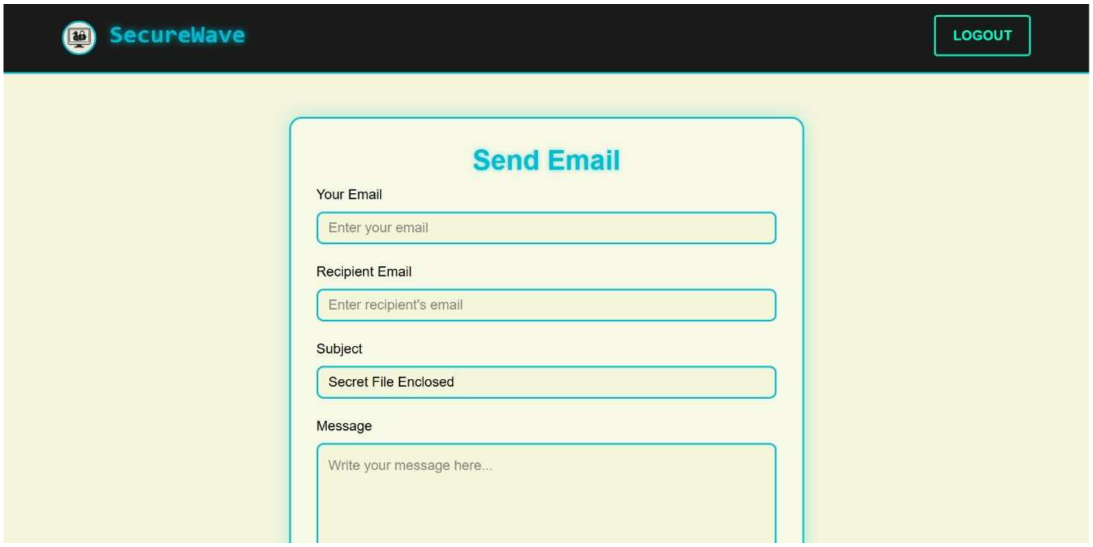
Decode Result

Your secret message:

hello world

Fig 5.17 Text to Video Decode Result

The fig 5.17, shows the hidden message in the encrypted video is extracted and read successfully. The decoded message, "hello," can be copied for use or reference to verify the process of retrieval.



Send Email

Your Email: Enter your email

Recipient Email: Enter recipient's email

Subject: Secret File Enclosed

Message: Write your message here...

Fig 5.18 Communication through mail

The fig 5.18, explains the communication through mail allows users to securely exchange information via encrypted email, ensuring privacy for account-related activities and data transmission within the platform.

6. Conclusions and Future Enhancements

6.1 Conclusion

This project successfully demonstrates a robust steganography platform that enables secure data encoding and retrieval across various media formats—text, image, audio, and video. By integrating cryptographic principles with steganographic techniques, the system enhances confidentiality and data integrity while maintaining the original media's quality. The platform's modular design, intuitive interface, and use of algorithms like Least Significant Bit (LSB) ensure both ease of use and effectiveness. It addresses limitations in existing tools by supporting multiple formats and offering reliable decoding. This solution contributes meaningfully to the growing demand for secure, concealed communication in today's digitally interconnected world.

6.2 Future Enhancements

For future enhancements, adding real-time steganographic chat would let users interact in real time and trade concealed messages inside multimedia, hence enhancing the platform. Cloud storage integration would allow encrypted items to be safely uploaded and downloaded. Although a mobile app could enable safe communication on the move, artificial intelligence-powered media optimization would boost embedding efficiency. Two-factor authentication and OTP-based logins help to further strengthen security.

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.

[11] https://www.geeksforgeeks.org/what-is-steganography/

[12] http://en.wikipedia.org/wiki/Transposition_cipher

[13] https://pypi.org/project/stegano/

[14] https://www.sciencedirect.com/science/article/pii/S1877050919313657

Glossary

1. Data Encryption: Using an algorithm and key, readable data (plaintext) is transformed into an unreadable format (ciphertext) to stop unwanted access.

2. Cryptographic Techniques: A collection of techniques for encrypting data and communications so that only those with permission can decipher them. comprises digital signatures, hashing, encryption, and decryption, among other things.

3. Steganographic Algorithms: Methods for obscuring the existence of secret information by enclosing it in non-secret data (such as pictures, sounds, or videos). Steganography, as opposed to cryptography, is more concerned with concealment than encryption.

4. Image-Based Security: A security method that entails enclosing or safeguarding data in digital photos, frequently using watermarking or steganography, in order to verify authenticity or ensure secure transmission.

5. Secure Decryption: Making sure that only authorized users with the right decryption key can access encrypted data (ciphertext) by transforming it back to its original form (plaintext).

6. Information Hiding: A general term for methods such as watermarking and steganography that entail hiding data inside other data to make it less visible or detectable by observers.

7. Steganography: Steganography is the process of enclosing confidential data in a non-secret medium (such as an audio, video, or image file) so that its existence is hidden. It is more concerned with hiding the message's existence than its content.

8. Cryptography: The science of protecting data by employing mathematical methods to change it from an unintelligible format (encryption) to a readable one (decryption). It guarantees data authenticity, confidentiality, and integrity.

9. Cipher Text: The jumbled, unintelligible result of an encryption algorithm is known as cipher text. It stands for plaintext that has been key-encrypted and rendered unintelligible without the right decryption.