A PROJECT REPORT ON

“IMAGE & AUDIO STEGANOGRAPHY”

Submitted by

Aakanksha Wadje (2021BCS049)

Gurudas Chavan (2021BCS037)

Pravin Narwade (2021BCS047)

Rahul Chafle (2021BCS061)

T.Y. B. Tech

UNDER THE GUIDANCE OF

Mrs. P. G. Kolapwar

Ms. Gauri Bhelonde

Ms. Pooja Kokare

Shri Guru Gobind Singhji Institute of Engineering & Technology
Nanded - 431606, India.
(An Autonomous Institute of Govt. of Maharashtra)

Year 2023-2024

Semester-V

CERTIFICATE

This is to certify that, the Project report entitled

“IMAGE & AUDIO STEGANOGRAPHY”

Submitted by

Aakanksha Wadje (2021BCS049)

Gurudas Chavan (2021BCS037)

Pravin Narwade (2021BCS047)

Rahul Chafle (2021BCS061)

As the partial fulfillment of the Technical Seminar
For the academic year 2023-2024

This project is a record of student’s own work, carried out by them under our supervision and guidance.

Mrs. P. G. Kolapwar **Ms. Gauri Bhelonde** **Ms. Pooja Kokare**

Acknowledgement

For all the efforts behind the project work, we first & foremost would like to express our sincere appreciation to respected **Mrs. P. G. Kolapwar, Ms. Gauri Bhelonde** and **Ms. Pooja Kokare**, for their extended help & suggestions at every stage of this project.

It is with a great sense of gratitude that we acknowledge the support, time to time suggestions are highly indebted to our guide.

Finally, we pay our sincere thanks to all those who indirectly and directly helped us towards the successful completion of this project report.

Abstract

Steganography is the art of hiding information and an effort to conceal the existence of the embedded information. It serves as a better way of securing message than cryptography which only conceals the content of the message not the existence of the message. Original message is being hidden within a carrier such that the changes so occurred in the carrier are not observable.

In this project we will discuss how digital images can be used as a carrier to hide messages. This paper also analyses the performance of some of the steganography tools. Steganography is a useful tool that allows covert transmission of information over an over the communications channel. Combining secret image with the carrier image gives the hidden image. The hidden image is difficult to detect without retrieval.

This project will take an in-depth look at this technology by introducing the reader to various concepts of Steganography, a brief history of Steganography and a look at some of the Steganographic technique.

KEYWORDS
Steganography, Steganalysis, Digital watermarking, Stego key, Stego image and Cryptography.

INDEX

Chapter 1 : Introduction

Steganography is a Greek word which means concealed writing. The word ‘steganos’ means covered and ‘graphical’ means writing. Thus, steganography is not only the art of hiding data but also hiding the fact of transmission of secret data. Steganography hides the secret data in another file in such a way that only the recipient knows the existence of message.

1.1 Objectives

- **Concealing Information :**

The primary objective of image steganography is to conceal sensitive or confidential information within digital images. This involves embedding data in such a way that the alterations are imperceptible to human observers, ensuring covert communication.

- **Maintaining Image Quality :**

Striking a balance between the hiding capacity and the visual quality of the cover image is a key objective. Steganographic methods aim to embed information without causing noticeable degradation in the appearance of the image, preserving its authenticity and natural appearance.

- **Security in Communication :**

Facilitating secure communication is a key objective. Image steganography aims to provide a layer of security for transmitted data, preventing unauthorized access and eavesdropping. This is particularly relevant in scenarios where traditional encryption methods might draw attention.

- **Real-world Applicability :**

Ensuring that steganographic methods are practical and applicable in real-world scenarios, including communication systems, digital forensics, and secure data storage, is a key objective. This involves addressing the diverse requirements of different applications.

1.2 Problem Statement

In the ever-expanding landscape of digital communication and data transmission, the confidentiality and security of information have become paramount. Traditional encryption methods play a crucial role in protecting data, but their use may draw attention to the very existence of sensitive content. In response to this challenge, image steganography emerges as an alternative strategy, allowing users to embed covert information within seemingly innocuous images.

1.1 Study of Project

The core idea behind image steganography is to embed secret data within the pixels of a host image in such a way that the alteration is imperceptible to the human eye. The cover image, as it is known, appears unchanged to casual observers, making it a covert vessel for the hidden information. This ability to conceal data within innocuous-looking images makes image steganography a valuable tool in scenarios where overt encryption might attract unwanted attention.

The process of image steganography involves selecting an appropriate cover image and embedding the secret information using various algorithms and techniques. The choice of algorithm depends on factors such as hiding capacity, visual quality, and resilience against detection. Popular methods include Least Significant Bit (LSB) substitution, frequency domain techniques like Discrete Cosine Transform (DCT), and spatial domain approaches that modify pixel values based on predefined patterns.

While image steganography offers a powerful means of securing sensitive data, it is not without challenges. Advances in both steganographic techniques and steganalysis methods have led to a perpetual cat-and-mouse game between those seeking to secure information and those attempting to uncover concealed messages.

This introduction sets the stage for exploring the intricacies of image steganography, delving into the methodologies, challenges, and advancements within this fascinating feld. As technology evolves, the importance of image steganography as a tool for secure communication and information protection becomes increasingly apparent, prompting ongoing research and innovation in this dynamic domain.

Chapter 2 : Literature Survey

A Survey of Steganography Techniques (2008) by Akansha Bansal and S.K. Muttoo :

This comprehensive survey provides an overview of different steganographic techniques, including image steganography. It covers classical methods and explores advancements in spatial domain techniques, transform domain techniques, and hybrid methods.

Digital Image Steganography: Survey and Analysis of Current Methods (2010) by R. Sridevi and Dr. M. Punithavalli :

The authors review contemporary steganographic methods, emphasizing digital image steganography. The survey discusses techniques such as LSB substitution, frequency domain methods, and their applications in secure communication.

A Survey of Steganography and Steganalysis Techniques in Image, Text, Audio and Video (2010) by Alireza Mansouri, Mohammad Reza Keyvanpour, and Sattar Hashemi :

This survey explores steganography and steganalysis across various media types, with a specific focus on image steganography. It discusses challenges, trends, and emerging technologies in the field.

Image Steganography Techniques: An Overview (2011) by Jyoti Yadav and R. C. Jain :

The survey provides an overview of image steganography techniques, categorizing them into spatial domain, transform domain, and compression domain methods. It discusses the advantages, limitations, and comparative analysis of different techniques.

A Survey on Image Steganography Techniques and its Applications (2012) by R. S. Bhuvaneswari, S. Anusuya, and S. Jothi :

Focusing on the applications of image steganography, this survey discusses various techniques, their strengths, and weaknesses. It also explores potential future directions in the feld.

Recent Advances in Image Steganography: A Review (2013) by A. G. Ananth and Dr. S. N. Sivanandam :

The survey covers recent advancements in image steganography, including the integration of encryption and compression techniques. It provides insights into the evolving landscape of steganography.

Chapter 3 : System Development

3.1 Project Plan

This project requires good knowledge of python and the Tkinter library. Tkinter is the python binding to the Tk toolkit which is used across many programming languages for building the Graphical user interface which is a GUI.

Also, we require a PIL module. This is the images module from the pillow. The PIL module helps to open, manipulate and save many different forms of images.

Below are steps to implement Python Image Steganography Project:

1. Import Modules.
2. Create a Function to make a main frame
3. Function to go back to the main frame
4. Function to Encoding and Decoding frame.
5. Create function for encoding image
6. Create function for decoding image
7. Function to decoding and generation of data
8. Function to modify the pixels of image
9. Function to enter the data pixels in image
10. Function to enter hidden text
11. GUI loop

3.2 Modules

3.2.1 Tkinter Module

- Tkintker is a standard GUI (Graphical User Interface) toolkit in Python. It provides a set of tools and widgets to create graphical user interfaces for desktop applications.

- Tkintker is included with most Python installations, making it easily accessible for developers. It is based on the Tk GUI toolkit.

- Tkintker provides various other widgets and options for organizing them. It also supports event handling, allowing you to respond to user actions like button clicks or key presses.

3.2.2 Pillow (PIL) Module

- Pillow is a comprehensive image processing library that supports opening, manipulating, and saving images in various formats. It provides functionalities such as resizing, cropping, rotating, filtering, drawing, and more.

- Pillow supports a wide range of image formats, including JPEG, PNG, GIF, BMP, TIFF, and others. It can handle both basic and advanced image processing tasks.

- The library is used for various tasks, such as working with images in web applications, performing image transformations in computer vision projects, and general image processing tasks.

- Pillow is extensible, allowing developers to create custom filters, effects, and operations on images.

- Pillow is compatible with both Python 2 and Python 3, making it versatile for various projects.

3.2.3 IO Module

- The io.open() function is a replacement for the built-in open() function. It returns a file-like object that can be used for reading or writing. This function is especially useful when working with different encodings.

- The io.StringIO class provides an in-memory stream for text data, while the io.BytesIO class is used for binary data. They allow you to read from or write to strings or bytes as if they were files.

- These classes provide buffering for input and output operations, improving performance by reducing the number of system calls.

- Since StringIO and BytesIO objects behave like file objects, they can be used in functions that expect file-like input.

- These classes provide additional functionality for buffered random access and text-mode I/O, respectively.

3.2.4 Software Requirements

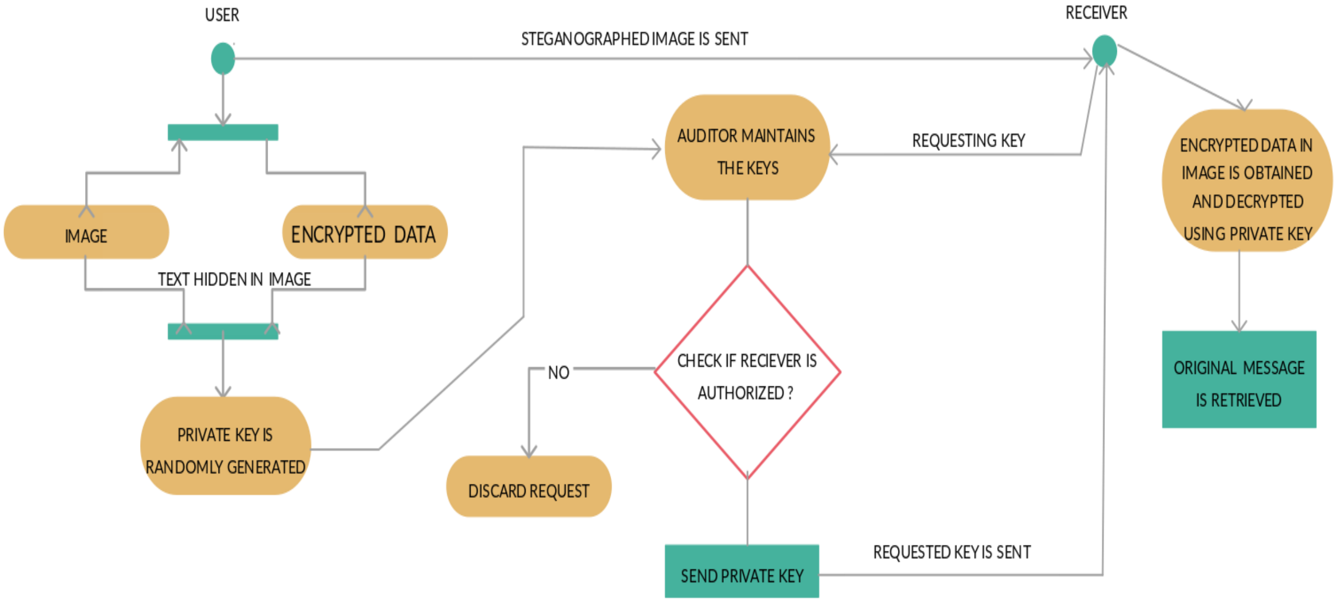
Software used	**:**	Python IDLE.
Operating System	**:**	Microsoft Windows 7 or above.

3.2.5 Hardware Requirements

Processor	**:**	Intel processor IV or above.
RAM	**:**	1 GB or above.
ROM	**:**	500 MB or above.

3.3 List of Figures

3.3.1 Activity Diagram :


USER
RECEIVER
STEGANOGRAPHED IMAGE IS SENT
AUDITOR MAINTAINS THE KEYS
REQUESTING KEY
ENCRYPTED DATA IN IMAGE IS OBTAINED AND DECRYPTED USING PRIVATE KEY
IMAGE
ENCRYPTED DATA
TEXT HIDDEN IN IMAGE
ORIGINAL MESSAGE IS RETRIEVED
NO
CHECK IF RECIEVER IS AUTHORIZED ?
PRIVATE KEY IS RANDOMLY GENERATED
DISCARD REQUEST
REQUESTED KEY IS SENT
SEND PRIVATE KEY

Chapter 4 : Implementation

4.1 Logic

Image steganography involves hiding information within an image in such a way that the alteration is imperceptible to the human eye. The fundamental concept is to use the least significant bits (LSBs) of the pixel values in the image to encode the hidden information. Here's a basic explanation of the logic behind image steganography:

Encoding :

- Represent Information :

Convert the information (message, text, another image) into binary format. This is often done by representing each character in the message as its ASCII value in binary.

- Open the Cover Image :

Choose an image (cover image) in which you want to hide the information.

- Access Pixels :

Access the pixel values of the cover image. In most cases, images are represented using three color channels: red, green, and blue.

- Modify Least Significant Bits (LSBs) :

Replace the least significant bits of the pixel values with the bits of the binary representation of the information. The least significant bits are altered because they have the least impact on the overall color of the pixel, making the changes less noticeable.

- Save the Modified Image:

Save the modified pixel values as a new image. The changes should be imperceptible to the human eye.

Decoding:

- Retrieve LSBs:

Access the least significant bits of the pixel values in the encoded image.

- Assemble Binary Information:

Assemble the binary representation of the hidden information by extracting the least significant bits from each pixel.

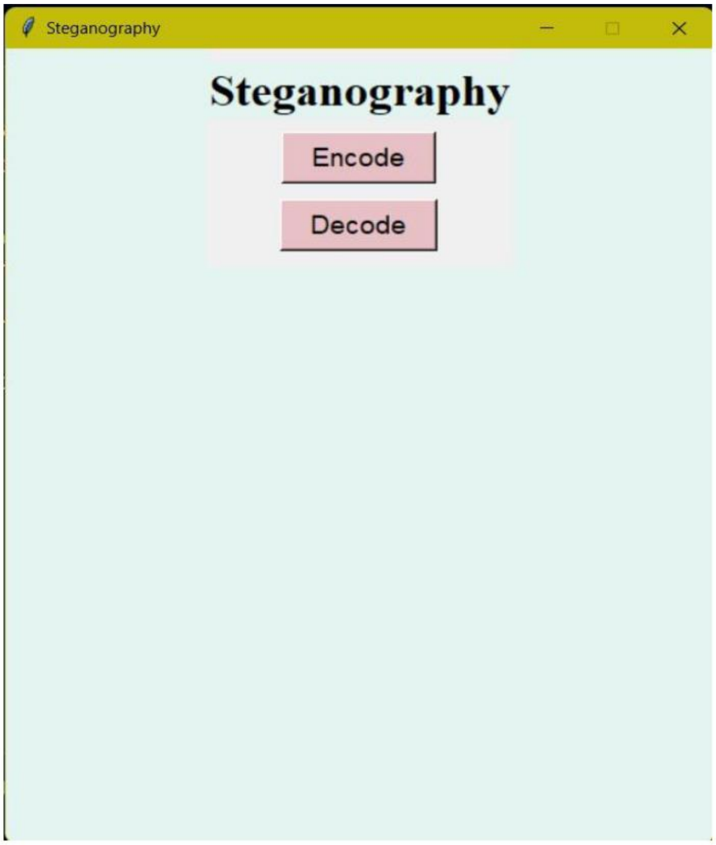
- Convert to Text or Other Data:

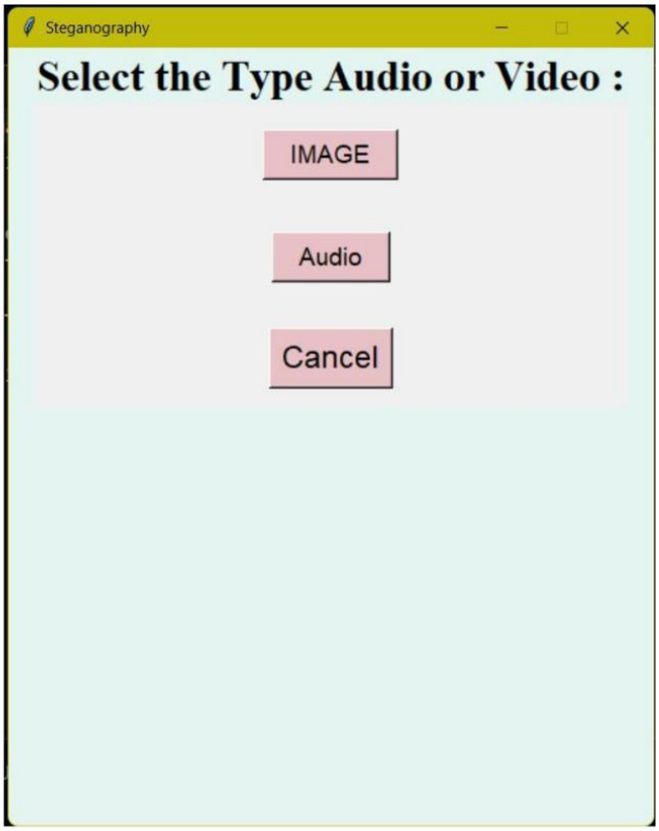
Convert the binary representation back into text, an image, or the original data format.

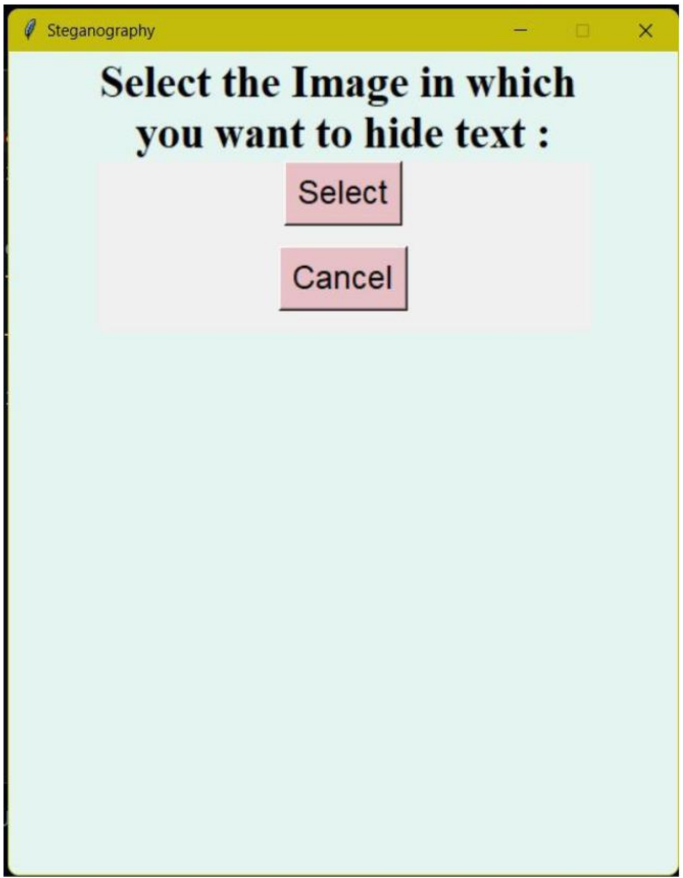
- Access Pixels of the Encoded Image :

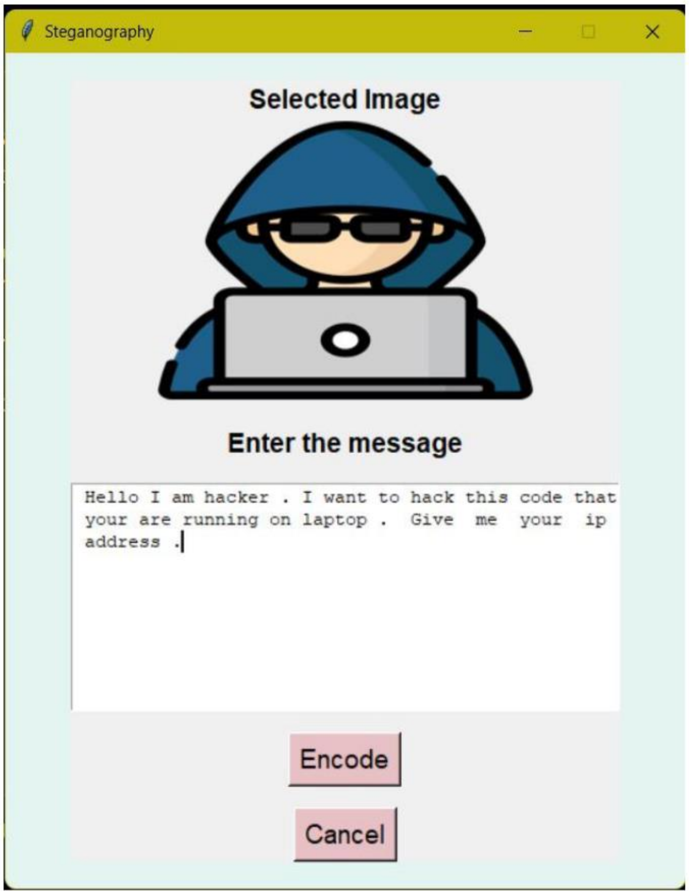
Open the steganographically encoded image.

4.2 Project Screenshots :

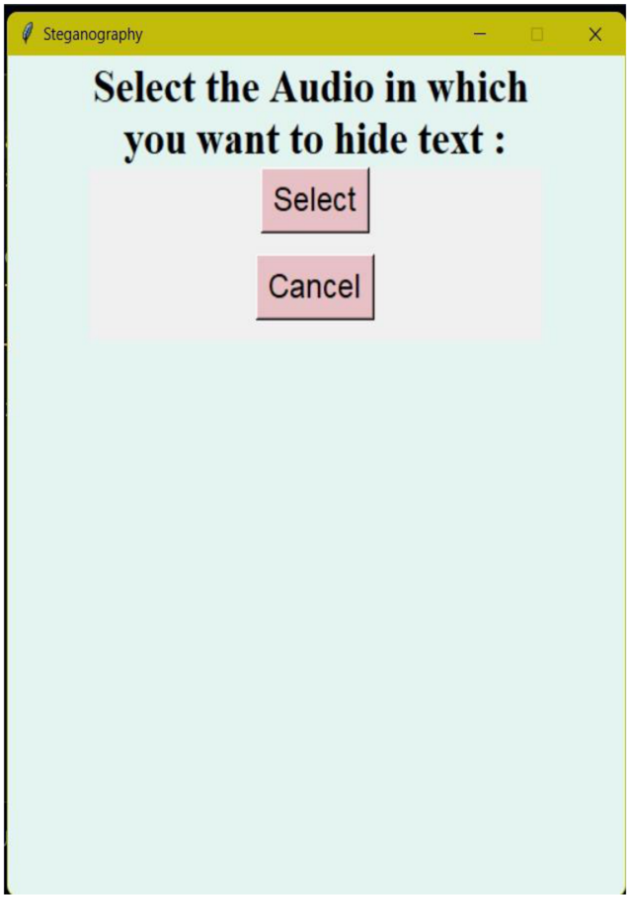




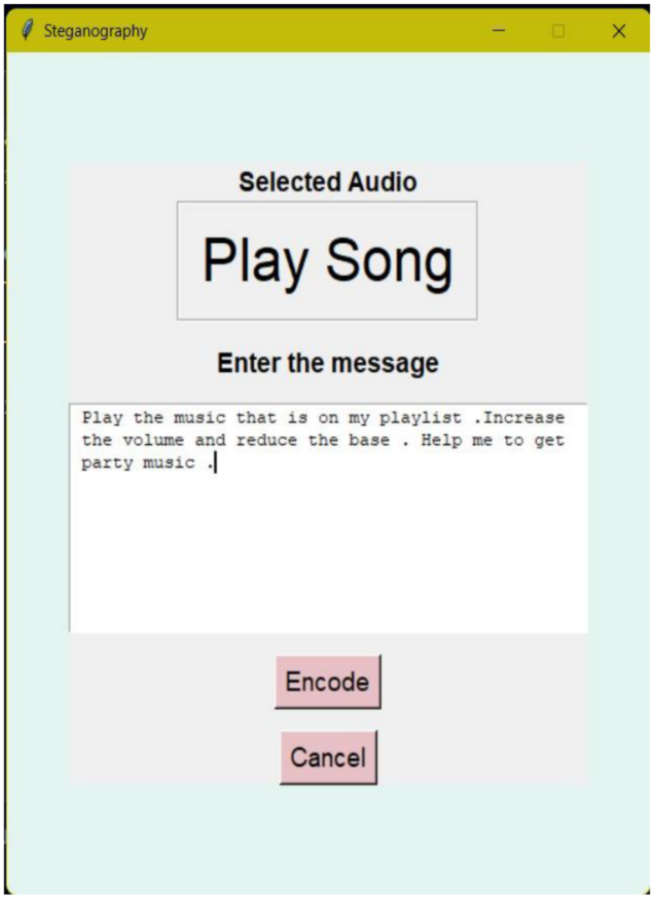




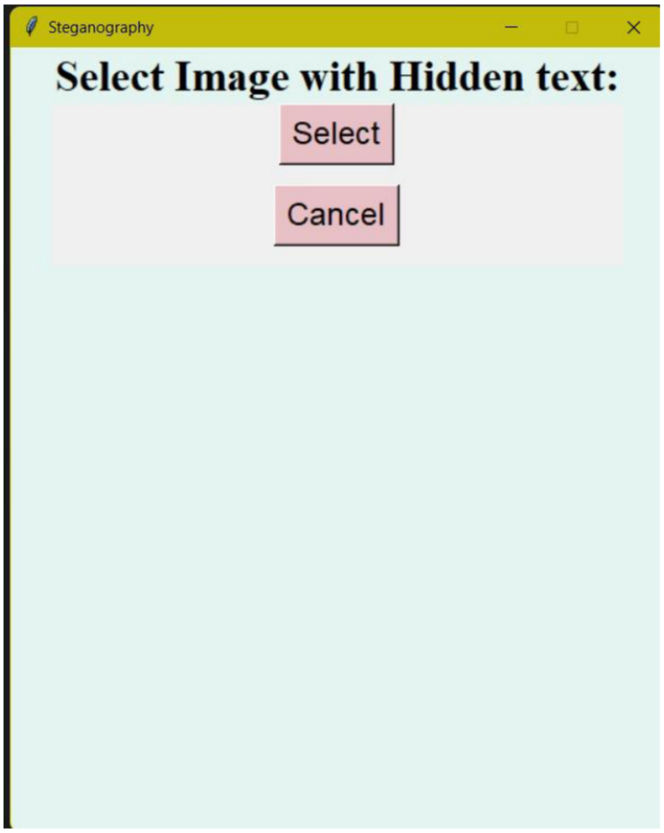
```
Hello I am hacker . I want to hack this code that
your are running on laptop .  Give  me  your  ip
address .
```



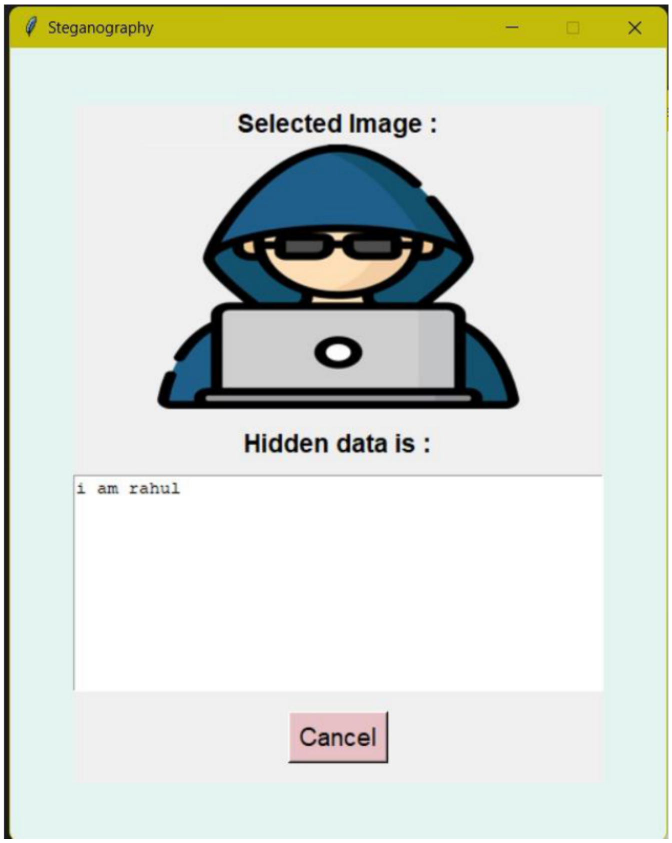
Select the Audio in which you want to hide text :



Play the music that is on my playlist .Increase the volume and reduce the base . Help me to get party music .



Select Image with Hidden text:



i am rahul

Chapter 5 : Conclusion

The Image Steganography project has been a comprehensive exploration into the field of secure communication and data protection through the concealment of information within images. The project aimed to implement a practical and effective steganography system using Python and the Pillow library.

The project successfully implemented image steganography, demonstrating the ability to hide information within images while maintaining visual imperceptibility. The encoding and decoding processes were executed seamlessly using Python, showcasing the practical application of steganographic techniques.

5.1 Future Scope

The future scope of image steganography is influenced by advancements in technology, emerging trends, and evolving security requirements. Here are some potential future directions for image steganography:

Deep Learning Techniques :

- Integration of deep learning techniques for more robust and adaptive steganography methods. Neural networks can be trained to better understand the patterns and features of cover images, leading to more secure hiding of information.

Adversarial Attacks and Defenses :

- Development of steganography techniques that can withstand adversarial attacks. Researchers may focus on creating more resilient methods as well as developing countermeasures to detect hidden information.

Multimedia Steganography :

- Expansion of steganography techniques to other multimedia formats such as audio and video. Research in hiding information in diverse multimedia content will likely be explored for various applications.

Blockchain and Watermarking :

- Integration of steganography with blockchain technology for secure data transfer and storage. Additionally, there may be increased interest in digital watermarking to prove the authenticity and ownership of images.

Quantum Steganography :

- Exploration of steganography techniques in the context of quantum computing. As quantum technologies advance, researchers may investigate how quantum principles can be applied to enhance the security of hiding information.

5.2 References

1. "Steganography and Digital Watermarking: A Practical Guide"
    - Author: Frank Y. Shih
    - Publisher: Wiley
    - Year: 2013
    - ISBN-13: 978-1118004643

2. "A Survey of Steganographic Techniques"
    a. Authors: Ruchika and Neeraj Kumar
    b. Published in: Journal of Network and Computer Applications, 2016.
    c. DOI: 10.1016/j.jnca.2016.06.006

3. Literature Survey,
   http://www.ijetajournal.org/volume11/issue-5.