INTERNATIONAL JOURNAL OF ELECTRONICS AND COMPUTER APPLICATIONS

ORIGINAL ARTICLE

Article access online

OPEN ACCESS

Received: 02.02.2025

Accepted: 25.06.2025

Published: 12.07.2025

Citation: Shejwal P, Salla R, Sanap S, Baride A, Patil P. (2025). LSB Steganography: A Key to Effectual Encryption and Decryption. International Journal of Electronics and Computer Applications. 2(1): 83-89. https://doi.org/10.70968/ijeaca.v2i1.D1003

* **Corresponding author**.

pallavi.shejwal@moderncoe.edu.in

Funding: None

Competing Interests: None

ISSN
Print: XXXX-XXXX
Electronic: 3048-8257

LSB Steganography: A Key to Effectual Encryption and Decryption

Pallavi Shejwal[1]*, Riddhi Salla[2], Shital Sanap[2], Arya Baride[2], Pratik Patil[2]

1 Assistant Professor, Department of Information Technology, Modern College of Engineering, Shivajinagar, Pune, Maharashtra, India
2 Student, B.E. Information Technology, Department of Information Technology, Modern College of Engineering, Shivajinagar, Pune, Maharashtra, India

Abstract

Steganography is an ancient process used in secrecy and has found new relevance in the modern digital era. In our day-to-day life, we rely on digital media for our personal and professional online communication, the need to protect sensitive information gains paramount importance[(1)]. The threats to hacking of sensitive data in the form of text, image and audio which may lead to heavy financial losses call for innovative and sophisticated methods to ensure encrypted end to end communication, protecting information from unauthorized access. In this regard, the challenge lies in encrypting and decrypting data securely when sending over communication media. Conventional encryption methods may not be full proof to handle new ways of data hacking techniques. Steganography has emerged as a suitable solution which enables the concealment of information which is in the form of image, text, audio and video. Conventional techniques may not fully address the challenges in a wide range of digital communication, necessitating the development of advanced methodologies. A lot of research work has been done in the domain of Security. The LSB Steganography technique has relevant features that collectively enhance its scope and applicability in a wide range of communication. This paper presents enhanced LSB steganography technique to encrypt and decrypt text, image and audio files successfully.

Keywords: Least Significant Bit; Steganography; Encryption; Decryption; Security

Introduction

In today's dynamic digital era, the exchange of sensitive information across online media or on websites has made data privacy and security more critical than ever. Traditional encryption and decryption techniques can still attract several serious challenges leading to potential attempts of cyber-attack which can lead to heavy financial losses. The idea of steganography was first introduced in the year 1983[(2)]. In Steganography, LSB (Least Significant Bit) steganography, offers an efficient alternative by hiding the very existence of a message within media like images, text, audio files making the hidden data virtually invisible

and difficult to hack.

The purpose of LSB Steganography is to provide a cutting-edge solution to the evolving problem faced in data security. By specifically leveraging the least significant bits (LSBs) of the red, green, and blue channels in an image, this technique hides messages or images without introducing significant changes. The primary objective of Steganography is to establish a virtual channel for transmitting information, thereby enhancing data security and privacy. The aim is to prepare a robust and versatile technique for secure communication which is capable of withstanding the challenges posed by current threats in data integrity.

The Least significant bit (LSB) Steganography boosts a rich array of features that collectively enhance its scope and applicability. Firstly, the system excels in message embedding, providing a seamless and concealed method for embedding messages within an image. This functionality ensures discreet communication, catering to scenarios where privacy and confidentiality are paramount.

Adding a layer of complexity to steganography, the system facilitates image embedding, allowing for the hiding of entire images within other images. This not only broadens the scope of concealed information but also introduces a heightened level of intricacy in the steganographic process. The system's versatility is further underscored by its seamless integration with various image formats, ensuring compatibility across different platforms. This adaptability enhances user convenience and promotes widespread usage across platforms.

Precision is a key focus of the system, particularly in its color channel manipulation. By meticulously manipulating the least significant bits of an image's red, green, and blue channels, the system achieves a level of precision that minimizes perceptible alterations to the visual content. The emphasis on user experience is evident.

Steganography scenario can be summarized in two different phases: encoding (embedding) phase with the help of secret key and decoding (extracting) secret data phase with the manner of preserving information in invisible form.

The paper is organized as follows:

Section 1 presents Introduction of Steganography technique. Section 2 describes the existing Methodologies used. Section 3 explains the proposed Methodology. Section 4 presents the Results and Discussion. Section 5 presents the Conclusion and future scope of research in LSB steganography. Section 6 lists the References.

Existing Methodology

Steganography has various useful applications. Secret Communications: secret information can be transmitted without being afraid of alerting danger from potential attackers[3]. Feature Tagging Elements: secret data can be embedded beyond an image, such as names of individuals tagged in a photo some locations in a map[4]. Copyright Protection: Aims to prevent data from being copied[4]. Different applications have different requirements of the steganography technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden[5]. In another research work, Video has been used as a spreading medium and then used it for concealment of an audio message and a document (in a pdf file) in a method that makes the information invisible using the least significant bit (LSB)[6]. For the purpose of secure communication, picture steganography, which comprises concealing secret messages in the cover image has been employed. Pixel value differencing (PVD) and least significant bit (LSB) replacement are the two most often used techniques for concealing information in photographs. The LSB approach works by swapping a bit of the secret message for each pixel in the cover image's least significant bit[7].

Proposed Methodology

The well-known approach that is utilized for steganography is the Least Significant Bit. This has become a prominent technique for present day steganography which utilizes Least significant bit (LSB) of picture's pixel data[8]. It inserts each piece of double content with one piece of every pixel in the original picture. This strategy works when the record is longer than the message document and if picture is grayscale, when applying LSB strategies to every bite of a 24 bit picture, three bits can be encoded into every pixel[9] Example: We can use images to hide things if we replace the last bit of every color's byte with a bit from the message.

Architecture diagram

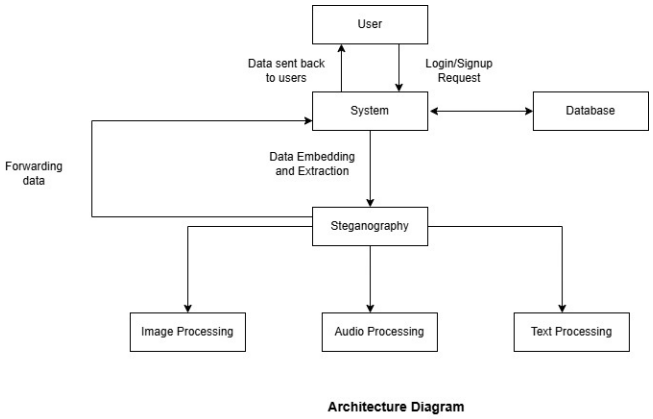

Fig 1. Proposed System Architecture

The architecture diagram illustrates the workflow of the LSB Steganography system. As shown in Figure 1, it shows the interaction between the user interface (React), the processing logic (Python modules), and the image input/output. It

highlights how secret data is embedded into and extracted from an image using the Least Significant Bit technique during encoding and decoding phases.

The architecture diagram illustrates the workflow of the LSB Steganography system. It shows the interaction between the user interface (React), the processing logic (Python modules), and the image input/output. It highlights how secret data is embedded into and extracted from an image using the Least Significant Bit technique during encoding and decoding phases.

Data Flow Diagram

The Level 0 DFD is the highest-level overview of a system. It shows the system as a single process node and illustrates how it interacts with external entities (like users or other systems). It doesn't show internal processes or data storage, just the basic input and output flows.

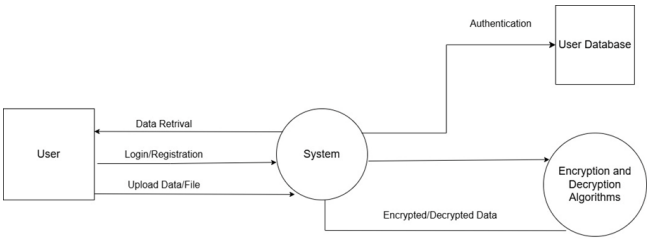

Fig 2. Data Flow Diagram (Level 0)

The Level 1 DFD as shown in Figure 3, expands the single process from the Level 0 DFD into several main subprocesses. It gives more insight into the major functions of the system but still stays at a high level.

The Level 2 DFD, as shown in Figure 4, goes into finer details of each Level 1 process, breaking them down into smaller subprocesses to show more specific tasks. Each process from Level 1 is broken down further until all steps are visible.

Class diagram

It provides a blueprint of the system by representing its classes, attributes, methods, and the relationships between classes. Class diagrams are essential for defining the structure of a system by detailing how classes interact and depend on each other.

Sequence Diagram

Shows the sequence of messages exchanged between objects to carry out a function. Useful for understanding the order of operations and interactions between system components.

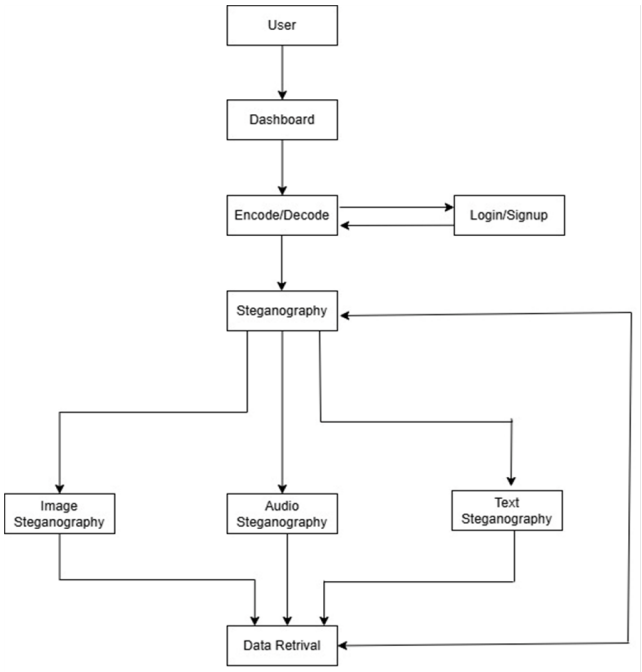

Fig 3. Data Flow Diagram (Level 1)

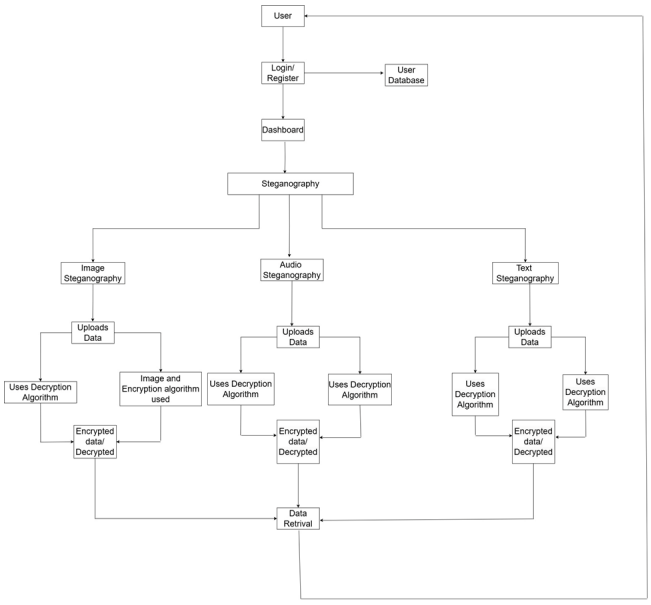

Fig 4. Data Flow Diagram (Level 2)

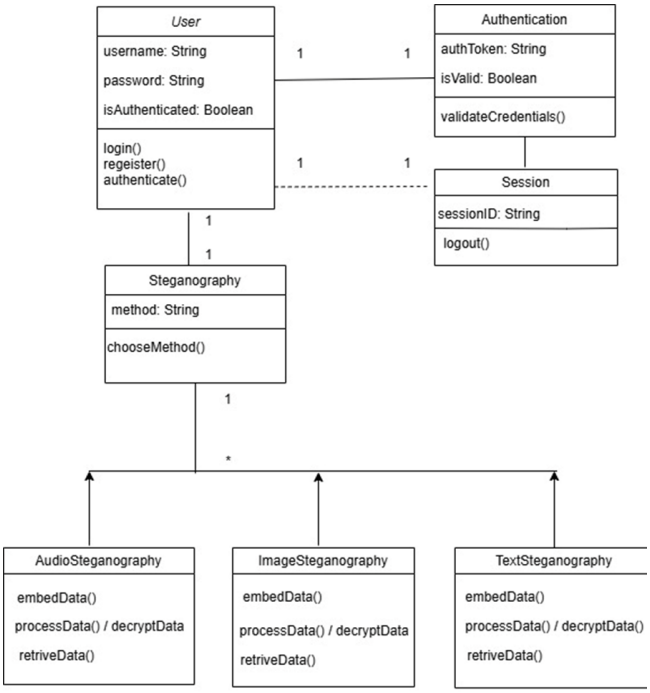

Fig 5. Class Diagram

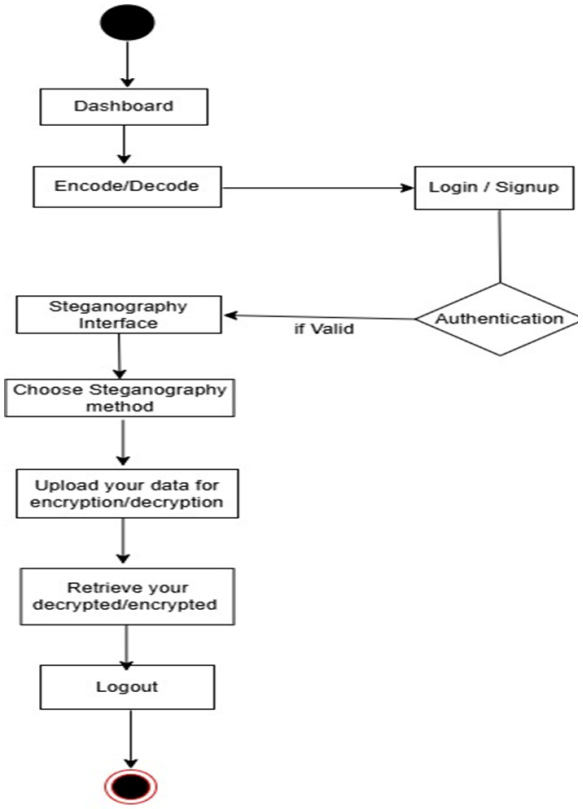

Fig 7. Activity Diagram

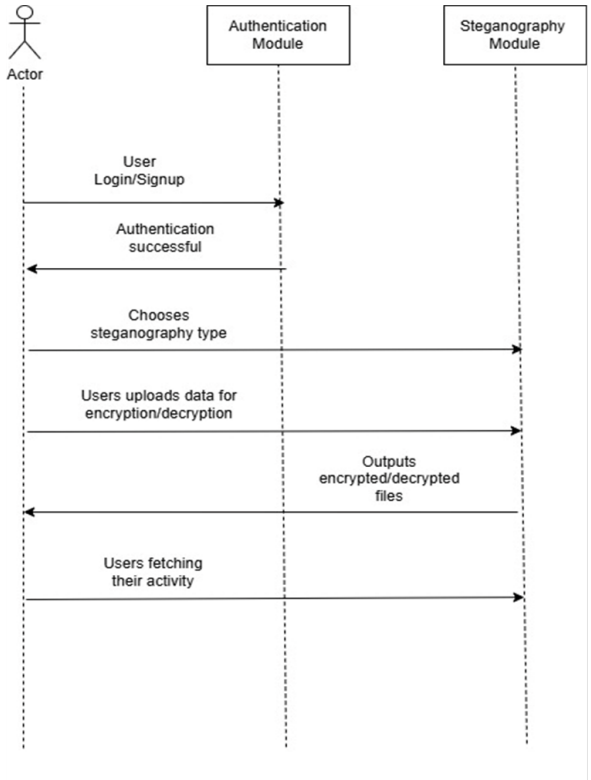

Fig 6. Sequence Diagram

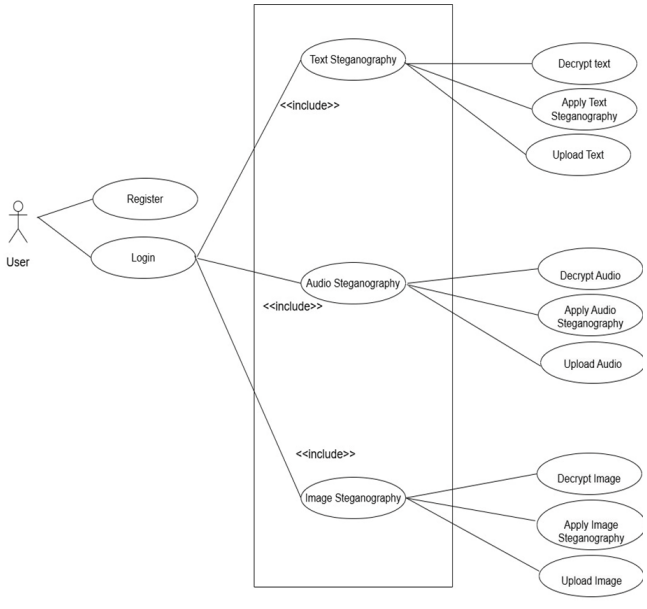

Fig 8. Use case Diagram

Overview of Modules

The Project modules are:

-User Interface design

-Encryption of Image, text and audio

-Decryption of Image, text and audio

-MongoDB: Database used for storage purposes

The LSB Image Steganography represents a comprehensive and versatile solution for secure and covert communication within the digital realm. Through the adept manipulation of least significant bits (LSBs) in image color channels, the system excels in embedding messages and images discreetly, fostering enhanced data security and privacy. The system's strengths lie in its user-friendly operation, dynamic application scenarios and precision in concealing information. The system currently confines audio steganography to the .wav format. In essence, the LSB Image Steganography project, with its current capabilities and future growth potential, stands as a robust tool for concealed communication, addressing the evolving challenges in data security within the digital landscape[10].

Technologies used for Frontend: ReactJS: A JavaScript library for building interfaces.

Backend: Python: A high-level, interpreted programming language.

Database: MongoDB: Database used for storage purposes Flask for integration of React and MongoDB.

GUI/WORKING MODULES

Fig 9. Homepage

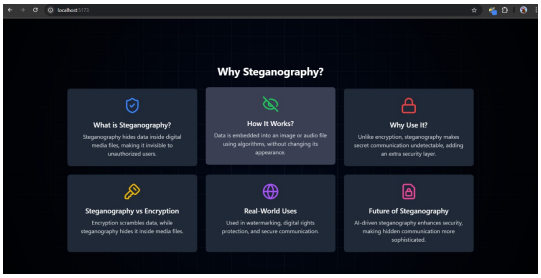

Fig 10. About Steganography

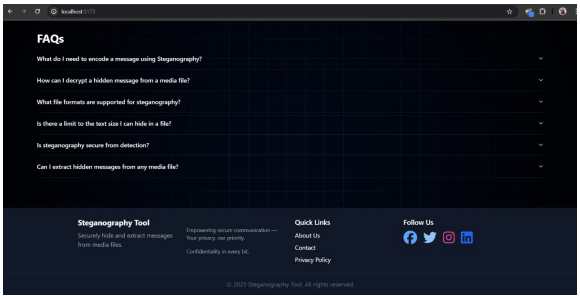

Fig 11. Frequently asked questions on Steganography

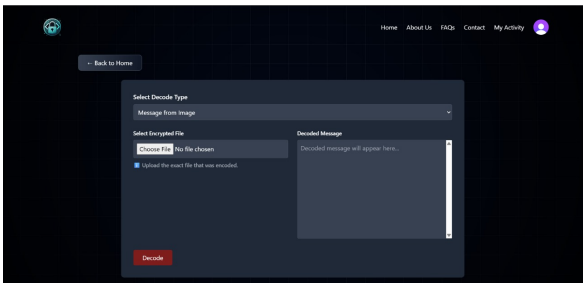

Fig 12. Select decode type in Steganography

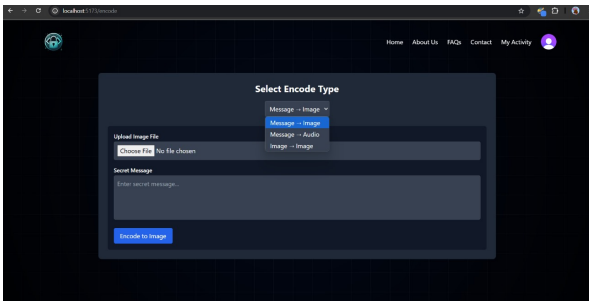

Fig 13. Select encode type in Steganography

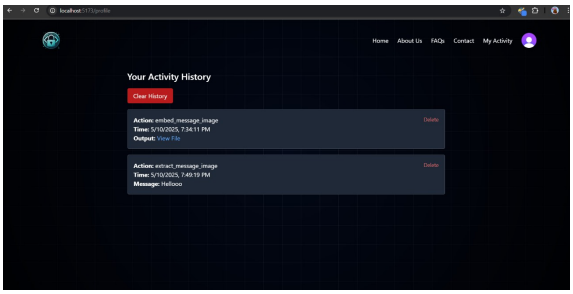

Fig 14. Show activity history

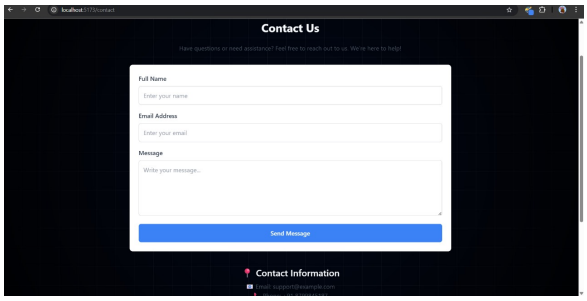

Fig 15. Contact us page

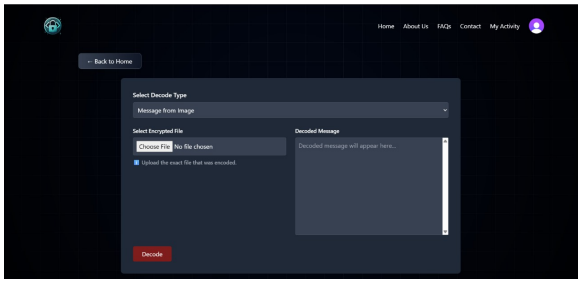

Fig 16. Select Decode type

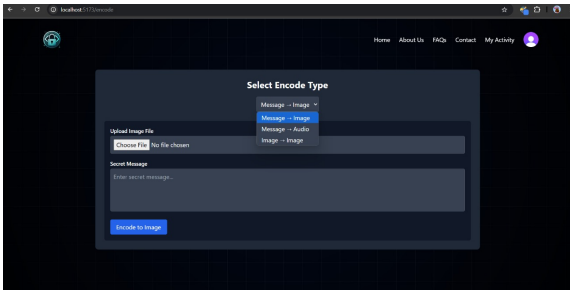

Fig 17. Select Encode type for Message to Image

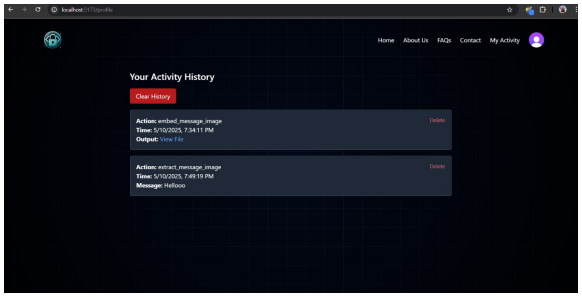

Fig 18. Show activity history

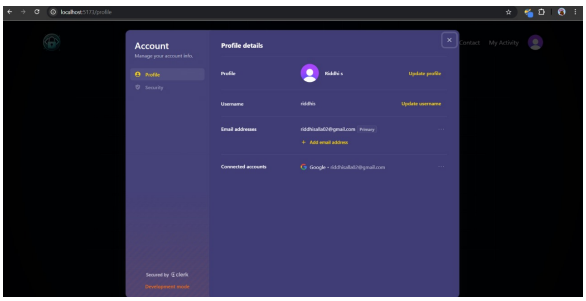

Fig 19. Profile details of user

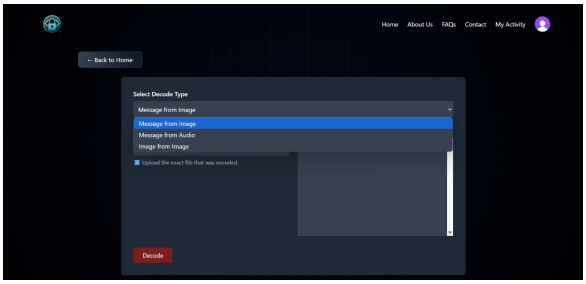

Fig 20. Select decode type

Results and Discussion

The steganography project successfully achieved its objectives by implementing and testing various encoding and decoding methods. Messages were successfully hidden within image and audio files using the developed encoding module. The decoding module was able to accurately extract these messages. Tests showed that the hidden messages retained their integrity after being encoded in different types of media files. The security module allowed for password protection on encoded messages, ensuring that only authorized users could decode sensitive information. The project maintained the original quality of the media files after encoding, with only minimal, imperceptible changes detectable by visual or auditory inspection. Overall, the project demonstrated a robust steganography tool that maintains data security and quality, meeting the objectives and requirements outlined at the beginning.

Conclusion and Future scope

In conclusion, the LSB Image Steganography project represents a comprehensive and versatile solution for secure and covert communication within the digital realm. Through the adept manipulation of least significant bits (LSBs) in image color channels, the system excels in embedding messages and images discreetly, fostering enhanced data security and privacy. The system's strengths lie in its user-friendly operation, dynamic application scenarios, and precision in concealing information. However, as with any technological endeavor,

certain limitations exist. The system can be extended to implement video steganography.

In future the system can be enhanced by adding more system security and efficiency by incorporating advanced algorithms. These additions aim to not only fortify the security measures but also optimize the overall performance of the steganographic processes. The utilization of advanced algorithms ensures that the website remains at the forefront of technological advancements in the field.

References

1) Provos N, Honeyman P. Detecting Steganographic Content on the Internet. 2002. Available from: https://www.researchgate.net/publication/2379632_Detecting_Steganographic_Content_on_the_Internet.
2) Krishnan RB, Yuvaraj D, Devi PS, Chooral VS, Kumar NR, Karthikeyan B, et al. An Improved Steganographic Scheme Using the Contour Principle to Ensure the Privacy of Medical Data on Digital Images. *Computer Systems Science and Engineering* . 2023;46(2):1563–1576. Available from: https://doi.org/10.32604/csse.2023.035307.
3) Zhang L, Wu J, Zhou N. Image Encryption with Discrete Fractional Cosine Transform and Chaos. In: and others, editor. 2009 Fifth International Conference on Information Assurance and Security. IEEE. 2009;p. 61–64. Available from: https://doi.org/10.1109/IAS.2009.89.
4) Ajit P, Chouhan K. A Study and literature Review on Image Steganography. *International Journal of Computer Science and Information Technologies (IJCSIT)*. 2015;6(1):685–688. Available from: https://www.ijcsit.com/docs/Volume%206/vol6issue01/ijcsit20150601152.pdf.
5) Kutade PB, Bhalotra PSA. A Survey on Various Approaches of Image Steganography. *International Journal of Computer Applications*. 2015;109(3):1–5. Available from: https://dx.doi.org/10.5120/19165-0620.
6) Ali HA, Jalil AJ, Hussein MK. Least significant bit technology for hiding text data using video steganography. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*. 2023;22(1):157–163. Available from: https://dx.doi.org/10.12928/telkomnika.v22i1.24029.
7) Akshitha S, Desai SA, Aishwarya MS, Sahana SU, Sridhar R. The Image Steganography Using LSB And PVD Algorithms. *International Journal of Research and Analytical Reviews*. 2023;10(2):237–249. Available from: https://www.ijrar.org/papers/IJRAR23B2960.pdf.
8) Potdar VM, Chang E. Grey level modification steganography for secret communication. In: 2nd IEEE International Conference on Industrial Informatics, 2004. INDIN '04. 2004. IEEE. 2005;p. 223–228. Available from: https://doi.org/10.1109/INDIN.2004.1417333.
9) Provos N, Honeyman P. Hide and seek: an introduction to steganography. *IEEE Security & Privacy*. 2003;1(3):32–44. Available from: https://dx.doi.org/10.1109/msecp.2003.1203220.
10) Amarendra K, Mandhala VN, Gupta BC, Sudheshna GG, and VVA. Image Steganography Using LSB. *International Journal of Scientific and Technology Research*. 2019;8(12):906–909. Available from: https://www.ijstr.org/final-print/dec2019/-Image-Steganography-Using-Lsb.pdf.