IMAGE STEGANOGRAPHY

A PROJECT REPORT

Submitted by:

Siddharth Dayal (21BCY10019)

Ruchi Bhattacharjee (21BCY10109)

Harshitaa Ashish (21BCY10123)

Swati (21BCY10210)

VELLORE INSTITUTE OF TECHNOLOGY
VIT
உழைப்பே உயர்வு தரும்

VIT®
BHOPAL
www.vitbhopal.ac.in

in partial fulfillment for the award of the degree

of

BACHELOR IN TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

WITH SPECIALIZATION IN CYBER SECURITY AND DIGITAL FORENSICS

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING

VIT BHOPAL UNIVERSITY

KOTHRI KALAN, SEHORE

MADHYA PRADESH - 466114

FEBRUARY 2023

BONAFIDE CERTIFICATE

Certified that this project report titled" Image **Steganography"** is the bonafide work of "Siddharth **Dayal (21BCY10019), Ruchi Bhattacharjee (21BCY10109), Harshita Ashish (21BCY10123) and Swati (21BCY10210)"** who carried out the project work under my supervision. Certified further that to the best of my knowledge the work reported at this time does not form part of any other project/research work based on which a degree or award was conferred on an earlier occasion on this or any other candidate.

PROGRAM CHAIR	**PROJECT GUIDE**
Dr. D Sarvanan, Program chair, CSE-Cyber	Dr. Soma Saha, Assistant professor
School of Computer Science and Engineering	School of Computer Science and Engineering
VIT BHOPAL UNIVERSITY	VIT BHOPAL UNIVERSITY

The Project Exhibition II Examination is held on February 2023

ACKNOWLEDGEMENT

First and foremost, I would like to thank the Lord Almighty for His presence and immense blessings throughout the project work.

I wish to express my heartfelt gratitude to Dr R. Rakesh, Assistant Professor, Program Chair of CSE-Cyber for much of his valuable support and encouragement in carrying out this work.

I would like to thank my internal guide Mr. Subhash Chandra Patel, for continually guiding and actively participating in my project, giving valuable suggestions to complete the project work.

I would like to thank all the technical and teaching staff of the School of Computer Science and Engineering, who extended directly or indirectly all support.

Last, but not the least, I am deeply indebted to my parents who have been the greatest support while I worked day and night for the project to make it a success.

LIST OF ABBREVIATIONS

- LSB - Least Significant Bit: A common technique in steganography that involves replacing the least significant bits of pixel values with hidden data.
- MSB - Most Significant Bit: The most significant bit in a binary representation of a number. In some steganographic methods, the most significant bits are used for hiding data.
- JPEG - Joint Photographic Experts Group: A popular image format, and JPEG steganography involves hiding data within JPEG images.
- PNG - Portable Network Graphics: Another common image format where steganographic techniques can be applied to hide data.
- GIF - Graphics Interchange Format: While less common, steganography can also be applied to GIF images.
- LSB Matching - A technique that involves making the least significant bit of a pixel value match the hidden data.
- Payload - The amount of data that can be hidden within a cover medium, such as an image.
- Cover Image - The original image or media that is used to hide data within.
- Stego Image - The resulting image or media after data has been hidden within it.
- Steganalysis - The process of detecting and analyzing steganographic content or techniques.
- Key - A secret or shared value that controls the steganographic process. It's often used to encrypt the hidden data for added security.
- Cryptography - The practice of securing the hidden data using encryption techniques.
- Carrier - The medium, such as an image or audio file, used to hide data.
- Hiding Capacity - The maximum amount of data that can be hidden within a carrier while maintaining imperceptibility.
- Embedding Rate - The rate at which data is hidden within the carrier, often expressed as bits per pixel (bpp).
- Cover Distortion - The perceptual changes or artifacts introduced in the carrier as a result of data embedding.
- JPEG - Joint Photographic Experts Group: An image format commonly used for image steganography.
- PNG - Portable Network Graphics: Another image format where steganographic techniques can be applied.
- SSB - Second Significant Bit: In some steganographic techniques, the second significant bit may be used for hiding data, especially when the LSB is not ideal.
- Steganalysis - The process of detecting and analyzing steganographic content or techniques.
- Cryptographic Steganography - The practice of using encryption in conjunction with steganography to enhance the security of hidden data.

LIST OF FIGURES AND GRAPHS AND MODULES

ABSTRACT

Image steganography is a technique that conceals information within digital images to protect sensitive data or enable covert communication. This paper explores the various methods and algorithms employed in image steganography, emphasizing the importance of embedding information in an imperceptible and secure manner. The research delves into the challenges associated with steganalysis, which is the art of detecting hidden data within images, and how modern steganographic methods aim to circumvent these detection techniques.

In addition, this research provides an overview of emerging trends in image steganography, such as the use of deep learning techniques for enhanced security and payload capacity. We discuss the potential applications in areas like secure communication, digital watermarking, and copyright protection, highlighting the ethical and legal considerations that accompany these applications.

TABLE OF CONTENTS (SPECIMEN)

<table>
<tr>
<td>1</td>
<td>1.1 Introduction

1.2 Motivation for the work

1.3 Problem Statement

1.6 Objective of the work</td>
<td>

1

.

.

.</td>
</tr>
<tr>
<td>2</td>
<td>CHAPTER-2:

RELATED WORK INVESTIGATION

2.1 Introduction
2.2 <Core area of the project>
2.3 Existing Approaches/Methods

2.3.1 Approaches/Methods -1

2.3.2 Approaches/Methods -2

2.3.3 Approaches/Methods -3

2.4 <Pros and cons of the stated Approaches/Methods ></td>
<td></td>
</tr>
</table>

5	**CHAPTER-5:** **TECHNICAL IMPLEMENTATION & ANALYSIS** 5.1 Outline 5.2 Technical coding and code solutions 5.3 Working Layout of Forms 5.4 Prototype submission 5.5 Test and validation 5.6 Performance Analysis(Graphs/Charts) 5.7 Summary	
6	**CHAPTER-6:** **PROJECT OUTCOME AND APPLICABILITY** 6.1 Outline 6.2 key implementations outlines of the System 6.3 Significant project outcomes 6.4 Project applicability on Real-world applications 6.4 Inference	

7	**CHAPTER-7:** **CONCLUSIONS AND RECOMMENDATION** 7.1 Outline 7.2 Limitation/Constraints of the System 7.3 Future Enhancements 7.4 Inference	
	Appendix A Appendix B References ***Note: List of References should be written as per IEEE/Springer reference format. (Specimen attached)***	

INTRODUCTION

The area of information security has taken centre stage in an era marked by the fast flow of digital information and the rising demand for safe communication. Image steganography is one of the most exciting and diverse techniques used to preserve the secrecy and integrity of digital data. Image steganography is an intriguing area of steganography, which is the art and science of concealing information in seemingly benign carriers such as photographs, audio files, or papers. This project report looks into the world of picture steganography, investigating its concepts, methodologies, and applications, as well as shining light on its importance in current information security.

As the digital world evolves and data transfer across networks becomes more ubiquitous, it is critical to ensure that sensitive information stays private. Image steganography, in this context, provides a way to embed hidden messages or data into photos while making them look as conventional, unmodified images to the naked eye. This new technology achieves two key goals: data concealing and data protection. By the conclusion of this research, readers will have a thorough grasp of picture steganography, including its historical development, fundamental concepts, diverse methodologies, and real-world applications spanning from cybersecurity to digital forensics.

The voyage begins with an introduction of steganography's history, providing insights into its ancient beginnings and progression into the digital era. As the digital world evolves and data transfer across networks becomes more ubiquitous, it is critical to ensure that sensitive information stays private. Image steganography, in this context, provides a way to embed hidden messages or data into photos while making them look as conventional, unmodified images to the naked eye. This new technology achieves two key goals: data concealing and data protection. By the conclusion of this research, readers will have a thorough grasp of picture steganography, including its historical development, fundamental concepts, diverse methodologies, and real-world applications spanning from cybersecurity to digital forensics.

The voyage begins with an introduction of steganography's history, providing insights into its ancient beginnings and progression into the digital era.

Following that, the paper digs into the fundamentals of picture steganography, clarifying the methods used to embed and retrieve concealed information. Readers will learn to appreciate

the inventive techniques utilised to hide data within an image's pixels through real-world examples and demonstrations that reveal the inner workings of this cryptographic art.

The research also explores approaches for the detection and avoidance of steganography in digital photographs, addressing the essential issue of the security and reliability of steganographic techniques. Given that this technology may be used to secure personal information while also serving as a possible conduit for the transfer of unlawful data, these features are crucial.

The paper concludes with a review of the numerous uses of picture steganography across a variety of industries, from protecting private military communications to facilitating covert data transmission in the healthcare industry. The goal of the paper is to provide readers a thorough understanding of image steganography so they may have a well-rounded understanding of this fascinating and crucial aspect of contemporary information security.

MOTIVATION FOR WORK

In this project on image steganography, our primary motivation stems from the pressing need to enhance digital security and privacy in an increasingly interconnected world. With the persistent threat of cyberattacks and data breaches, concealing information within images has emerged as a critical tool to safeguard sensitive data from prying eyes. Our project is driven by the desire to explore and develop innovative techniques in this field, ultimately contributing to the protection of individuals and organizations in the digital age. We are also motivated by the intellectual challenges and interdisciplinary nature of steganography, offering us an opportunity to apply our knowledge in computer science and signal processing to solve complex problems. Additionally, we recognize the importance of ethical considerations, ensuring that our work aligns with responsible and legitimate use of steganography technology, a crucial aspect we aim to address through our project.

PROBLEM STATEMENT

Steganography hides the very existence of a message, information can be hidden in carriers such as images, audio files, text files, videos and data transmissions. Steganography is a technique for data hiding such that the existence of the secret message is concealed. No one is aware about the existence of the message except the intended recipients. And steganalysis is to identify suspected information streams, determine whether or not they have hidden messages encoded into them, and, if possible, recover the hidden information.

OBJECTIVE OF THE WORK

The objective of our work in this project on image steganography is to develop, evaluate, and demonstrate effective techniques for embedding and extracting concealed information within digital images. Specifically, we aim to achieve the following key objectives:Algorithm Development: Our primary goal is to create novel steganographic algorithms that enable the seamless embedding of data within image files while minimizing perceptual changes to the original image. These algorithms should be robust against detection and capable of concealing various types of information.Security and Privacy Enhancement: We aim to contribute to the enhancement of digital security and privacy by providing tools and methods that individuals and organizations can use to protect their sensitive data. Our work seeks to bolster the confidentiality and integrity of information transmitted through visual media.Performance Assessment: We intend to rigorously evaluate the performance of our steganographic techniques. This includes measuring factors such as data hiding capacity, image quality preservation, and resistance to detection. Through comprehensive testing, we aim to ensure the practical viability of our methods. Real-World Applicability: Our project emphasizes the practical application of steganography. We aspire to demonstrate how the developed techniques can be deployed in various real-world scenarios, such as secure communication, data protection, and digital forensics.Ethical Use and Awareness: An important objective is to promote ethical and responsible use of steganography. We aim to raise awareness about the technology's potential for both constructive and potentially harmful applications and provide guidelines for its responsible implementation.By achieving these objectives, our project endeavors to make a significant contribution to the field of image steganography, advancing both the theoretical understanding and practical utility of this technology in contemporary information security and privacy contexts.

LITERATURE REVIEW

Introduction

Steganalysis is the art of seeing the unseen; to separate stego objects and notstego-objects with practically no information about the steganography based algorithms. The objective of steganalysis is to gather any evidence about the presence of hidden data.
The documents without any hidden messages are called clean documents and the documents with hidden messages are named cover or stego documents.
Steganalysis is usually performed in one of two ways: signature analysis and blind detection. In signature analysis, the steganographic hiding method is known, which makes detection easier. Embedding algorithms always leave a particular signature, which can be tracked for detection.

Concept

Steganographic techniques have been used for centuries. Steganography has been widely used in historical times, especially before cryptographic systems were developed. The first known application dates back to the ancient Greek times, when messengers tattooed messages on their shaved heads and then let their hair grow so the message remained unseen.
The word steganography is based on the Greek word for “covered writing” (steganos = unseen or hidden; graphia = writing), protection of the message is assured by hiding the existence of the message altogether. Sending undecipherable messages is the technique of cryptography and both techniques are often used in conjunction.

Algorithms Used

Least Significant Bit Industry:

Least significant bit (LSB) insertion is a common and simple method to embed data in an image file. In this approach the LSB of a byte is restored with an M’s bit. This technique operate well for image steganography. For hiding data within the images, the LSB (Least Significant Byte) approach is generally used.
An image file is a file that shows multiple colors and intensities of light on different location of an image. The best type of image files to hide data inside is a 24 Bit BMP (Bitmap) image.
When an image is of large quality and resolution it is simpler to hide information within image. Although 24 Bit images are best for hiding data because of their size.

- It can choose a cover image of size M*N as an input.
- The message to be hidden is embedded in RGB element only of an image.

- It can need a pixel selection filter to acquire the best location to hide information in the cover image to acquire a better cost.

- The filter can be used to Least Significant Bit (LSB) of each pixel to conceal record, leaving most significant bits (MSB).

- After that Message is hidden utilizing Bit Replacement method.

Algorithm for embedding data inside image

Begin Input: Cover_Image, Secret_Message, Secret_Key;

Transfer Secret_Message into Text_File;

Zip Text_File; Convert Zip_Text_File to Binary_Codes;

Convert Secret_Key into Binary_Codes;

Set BitsPerUnit to Zero; Encode Message to Binary_Codes;

Add by 2 unit for bitsPerUnit;

Output: Stego_Image;

End

Algorithm for extracting data from stego image

Begin

Input: Stego_Image, Secret_Key;

Compare Secret_Key;

Calculate BitsPerUnit;

Decode All_Binary_Codes;

Shift by 2 unit for bitsPerUnit;

Convert Binary_Codes to Text_File;

Unzip Text_File;

Output Secret_Message;

End

IMPLEMENTATION

1.1 Software Required:

- Windows

1.2 Tools and Technologies

- Python

The language of select for this project was Python. This was a straightforward call for many reasons.

Python as a language has a vast community behind it. Any problems which may be faced is simply resolved with visit to Stack Overflow. Python is the foremost standard language on the positioning that makes it is very straight answer to any question.Python is an abundance of powerful tools ready for scientific computing Packages. The packages like NumPy, Pandas and SciPy area unit freely available and well documented. These Packages will intensely scale back, and variation the code necessary to write a given program. This makes repetition fast. Python is a language as forgiving and permits for the program that appear as if pseudo code. This can be helpful once pseudo code give in tutorial papers should be required and verified. Using python this step is sometimes fairly trivial. However, Python is not without its errors. The python is dynamically written language and packages are area unit infamous for Duck writing. This may be frustrating once a package technique returns one thing that, for instance, looks like an array instead of being an actual array. Plus, the standard Python documentation did not clearly state the return type of a method, this can't lead without a lot of trials and error testing otherwise happen in a powerfully written language. This is a problem that produces learning to use a replacement Python package or library more difficult than it otherwise may be.

- Virtual Studio Code

Visual Studio Code (VS Code) stands out as an exceptionally versatile and user-friendly code editor, prized for its remarkable usability. It has garnered widespread acclaim for its lightweight design, robust features, extensive extension library, and cross-platform compatibility, making it the preferred choice for developers across the globe. The software's minimalistic and intuitive interface offers an excellent user experience, allowing developers to dive right into their coding tasks with ease.

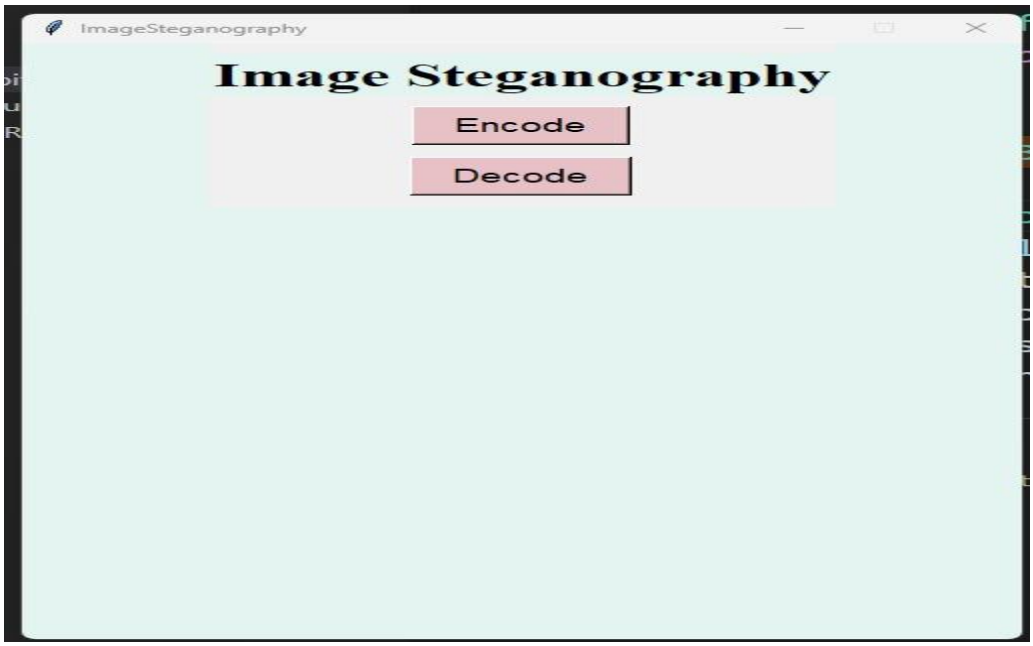
One of the standout features of VS Code is its integrated support for Git, a version control system widely used in software development. This built-in Git integration streamlines the process of managing code repositories, making it easier for developers to collaborate and track changes to their projects.

Additionally, VS Code boasts IntelliSense, an intelligent code completion and suggestion feature that accelerates the coding process by providing context-aware recommendations. This feature significantly reduces the chances of errors and accelerates coding, particularly for languages like Python, JavaScript, and TypeScript. Furthermore, the code editor includes debugging tools that facilitate the identification and resolution of issues, ensuring smooth and error-free coding.

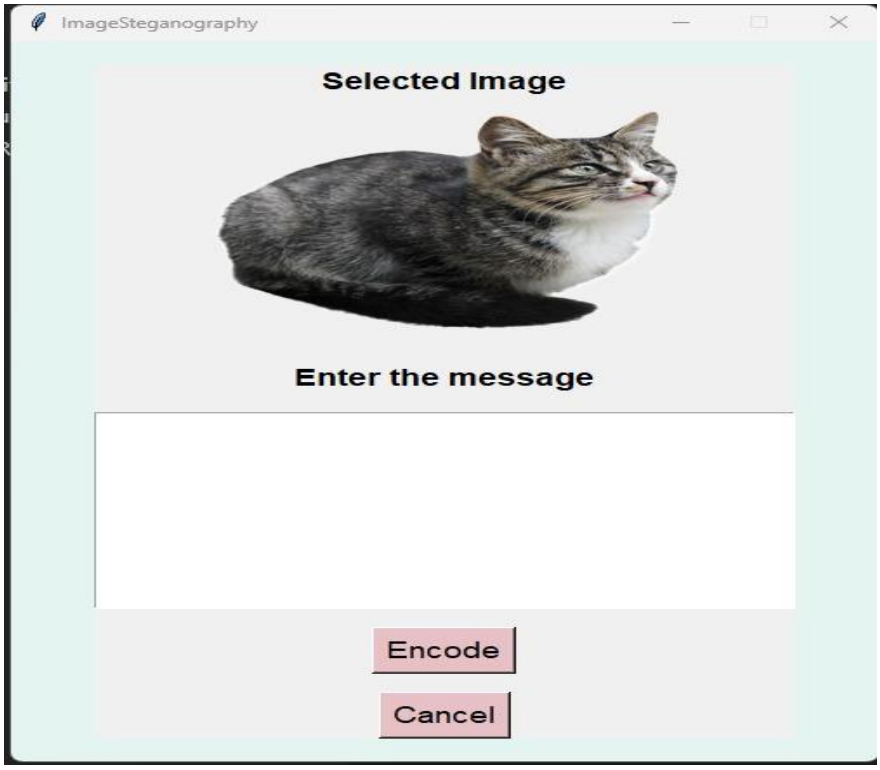
What sets VS Code apart is its adaptability, with support for a vast array of programming languages and frameworks. Its constant updates and a vibrant developer community continually enhance its functionality, ensuring that it remains a top choice for software development projects of all sizes and complexities. Whether you are a seasoned developer or a beginner, Visual Studio Code is a versatile and efficient tool that caters to a broad spectrum of coding needs.

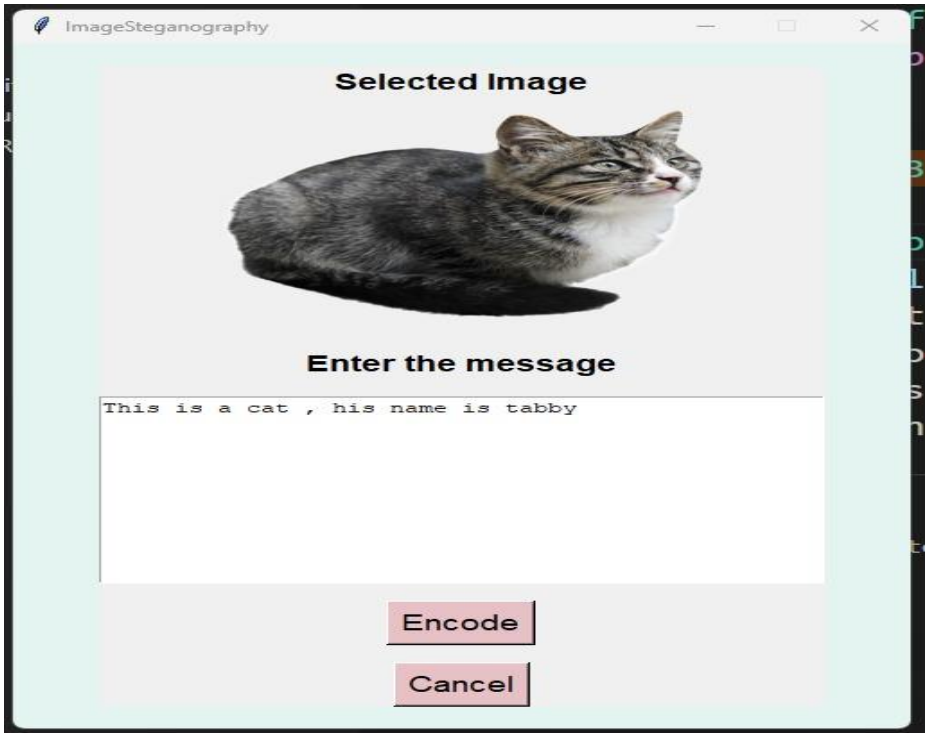
1.3 Implementation Display:

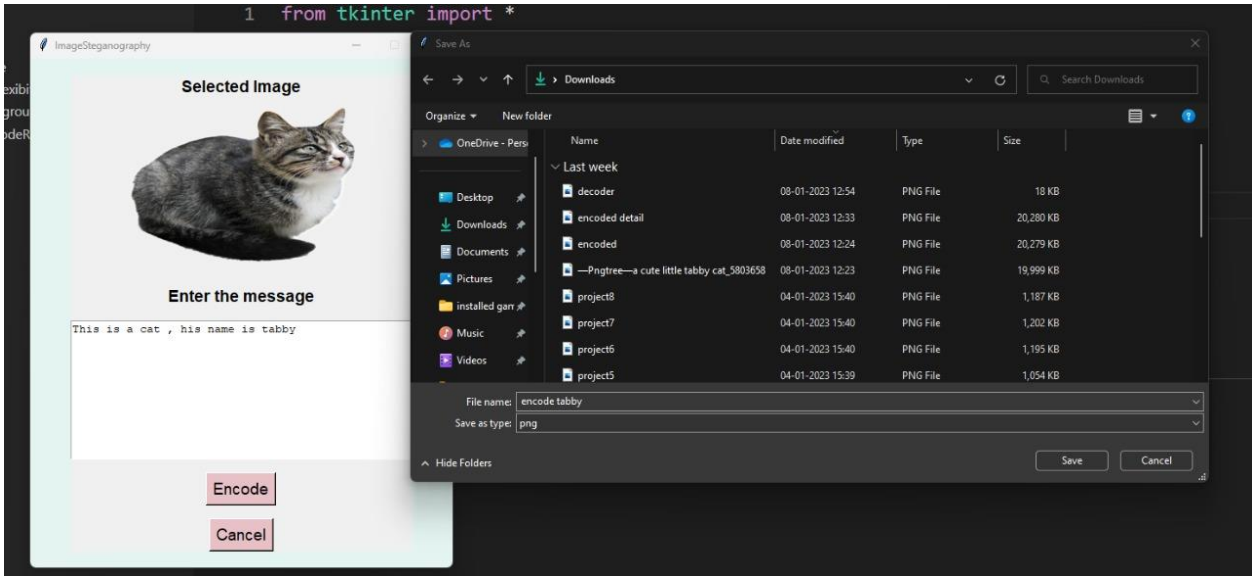
- Encoding

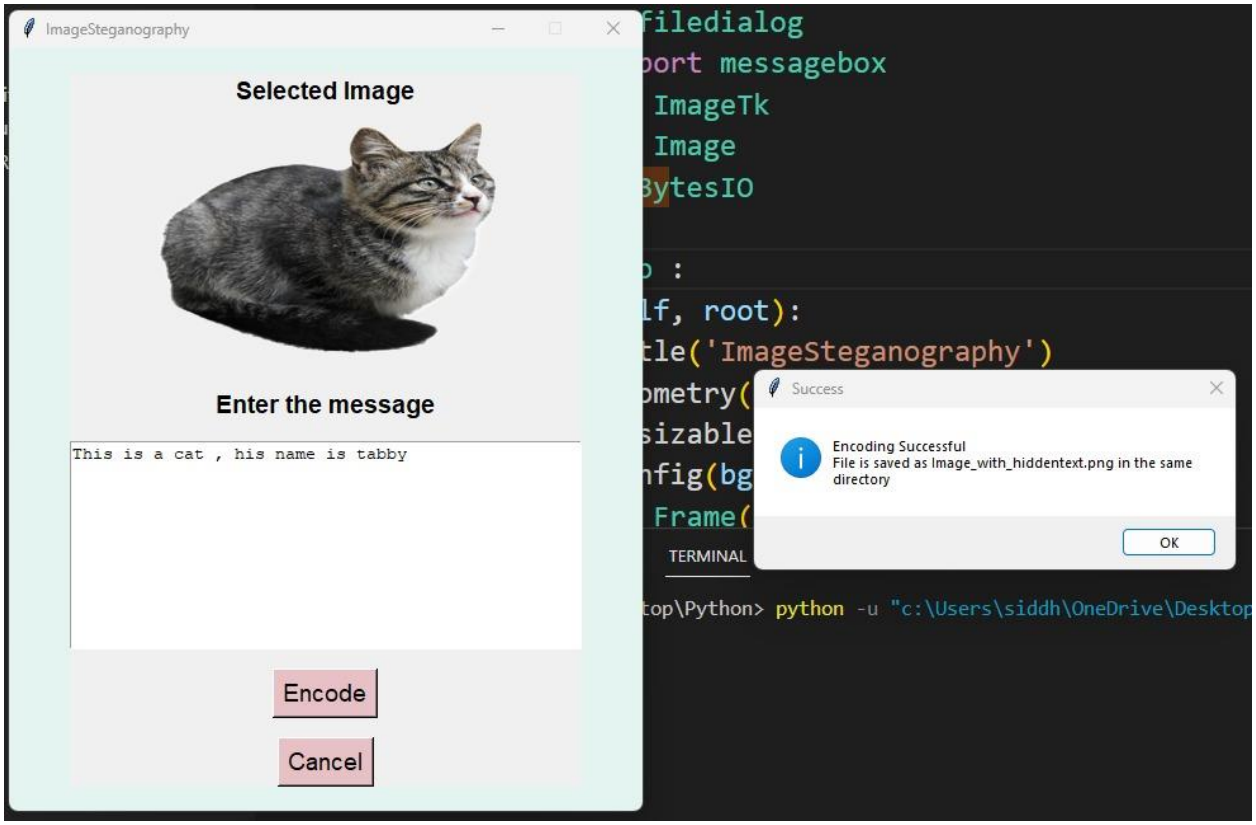

ImageSteganography
Image Steganography
Encode
Decode


ImageSteganography
Select the Image in which you want to hide text :
Select
Cancel

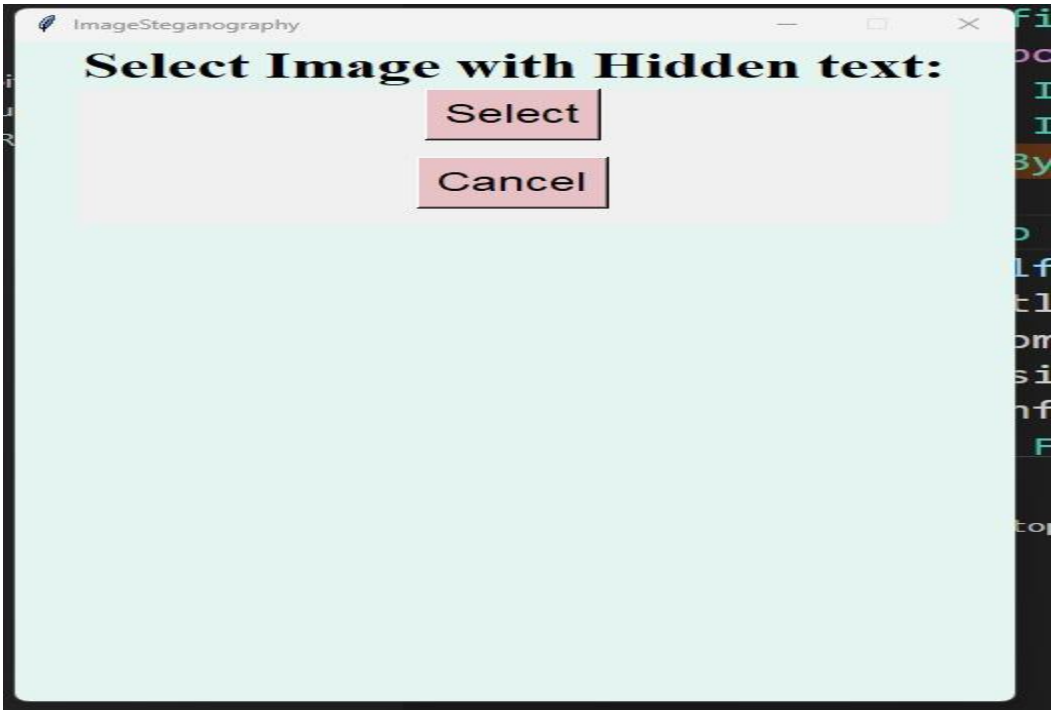

ImageSteganography
Selected Image
Enter the message
Encode
Cancel

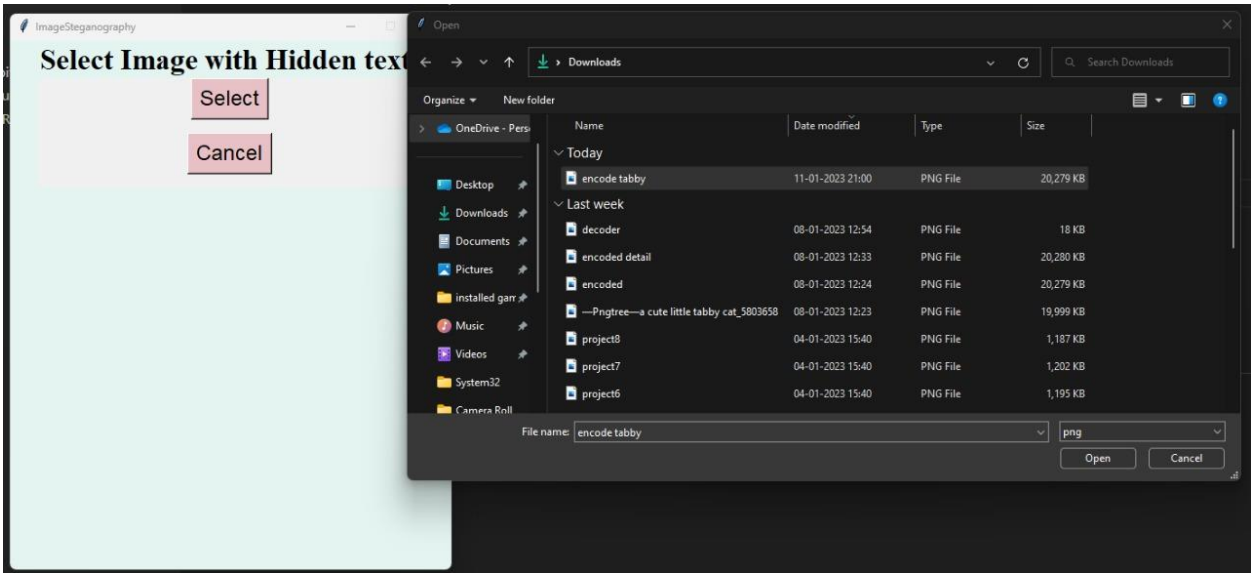

ImageSteganography
Selected Image
Enter the message
This is a cat , his name is tabby
Encode
Cancel


from tkinter import *
ImageSteganography
Selected Image
Enter the message
This is a cat , his name is tabby
Encode
Cancel
Save As
Downloads
Search Downloads
Organize
New folder
OneDrive - Pers
Desktop
Downloads
Documents
Pictures
installed gam
Music
Videos
Name
Date modified
Type
Size
Last week
decoder 08-01-2023 12:54 PNG File 18 KB
encoded detail 08-01-2023 12:33 PNG File 20,280 KB
encoded 08-01-2023 12:24 PNG File 20,279 KB
—Pngtree—a cute little tabby cat_5803658 08-01-2023 12:23 PNG File 19,999 KB
project8 04-01-2023 15:40 PNG File 1,187 KB
project7 04-01-2023 15:40 PNG File 1,202 KB
project6 04-01-2023 15:40 PNG File 1,195 KB
project5 04-01-2023 15:39 PNG File 1,054 KB
File name: encode tabby
Save as type: png
Hide Folders
Save
Cancel


ImageSteganography
Selected Image
Enter the message
This is a cat , his name is tabby
Encode
Cancel
filedialog
port messagebox
ImageTk
Image
BytesIO
lf, root):
tle('ImageSteganography')
ometry(
sizable
nfig(bg
Frame(
TERMINAL
top\Python> python -u "c:\Users\siddh\OneDrive\Desktop
Success
Encoding Successful
File is saved as Image_with_hiddentext.png in the same directory
OK

- Decoding


ImageSteganography
Select Image with Hidden text:
Select
Cancel


ImageSteganography
Select Image with Hidden text
Select
Cancel
Open
Downloads
Search Downloads
Organize
New folder
OneDrive - Pers
Desktop
Downloads
Documents
Pictures
installed gam
Music
Videos
System32
Camera Roll
Name
Date modified
Type
Size
Today
encode tabby 11-01-2023 21:00 PNG File 20,279 KB
Last week
decoder 08-01-2023 12:54 PNG File 18 KB
encoded detail 08-01-2023 12:33 PNG File 20,280 KB
encoded 08-01-2023 12:24 PNG File 20,279 KB
---Pngtree---a cute little tabby cat_5803658 08-01-2023 12:23 PNG File 19,999 KB
project8 04-01-2023 15:40 PNG File 1,187 KB
project7 04-01-2023 15:40 PNG File 1,202 KB
project6 04-01-2023 15:40 PNG File 1,195 KB
File name: encode tabby
png
Open
Cancel

ImageSteganography

Selected Image :

Hidden data is :

This is a cat , his name is tabbyÿ

Cancel

CONCLUSION

In conclusion, the Image Steganography project has been a journey through the fascinating world of data concealment within images, shedding light on the historical evolution, principles, techniques, and real-world applications of this intriguing field. Steganography, as an age-old art, has seamlessly transitioned into the digital age, offering a vital solution for ensuring data privacy and security.

Throughout this project, we've delved into the core principles of image steganography, unravelling the ingenious techniques used to embed information within the pixels of an image. We've explored both the creative artistry and the mathematical precision involved in the practice of hiding data within the visual spectrum.

Moreover, the project has emphasized the importance of security and robustness in steganographic techniques. By understanding the methods for detecting and preventing steganography, we've recognized the dual nature of this technology—a tool for safeguarding privacy and a potential vector for covert data transmission. This knowledge is indispensable in the ever-evolving landscape of digital security.

The significance of this project extends beyond theoretical understanding, as image steganography finds applications in diverse domains. From securing military communications to enabling clandestine data transfer in healthcare and various other fields, it's a technology that continues to evolve and adapt to meet contemporary challenges.

As we conclude this project, we're reminded of the perpetual importance of data security and the pivotal role that image steganography plays in this realm. It has been a journey of discovery, appreciation, and reflection, and it is our hope that the insights gained here will serve as a foundation for future explorations and applications in the field of information security and cryptography.

REFERENCES

https://www.ieee.org/searchresults/index.html?q=steganalysis#gsc.tab=0&gsc. q=steganalysis&gsc.page=1

https://link.springer.com/search?query=steganalysis

https://www.researchgate.net/publication/292310394_Image_Steganography_ Techniques_An_Overview

https://www.geeksforgeeks.org/image-steganography-in-cryptography/

Huaiqing Wang and Shuozhong Wang. 2004. Cyber warfare: steganography vs. steganalysis. Commun. ACM 47, 10 (October 2004), 76–82.