**Text-Image-Audio Steganography**

The project submitted to the

SRM University – AP, Andhra Pradesh

for the partial fulfillment of the requirements to award the course

**IDP100**

Offered by the

**Computer Science and Engineering**

**School of Engineering and Sciences**

Submitted by

**Mohith Sashank Namburu**

**A picture containing text

Description automatically generated**

Under the Guidance of

**Dr. Kakumani K C Deepthi**

**Assistant Professor**

**Department of CSE**

**SRM University–AP**

**Neerukonda, Mangalagiri, Guntur**

**Andhra Pradesh – 522 240**

**November, 2023**

# Certificate

Date: 20-Jan-24

This is to certify that the work present in this Project entitled “**Text-Image-Audio Steganography**” has been carried out by **Mohith Sashank Namburu** under my supervision. The work is genuine, original, and suitable for submission to the SRM University – AP for the award of Bachelor of Technology in the **School of Engineering and Sciences**.

**Supervisor**

(Signature)

Dr. Kakumani K C Deepthi

Assistant Professor,

Department of Computer Science Engineering.

SRM University AP.

# Acknowledgments

# In making this project, and completing it successfully, I had to get help and guidance from my instructor. I am grateful that I was given the opportunity to make this project, which has enhanced my knowledge in so many aspects.

# I would like to show my gratitude to my course instructor, Dr. Kakumani K C Deepthi for giving me great guidance for this project. I wish to extend my special thanks to my teammates who have always been supportive and guided me throughout this project.

# Table of Contents

[Certificate](#_Toc105799088) II

[Acknowledgment](#_Toc105799089) III

[Table of Contents……………………………………………………………..IV](#_Toc105799090)

[List of Figures V](#_Toc105799092)

[Abstract VI](#_Toc105799091)

[1. Introduction](#_Toc105799099) 1

[1.1 MSB and LSB 1](#_Toc105799100)

[2. Background 2](#_Toc105799102)

[3. Proposed Approach 3](#_Toc105799106)

[3.1 Algorithm 3](#_Toc105799104)

[3.2 System Design 4](#_Toc105799104)

[4. Results and Discussion 5](#_Toc105799107)

[5. Conclusion 9](#_Toc105799108)

[References 10](#_Toc105799109)

# List of Figures

Figure 1 : MSB……………………………………………………………..……………1

Figure 2 : LSB………………………………………………………………..………….1

Figure 3 : Original and Steganography image…..……………………………….…..2

Figure 4 : Basic Flowchart of steganography………...………………………………3

Figure 5 : Flowchart of Text, Audio and Video Steganography……………………4

Figure 6 : Web Page of Steganography………………………………………………5

Figure 7 : Working of encode section…………………..…………………………….6

Figure 8 : Secret Message encoded file……………………………………….……...6

Figure 9: Working of decode section…………………………………..….………....7

Figure 10: Audio Steganography…..…………………………………..….………....8

Figure 11: Text Steganography……..…………………………………..….………....8

# Abstract

Steganography refers to the concealment of confidential data within a common medium, like a text, image, or audio file, without altering its original appearance, in order to evade detection. This method is used for several purposes, including protecting data privacy, preventing unauthorized access to data, and ensuring safe information transmission over insecure networks. While steganography can be used for legitimate purposes such as by military, law enforcement, and journalism, it can also be employed for malicious activities like cybercrime and terrorism. The least significant bit (LSB) of each letter in text & audio and the LSB of each pixel in images are altered in steganography to make the alterations invisible. Advanced steganography algorithms like Masking & Filtering and Encrypt & Scatter have improved security against steganalysis assaults while producing higher-quality stego images. The method’s capability for concealing text with an unlimited hidden text size in text, audio, and images will be employed in the outcome.

# 1. Introduction

Steganography is a technique used by military personnel to securely communicate without leaving any trace of their activity. This method of communication involves hiding data within other data, such as text, images, or audio. This allows the user to send a message without anyone knowing the true content of the message. By using this method, military personnel can securely transmit sensitive information without the risk of it being intercepted or compromised. Steganography can also be used to verify the authenticity of a message, as it is much more difficult to forge a message that has been encoded using steganography. Overall, this technique allows military personnel to securely and covertly communicate with one another, ensuring that their information remains confidential.

**1.1 MSB and LSB:**

In computing, the most significant bit (MSB) is the bit with the highest value in a binary number. It is usually the leftmost bit, or the first bit transmitted in a sequence. For example, in the binary number 1000, the MSB is 1. The MSB has the greatest effect on the number. For example, in the binary number 0011 0101, the most significant 4 bits are 0011.

To find the MSB, you can:

Divide the number by 2 in multiple steps until the number reaches zero

Use the formula MSB = floor(log2n)

Count the number of leading zeroes in a fixed integer (32 bits) using a built-in function

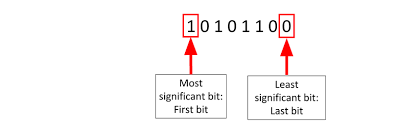
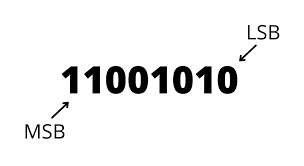
The least significant bit (LSB) is the lowest bit in a series of binary numbers. It is located at the far right of a string. For example, in the binary number 10111001, the LSB is the far right 1. Binary number 0011 0101: The most significant 4 bits are 0011, and the least significant 4 bits are 0101.

To find the LSB, you can:

The value at the least significant bit position = x & 1.

The value of the isolated least significant 1 = x & -x.

The zero-based index of the isolated least significant 1 = log2(x & -x)



**Figures 1&2: MSB and LSB**

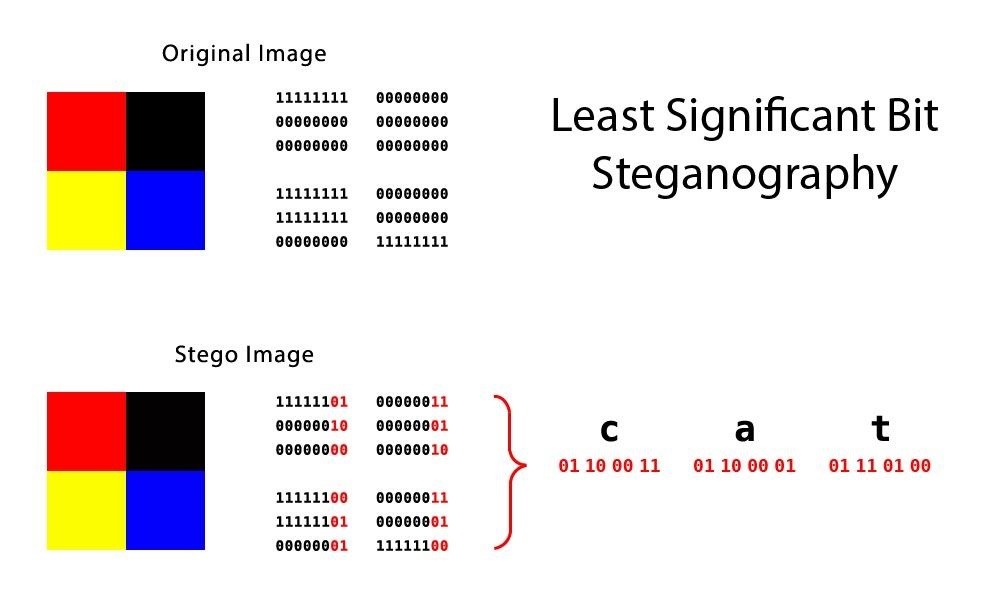
# 2. Background

The military uses steganography in a variety of ways, including covert communication, secure data storage, and hiding classified information. For example, a soldier may use steganography to securely communicate a message to another soldier by hiding it in a seemingly innocent image or audio file. Similarly, classified data can be hidden within an image or audio file, making it difficult to detect without the proper tools.

Overall, steganography is a powerful and important tool for the military, allowing it to securely communicate and store sensitive and classified information.

**Other possibilities:**

Other possibilities or future improvements include encrypting the text using more secure encryption algorithms such as AES or RSA and then hiding the encrypted text in an image. Then the image can be encrypted and sent to the receiver.

****

**Figure 3: Original & Steganography image**

# 3. Proposed Approach

## Algorithm:

The algorithm for Image LSB (Least Significant Bit) Steganography involves embedding information by manipulating the least significant bit of each pixel in an image. Below is a simple algorithm outlining the steps for hiding and extracting data using LSB Steganography

Hiding Data (Encoding):

1. Input: Original Image, Data to Hide

2. Convert Data to Binary:

•Convert the data (e.g., characters or bytes) into binary format.

3. Embed Data into Image:

•For each pixel in the image:

•Retrieve the RGB values of the pixel.

•Modify the (LSB) of each RGB channel to match the bit of the binary data.

4. Output: Modified Image

Extracting Data (Decoding):

1. Input: Modified Image

2. Initialize Empty Binary Data String:

•Create an empty binary string to store the extracted binary data.

3. Extract Data from Image:

• For each pixel in the modified image:

•Retrieve the LSB of each RGB channel.

•Append the LSB values to the binary data string.

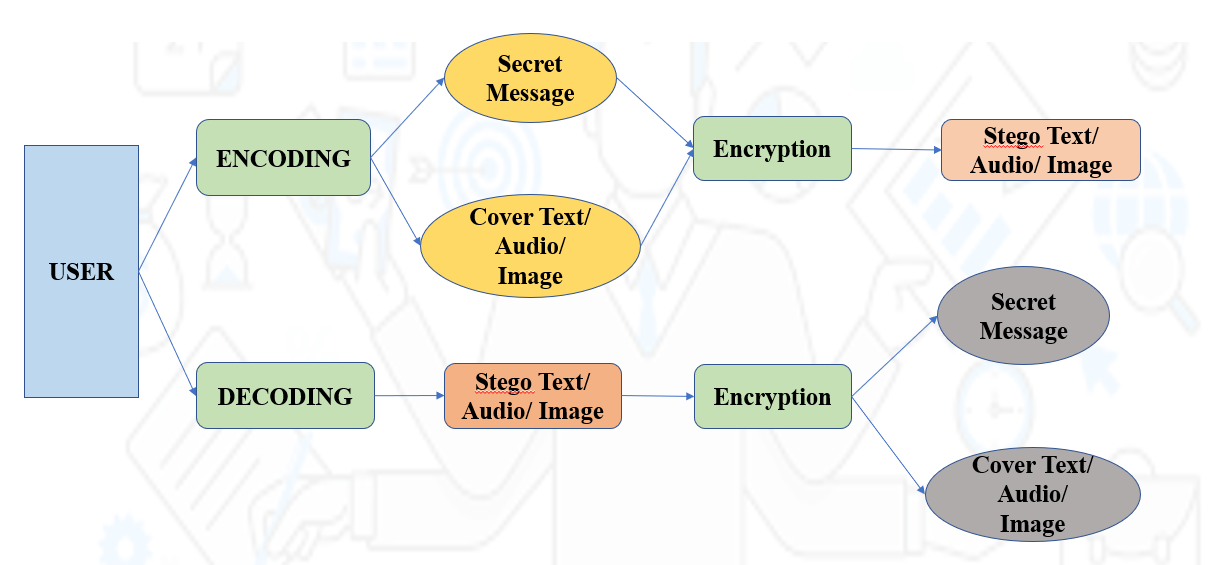
4. Convert Binary Data to Original Format:

•Convert the binary data string back to the original format (e.g., characters or bytes).

5. Output: Extracted Data

## 

## Figure 4: Basic flowchart of Steganography



## Figure 5: Detailed flowchart of Text, Image and Audio Steganography

## System Design:

Image Steganography is a technique used to hide secret information in an image. The system design of Image Steganography consists of the following steps:

1. Data Embedding: This process involves selecting the secret data to be embedded, choosing an appropriate algorithm, and encoding it into a suitable format such as ASCII or binary.

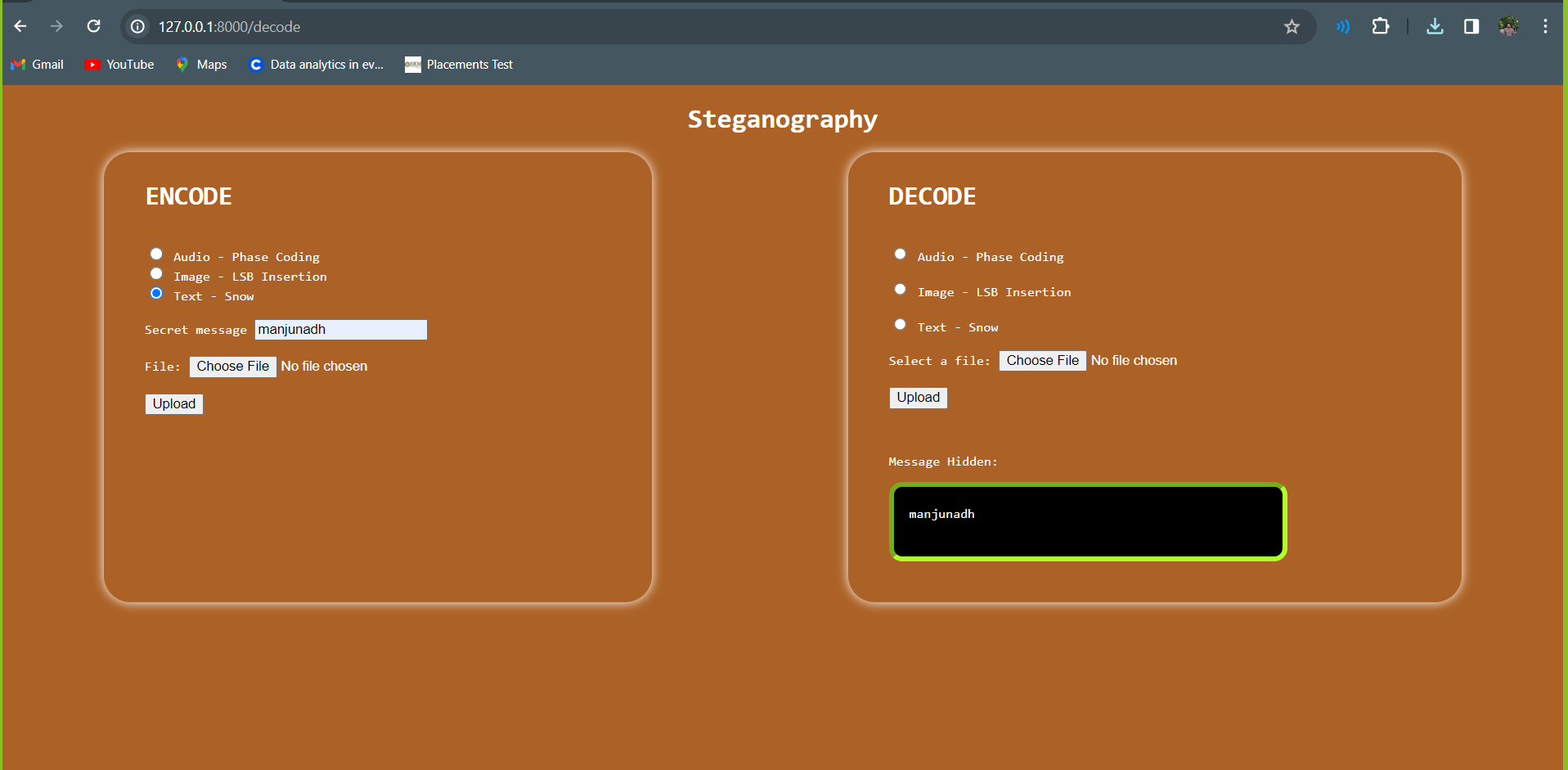
2. Steganography: This is the process of hiding the secret data inside the image. It can be done by replacing some of the least significant bits in the image with the secret data.

3. Data Extraction: This is the process of extracting the secret data from the image. It is done by reading the least significant bits of the image and decoding the secret data.

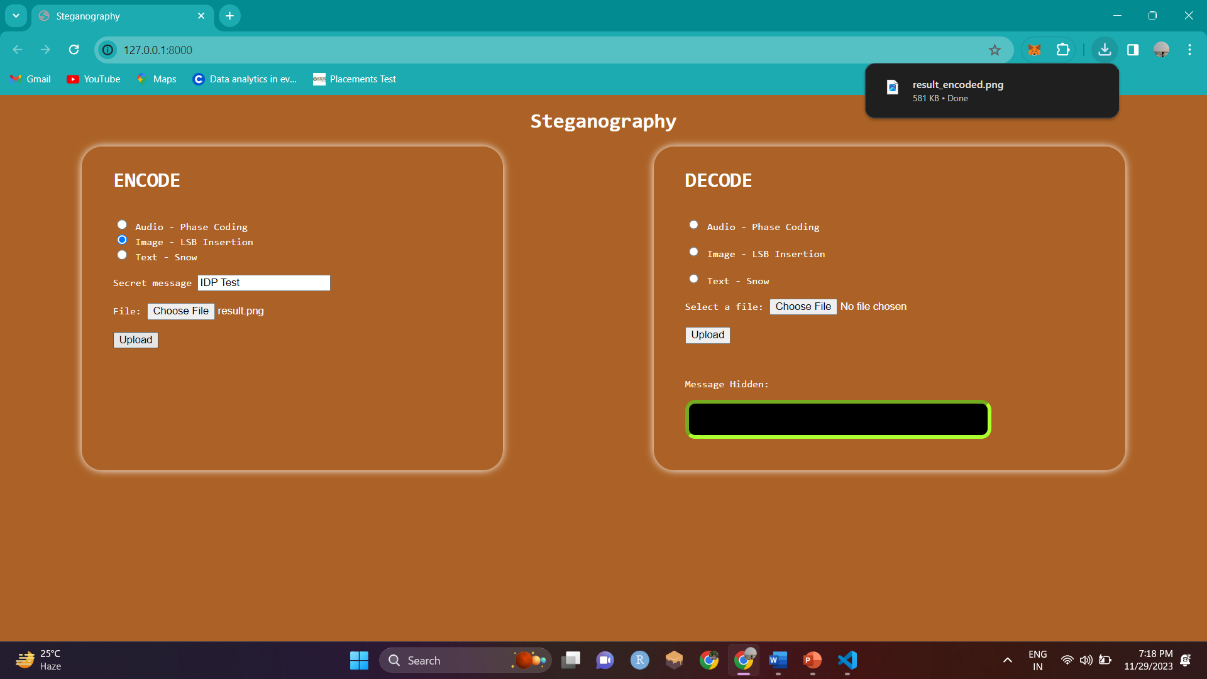
# 4. Results & Discussion:

* The expected outcome of embedding secret messages in realistic texts, audio, and images is that the messages will be well hidden and difficult to detect by unauthorized parties while being easily retrievable by the intended recipient.
* The capacity of advanced algorithms to embed large amounts of data in the text, audio, or image while maintaining the file’s quality can also allow for more information to be transmitted within a single text document, audio, and image file.
* In total, Steganography provides a secure and reliable way to transmit sensitive information while maintaining the message passed.
* As we can see the output of the project the image, text, or audio we are given is encrypted with the secret message and when we try to decode it we upload the secret message encoded file that is in our downloads and after uploading we can see the hidden message that was encrypted before.

**Sample inputs & outputs:**

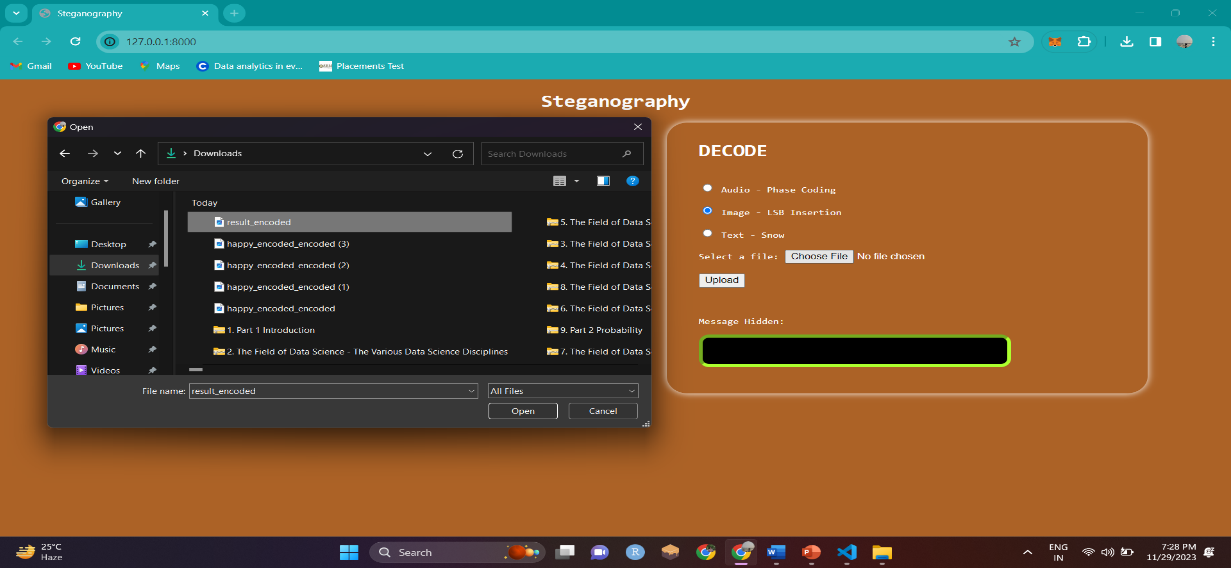
****

**Figure 6: Web Page of Steganography**



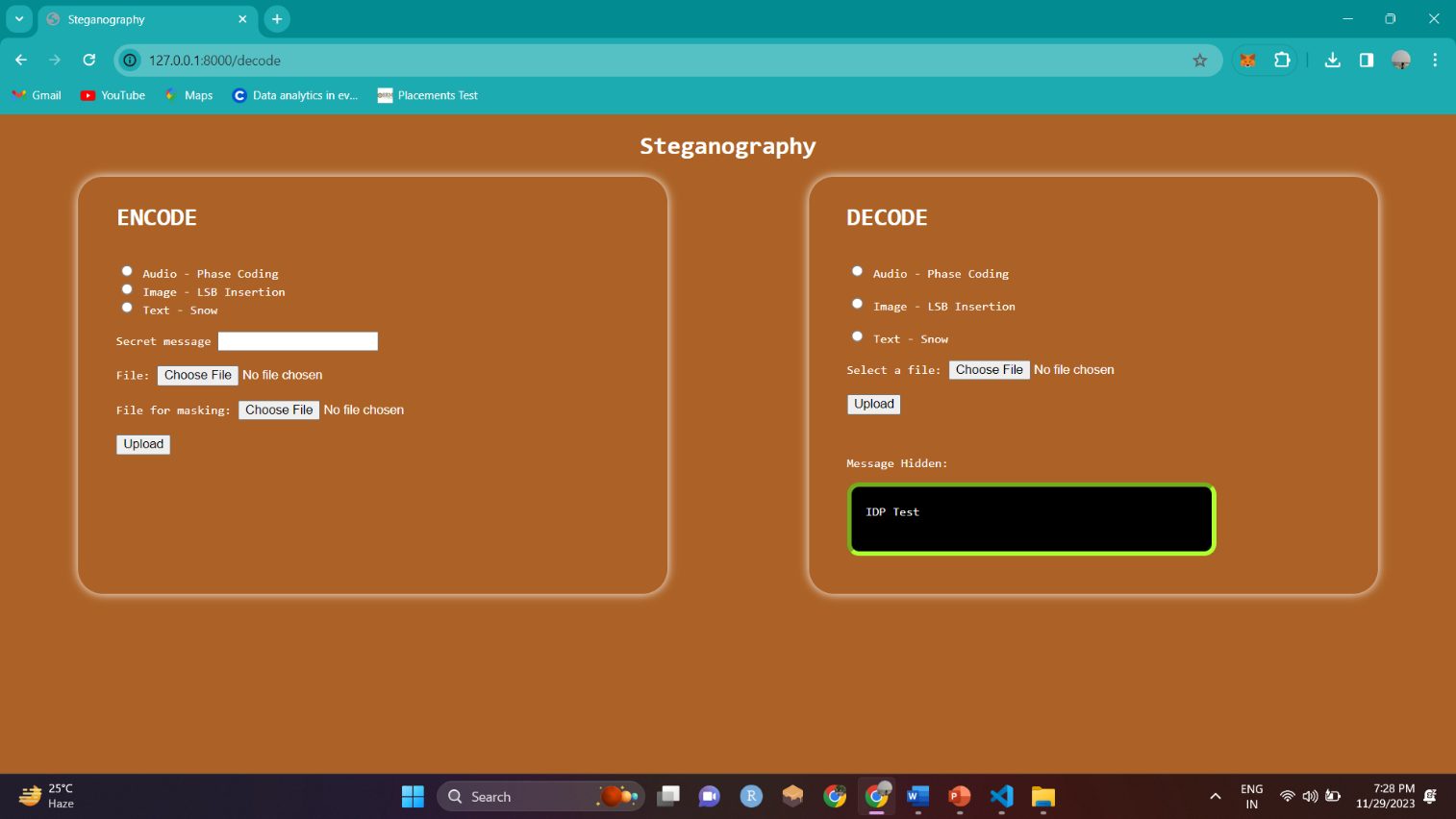
**Figure 7: Working of encode section**

* The web Page of our project contains two sections which are encode and decode where the user can select whether to use which of the three formats the user wants to hide the message.
* After choosing the format the user needs to enter the message and upload the file with respect to the format the user has given and when the user uploads it, the user will get a downloadable file where the secret message is hidden and there will be no difference between the original and secret message encoded file.
* As we can see in the above picture we can see the secret message encoded image file is downloaded.



**Figure 8: Secret message encoded file**

* The above picture shows us the secret message encoded image file and user needs to upload it to decode to see the hidden message in that image file.
* This way when any organization, individual, military or any kind of body when they want to hide a message they can use our platform to hide it and send it to the destination body without any data breach so that the plan of immediate action can be designed by the desired decoder.



**Figure 9: Working of the Decode Section**

* After finishing the encoding part of our project the end user needs to upload the secret message encoded file which was sent by the encoder and the decoder needs to upload that file and choose the file format which was sent by the encoder and upload it.
* The second when the decoder uploads the file decoder can see the secret message that was hidden by the encoder, The above image we can see the secret message “IDP Test” which was given by the encoder with the original image file.

**Working of the Audio Steganography :**

****

**Figure 10: Audio Steganography**

**Working of the Text File Steganography :**

****

**Figure 11: Text File Steganography**

# 5. Conclusion :

In conclusion, steganography is a powerful tool for secure communication and data hiding. It allows for secure data exchange and storage by hiding data in plain sight. It has many applications in both commercial and military contexts and can be used in a wide variety of ways. Steganography is an important component of any information security strategy, as it allows for secure communication and data storage that is undetectable by conventional methods of detection. As technology continues to evolve, the uses of steganography are sure to expand

1. Capacity: Steganography has limited capacity for hiding data due to the fact that it can only hide limited amounts of data in a given medium.

2. Detectability: Steganography is not completely secure as there are various ways to detect hidden messages. 3. File size: Steganography usually increases the size of the file, thus making it more obvious that something is hidden in the medium.

4. Complexity: It can be quite complex to hide data in a medium, and it requires specific software or tools to successfully complete the task.

5. Cost: Steganography requires additional hardware or software, which may add additional costs.

**References:**

[1] Samruddhi Deshmukh, Mitalee Manware, Radhika Chhablani, Shweta Meshram (A Review Paper on Text steganography - July 2022 International Journal of Research in Engineering and Science)

[2] Muhammad Adnan Aslam, Muhammad Rashid, Farooque Azam, Muhammad Abbas, Yawar Rasheed, Saud S. Alotaibi, Muhammad Waseem Anwar (Image Steganography using Least Significant Bit (LSB) - A Systematic Literature Review - January 2022 2nd International Conference on Computing and Information Technology)

[3] Amitava Podder, Piyal Roy, Smaranika Roy (Steganography Techniques - An Overview - November 2022 International Journal of Scientific Research in Computer Science Engineering and Information Technology)

[4] Vivek Sharma S, Monika Raj, Swathi S (A Survey of Text Steganography Methods - May 2021 International Journal of Scientific Research in Science and Technology)

[5] Rini Indrayani (Modified LSB on Audio Steganography using WAV Format - January 2021 3rd International Conference on Information and Communications Technology)