DATA HIDER

A MINI PROJECT REPORT

Submitted by

ANTHONI THOMAS.R (732119205005)

LAKSHMANAKUMAR.V (732119205024)

PON PANDIAN.P (732119205038)

SEKAR.S (732119205047)

In partial fulfilment for the award of the degree of

BACHELOR OF TECHNOLOGY

in

INFORMATION TECHNOLOGY

NANDHA COLLEGE OF TECHNOLOGY, ERODE-52

DEPARTMENT OF INFORMATION TECHNOLOGY

ANNA UNIVERSITY, CHENNAI - 600 025

JUNE 2022

ANNA UNIVERSITY: CHENNAI 600 025

BONAFIDE CERTIFICATE

Certified that this Mini Project report titled "DATA HIDER" is the bona-fide work of ANTHONI THOMAS.R (732119205005), LAKSHMANAKUMAR.V (732119205024), PON PANDIAN.P (732119205038) and SEKAR.S (732119205047) who carried out the project under my supervision.

……...	**…….**
SIGNATURE	**SIGNATURE**
Mr.T.SURESHKUMAR,.M.E.,(Ph.D).,	**Mr.T.KRISHNAKAARTHIK,M.E.,(Ph.D).,**
HEAD OF THE DEPARTMENT	**SUPERVISOR**
Information Technology,	Assistant Professor,
Nandha College Of Technology,	Information Technology ,
Erode-638052	Nandha College Of Technology,
	Erode-638052

Submitted for the end semester university mini project viva-voce examination held on_____.

Internal Examiner **External Examiner**

ACKNOWLEDGEMENT

We express our thanks to our beloved chairman of Sri Nandha Educational Trust **Thiru. V. Shanmugan** and our beloved Secretaries, **Thiru. S. Nandhakumar Pradeep** and **Thiru. S. Thirumoorthi** of Nandha Educational Institutions for theirsupport in successful completion of our project work.

We specially thank **Dr. S. Arumugam**, Chief Executive Officer of Nandha Educational Institutions for his affection and support in all aspects have made as tocomplete the course successfully.

We wish to express our deep sense of gratitude to our beloved Principal **Dr.S.Nandagopal,M.E.,Ph.D.,** for the excellent facilities and continual support provided during the course study and project.

We articulate our genuine and sincere thanks to our dear hearted Head of the Department **Mr.T.Sureshkumar,M.E.,(Ph.D).,** who has been the key spring of motivation to us throughout the completion of our course and our project work.

We articulate our genuine and sincere thanks to our Project Guide Mr.T.Krishnakaarthik,M.E.,(Ph.D)., who has been the key spring of motivation to us throughout the completion of our course and our project work.

We articulate our genuine and sincere thanks to our Project coordinator **Mr.T.Krishnakaarthik,M.E.,(Ph.D).,** for providing us support for our project. We are very much gratified to all the teaching and non-teaching staff of our department who has direct and indirect stroke throughout our progress. Our heartfelt thanks to our friends who have supported us with their unconditional love and encouragement. Finally, we would like to thank the Almighty for his blessings.

TABLE OF CONTENTS

ABSTRACT

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different camera file formats can be used, but digital images are the most popular became of their frequency on the Internet. For hiding secret information in images, there exists a large variety of stegnography techniques some are more implex than others and all of them have respective string and weak points. Different applications have different requirements of the steganography technique word. mFor example, some applications may require absolute invisibility of the secret information, while others require a larger secrect message to be hidden. This project hides the message with in the image For a more secure approach, the poject it allows user to choose the hits for replacement instead of LSB replacement In the Image viewer select the cover image with the series text or text file and hide it in to the image with the hit employment choice, it help to genetate the secure stego in the stegno area is set to the destination with the help of a private or public communication network on the other side of the receiver and the receiver download the stegno image and using the software retrieve the secret text hidden in the stege image.

LIST OF FIGURES

LIST OF ABBREVATIONS

PIP	**:**	Performance Improvement Plan
CMD	**:**	Command Prompt
PY	**:**	Python
IDLE	**:**	Integrated Development and Learning
E-COMMERCE	**:**	Electronic Commerce
BMP	**:**	BitMap
LSB	**:**	Least Significant Bit
OS	**:**	Operating System
RAM	**:**	Random Access Memory
PNG	**:**	Portable Network Graphics
JPG	**:**	Joint Photographic Experts Group
GIF	**:**	Graphics Interchange Format

CHAPTER 1

INTRODUCTION

1.1 MOTIVATION

As the advancement of the internet increased, it has become an important factor in information technology and plays a vital role in communication The security of information is becoming a bigger concern Cryptography is the technique which secures the communication. There are various methods developed for encrypting and decrypting the information, which secures the message. Due to the increase of the technology, sometimes cryptography is not enough for keeping the information as secret. It also important to retain the existence of the information secret. Steganography is the technique which is used to implement it. It is achieved by hiding the information inside other information, thus the existence of communicated message is hidden.

This chapter provides the information about how steganography is different from cryptography and also how the steganography process is performed. During the Second World War, Germans developed the Microdot technique. Using that technique, they have decreased the size of the information such as photographs to the typed period size. It is very difficult to detect, as the cover message is sent over a channel which contains the hidden message on one period of the paper. In today's world steganography is most commonly used on computers with networks as the delivery channels and digital data as the carriers (Provos & Honeyman, 2003).

Steganography is different from the cryptography because cryptography focuses on keeping information secret whereas steganography focuses on making the existence of the information secret. Though both ways are used to protect the data/information from outsiders, the technology is not perfect and can compromised. Once it is suspected or revealed that the hidden information ex-

ists, the steganography purpose is defeated partly. Steganography can be strengthened by combining it with the cryptography. It is known that watermarking is a method used for hiding the trademark information in software, images and music. It is not considered as original form of steganography (Patel, & Tahilraman, 2016.).

In steganography the message is hidden in the image, but watermarking will add something on top of the image for example a word "Confidential", which will become part of the picture. There is a misconception that steganography is related or similar to encryption, but in real they are different. Encryption is a technology which converts the message from a readable to an unreadable format for protecting the sensitive data. Whereas, in steganography the information is hidden from the plain view and it is not mandatory to be encrypted.

1.2 OBJECTIVE

The internet is considered the most powerful tool of information and communication technology. The underlying issue has always been security that is provided to secure the information.

Unfortunately, sometimes it is not enough to keep the contents of a message secret but also to send the secret information securely. How a secret and confidential information is hidden and communicated securely, and which will be the best way for communicating. These are the things to know, for achieving the safe communication.

1.3 PROJECT OVERVIEW

The growing use of Internet needs to take attention while we send and to receive personal information in a secured manner. For this, there are many approaches that can transfer the data into different forms so that their resultant data can be understood if it can be returned back into its original form. This technique is known as encryption. However, a major disadvantage of this method is that the existence of data is not hidden. If someone gives enough time then the unreadable encrypted data may be converted into its original form. A solution to this problem has already been achieved by using a "steganography" technique to hide data in a cover media so that other cannot notice it.

The characteristics of the cover media depends on the amount of data that can be hidden, the perceptibility of the message and its robustness. In this document, We propose a new system for hiding data stands on many methods and algorithms for image hiding where We store on data file, called sink file in an image file called as container image. The primary objective is to use steganography techniques so as to provide more security and simultaneously using less storage.

CHAPTER 2

SYSTEM REQUIREMENTS

2.1 HARDWARE REQUIREMENTS

Processor	**:**	Intel Core-i3
RAM	**:**	Min 2gb

2.2 SOFTWARE REQUIREMENTS

Operating System	**:**	Windows10
Tool	**:**	Python IDLE, Command Prompt, PIP
Language	**:**	Python

2.3 SOFTWARE DESCRIPTIONS

The execution phase was developed based upon three phases. The different phases are encryption, decryption and implementation phases. We require few hardware and software interfaces for implementing these phases. The software interface which is implemented in this project is done using the Python IDLE running in the Windows environment. The main aim of the project is to improve the data security when the data is transmitted using the transmission medium. This can be done by embedding the secret data into the image file and then transmitting the encrypted data through the transmission medium. Then, the carrier image file is decrypted at the destination by using the secret key. For implementing the above procedure, we used the Python IDLE to create the steganographic application. The proposed method in this project can be used for both "encryption" and "decryption" of the message from the digital image.

CHAPTER 3

APPLICATIONS OF SYSTEM

3.1 ADVANTAGES

The main advantages of this system is Security that it provides security to your messeages without knowing to third party. Number of hits have been replaced according to user or sender, therefore third party cannot question password Normal network user cant goes image in steganography anyone cannot jump as a suspect by looking images.

- It is Reliable.
- Easy to use
- Easy Maintenance
- System have been secured by password authentication..

3.2 DISADVANTAGES

Images can have attacks like diluting, nosing, contrast changes and so on Number hits of pixel should be replaced by equal hits of manage. If someone is eavesdropping then then there is probability of age get unfold. If more than two people having satue steganography, software then hidden the message. This software has been implemented by python, which is open source, therefore mode is readable so anyone with bad mentality can make software perfoms a inverse operation. Only unintended user may know the actual working of software. Intruder may penetrate suspecting images to get hidden data.

3.3 APPLICATIONS

- Confidential Communication and secret data storing.
- Protection AI data Alteration: Acess Control System for Digital Content Distribution.
- E-Commerce.
- Malia.
- Database Systems .

CHAPTER 4

IMPLEMENTATION

4.1 PROBLEM STATEMENT

This project addresses the security problem of transmitting the data over internet network, the main idea coming when we start asking that how can we send a message secretly to the destination? The science of steganography answers this question. Using steganography, information can be hidden in carriers such as images, audio files, text files, videos and data transmissions. In this document, we proposed some methods and algorithms of an image steganography system to hide a digital text of a secret message.

The internet is considered the most powerful tool of information and communication technology. The underlying issue has always been security that is provided to secure the information.

Unfortunately, sometimes it is not enough to keep the contents of a message secret but also to send the secret information securely. How a secret and confidential information is hidden and communicated securely, and which will be the best way for communicating. These are the things to know, for achieving the safe communication.

4.2 Nature and Significance of the Problem

The purpose was to analyze the information hiding techniques that may help the users. sharing the information so that, such information will reach the intended person(s) without being detected by other computer users (intruders or attackers) when carrying out day to day tasks and organizational activities

4.3 **Background Related to the Problem**

Hiding information into a medium requires following elements.

- The cover medium(C) that holds the secret message.
- The secret message (M), it can be a plain text, an image file or any other type of data.
- The steganography techniques which are going to be used to hide the information
- A stego-key (K) which will be used for hiding and un-hiding the message.

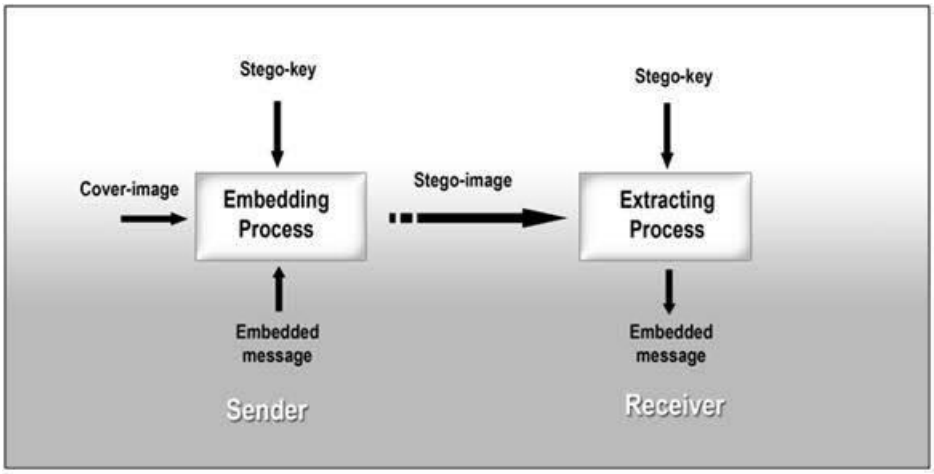

FIGURE : 4.3.1 – BACKGROUND PROCESS

4.4 Types of Steganography

Image steganography. This is the popular method in which images are used as the cover medium for steganography. A message is inserted in a digital image by using an algorithm and the secret key. There are various ways for embedding the secret message into an image. Also, the secret key is an optional thing unless it is required.

Though, it adds additional security for the information that is being transferred. The result which is a stego-image is sent to the receiver. On the receiver side, the stego-image is processed by the extraction of algorithm using the same secret key.

In the process of communicating the stego-image, other than the authenticated persons nobody can be able to notice the existence of the secret message which is hidden in the image though they identify the transmission of a stego-image. So, it overcomes the problem of suspicion by the attacker or unauthorized persons who capture the information during the communication (Banerjee & Indradip, 2011).

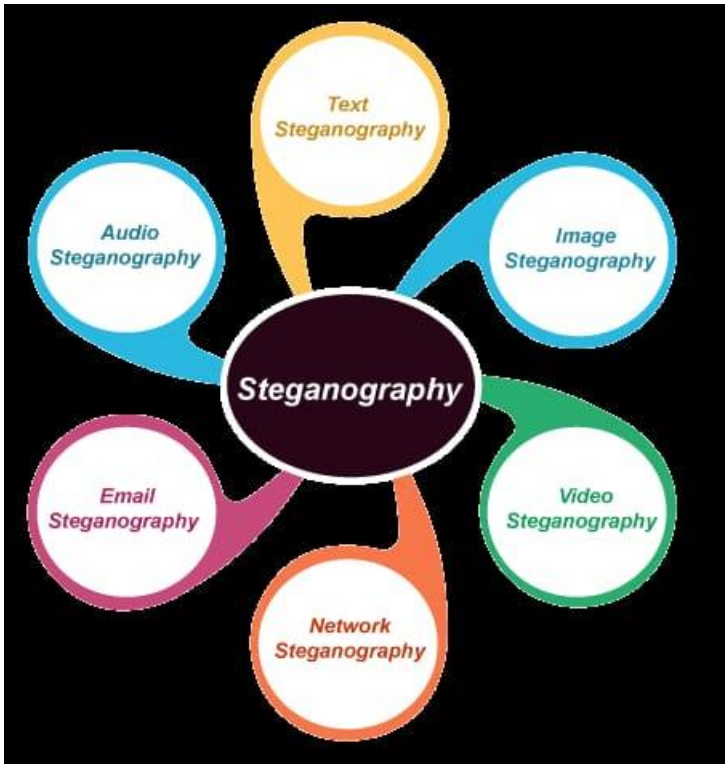

FIGURE : 4.4.1 – TYPES OF STEGANOGRAPHY

4.5 Overview of Image Steganography

The overall process of the image steganography is to hide the sensitive data or information inside a cover image without the degradation of the original image, hence providing the security by which no unauthorized person can access the information which is hidden. There are different methods by which an image steganography is achieved. Below is the classification of the techniques of the image steganography.

CHAPTER 5

TESTING

Testing is the process of evaluating a system or its component(s) with the intent to find whether it satisfies the specified requirements or not. In simple words, testing is executing a system in order to identify any gaps, errors, or missing requirements in contrary to the actual requirements. A process of analyzing a software item to detect the differences between existing and required conditions (that is defects/errors/bugs) and to evaluate the features of the software item.

Unit Testing

Unit testing is performed by the respective developers on the individual units of source code assigned areas. The developers use test datathat is different from the test data of the quality assurance team. The goal of unit testing is to isolate each part of the program and show that individual parts are correct in terms of requirements and functionality.

Integration Testing

Integration testing is defined as the testing of combined parts of an application to determine if they function correctly. Integration testing can be done in two ways: Bottom-up integration testing and Top-down integration testing.

Bottom-up integration

This testing begins with unit testing, followed by tests of progressively higher-level combinations of units called modules or build

Top-down integration

In this testing, the highest-level modules are tested first and progressively lower-level modules are tested there after.We manually tested the code using the Python IDLE , Command Prompt and using the PIP package.

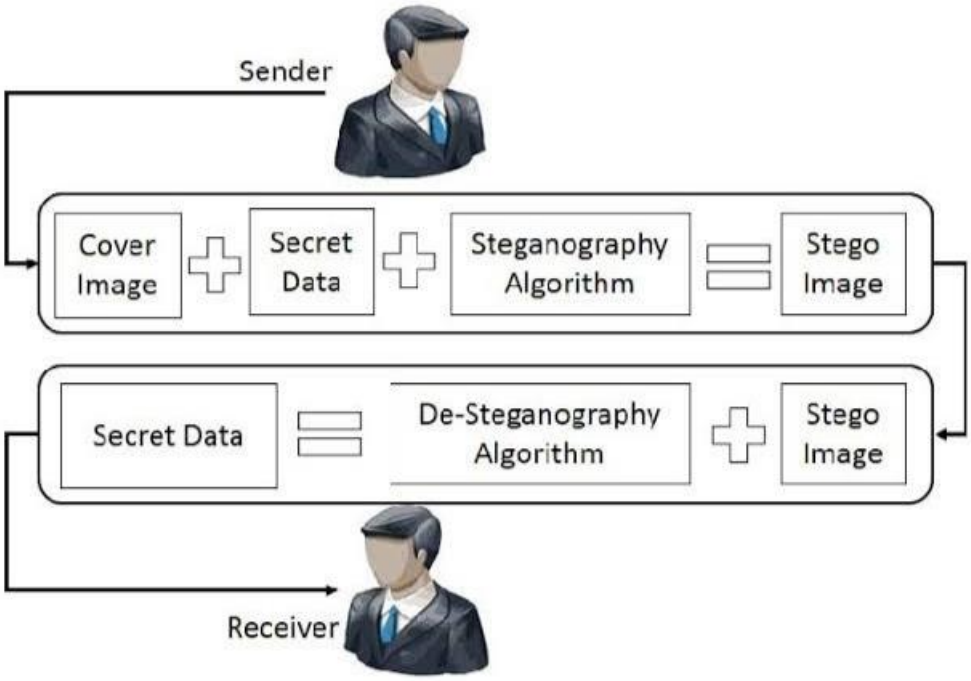

FIGURE : 5.1 – SENDER AND RECEIVER DIAGRAM

CHAPTER 6

CONCLUSION AND FUTURE RECOMMENDATIONS

CONCLUSION

Although only some of the main image steganographic techniques were discussed in this document, one can see that there exists a large selection of approaches to hiding information in images. All the major image file formats have different methods of hiding messages, with different strong and weak points respectively. Where one technique lacks in payload capacity, the other lacks in robustness. For example, the patchwork approach has a very high level of robustness against most type of attacks, but can hide only a very small amount of information.

Least significant bit (LSB) in both BMP and GIF makes up for this, but both approaches result in suspicious files that increase the probability of detection when in the presence of a warden.

The proposed approach in this project uses a new steganographic approach called image steganography. The application creates a stego image in which the personal data is embedded inside the cover file image.

Used the Least Significant Bit algorithm in this project for developing the application which is faster and reliable and compression ratio is moderate compared to other algorithms.

FUTURE RECOMMENDATIONS

The major limitation of the application is designed for images cover files. It accepts only images as a carrier file. The future work on this project is to improve the compression ratio of the image to the text. This project can be extended to a level such that it can be used for the different types of multimedia files.

APPENDIX

CODING

```
from tkinter import *
from tkinter import filedialog
import tkinter as tk
from PIL import Image,ImageTk
import os
from stegano import lsb #pip install stegano


root=Tk()
root.title("Steganography - Hide a Secret Text Message in an Image")
root.geometry("700x500+250+180")
root.resizable(False,False)
root.configure(bg="#2f4155")


def showimage():
  global filename
  filename=filedialog.askopenfilename(initialdir=os.getcwd(),title='Select Im-
age File',filetype=(("PNG file","*.png"),("JPG File","*.jpg"),("All
file","*.txt")))
  img=Image.open(filename)
  img=ImageTk.PhotoImage(img)
  lbl.configure(image=img,width=250,height=250)
```

```
    lbl.image=img
def Hide():
    global secret
    message=text1.get(1.0,END)
    secret=lsb.hide(str(filename),message)
def Show():
    clear_message=lsb.reveal(filename)
    text1.delete(1.0, END)
    text1.insert(END, clear_message)
def Save():
    secret.save("hidden.png")

#icon
image_icon=PhotoImage(file="logo.jpg")
root.iconphoto(False,image_icon)



#logo
logo=PhotoImage(file="logo.png")
Label(root,image=logo,bg="#2f4155").place(x=10,y=0)
Label(root,text="DATA HIDER",bg="#2d4155",fg="white",font="arial 25
bold").place(x=100,y=20)

#first Frame
f=Frame(root,bd=3,bg="black",width=340,height=280,relief=GROOVE)
```

```
f.place(x=10,y=80)

lbl=Label(f,bg="black")
lbl.place(x=40,y=10)

#second Frame
frame2=Frame(root,bd=3,width=340,height=280,bg="white",relief=GROOVE)
frame2.place(x=350,y=80)
text1=Text(frame2,font="Robote
20",bg="white",fg="black",relief=GROOVE,wrap=WORD)
text1.place(x=0,y=0,width=320,height=295)
scrollbar1=Scrollbar(frame2)
scrollbar1.place(x=320,y=0,height=300)
scrollbar1.configure(command=text1.yview)
text1.configure(yscrollcommand=scrollbar1.set)

#third Frame
frame3=Frame(root,bd=3,bg="#2f4155",width=330,height=100,relief=GROOV
E)
frame3.place(x=10,y=370)

Button(frame3,text="Open Image",width=10,height=2,font="arial 14
bold",command=showimage).place(x=20,y=30)
Button(frame3,text="Save Image",width=10,height=2,font="arial 14
bold",command=Save).place(x=180,y=30)
```

```
Label(frame3,text="Picture, Image, Photo
File",bg="#2f4155",fg="yellow").place(x=20,y=5)

#fourth Frame
frame4=Frame(root,bd=3,bg="#2f4155",width=330,height=100,relief=GROOV
E)
frame4.place(x=360,y=370)

Button(frame4,text="Hide Data",width=10,height=2,font="arial 14
bold",command=Hide).place(x=20,y=30)
Button(frame4,text="Show Data",width=10,height=2,font="arial 14
bold",command=Show).place(x=180,y=30)
Label(frame4,text="Picture, Image, Photo
File",bg="#2f4155",fg="yellow").place(x=20,y=5)
root.mainloop()
```

SCREENSHOTS

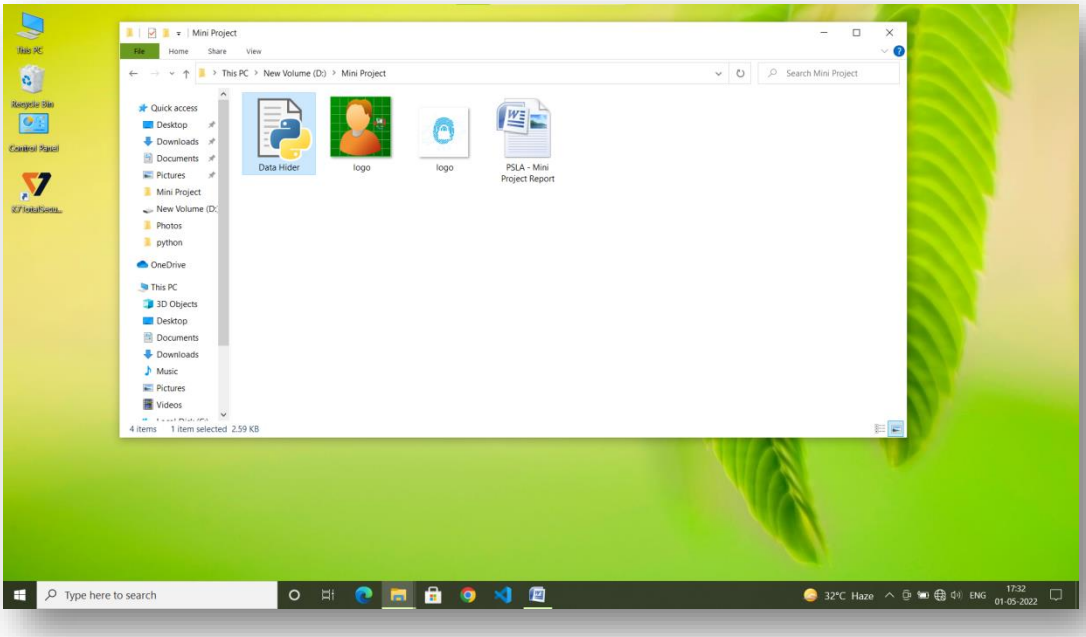

FIGURE:A.2.1 – FILE LOCATION

.

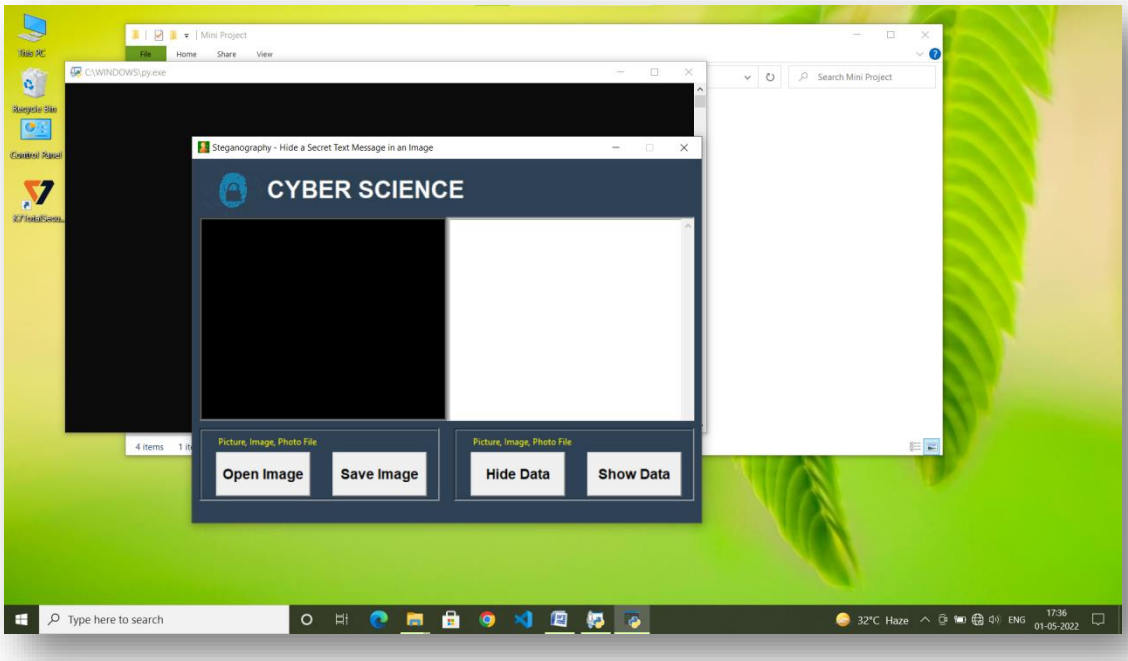

FIGURE:A.2.2 – SENDER END

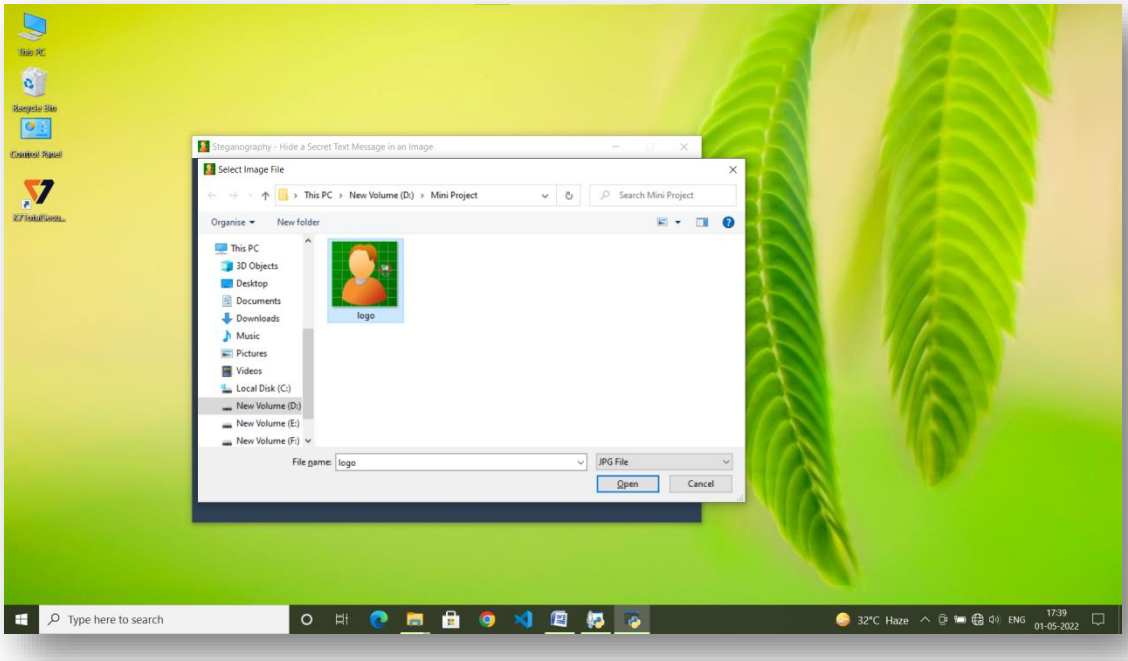

FIGURE:A.2.3 – SELECT COVER IMAGE

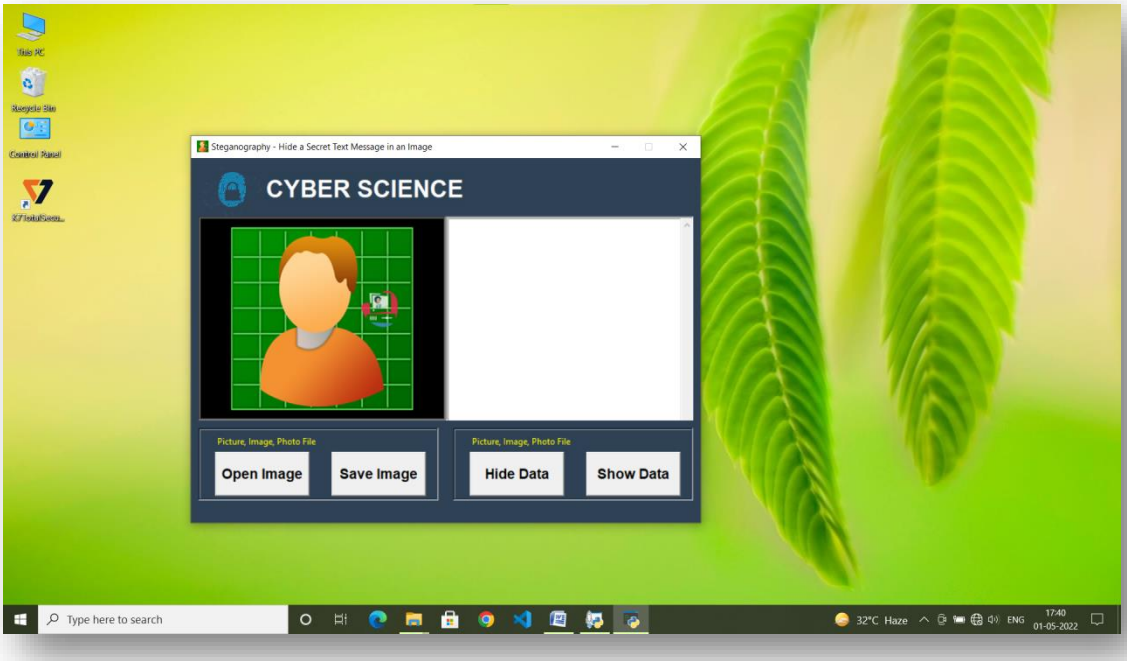

FIGURE:A.2.4- COVER IMAGE

FIGURE:A.2.5- SECRET MESSAGE

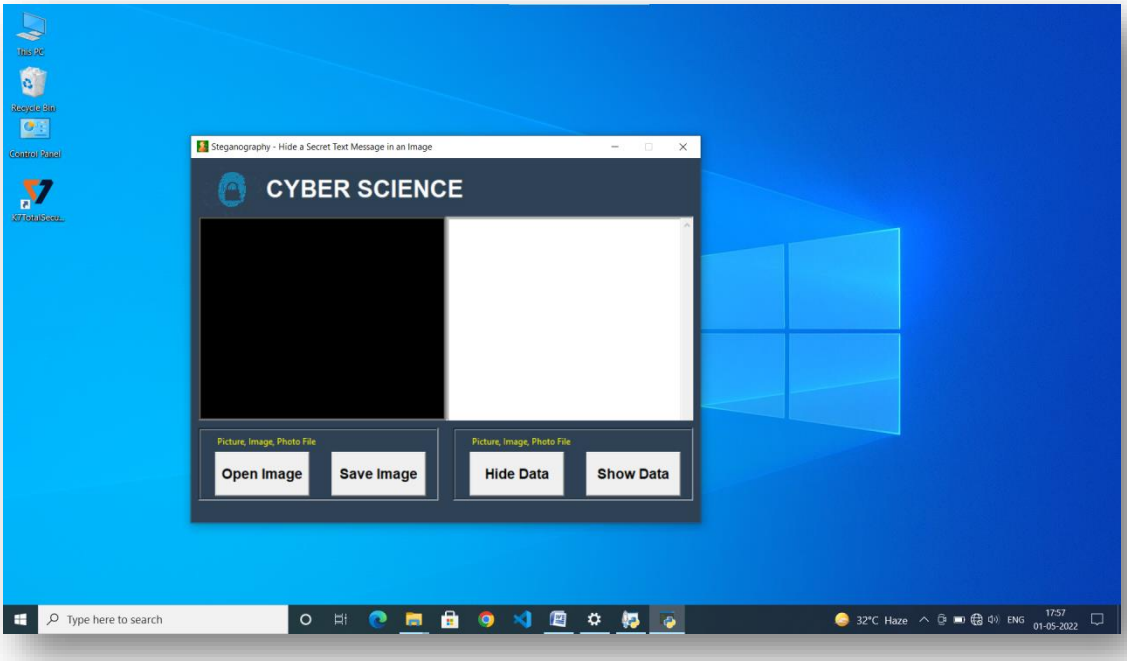

FIGURE:A.2.6 – RECEIVER END

FIGURE:A.2.7 – SELECT THE RECEIVED IMAGE

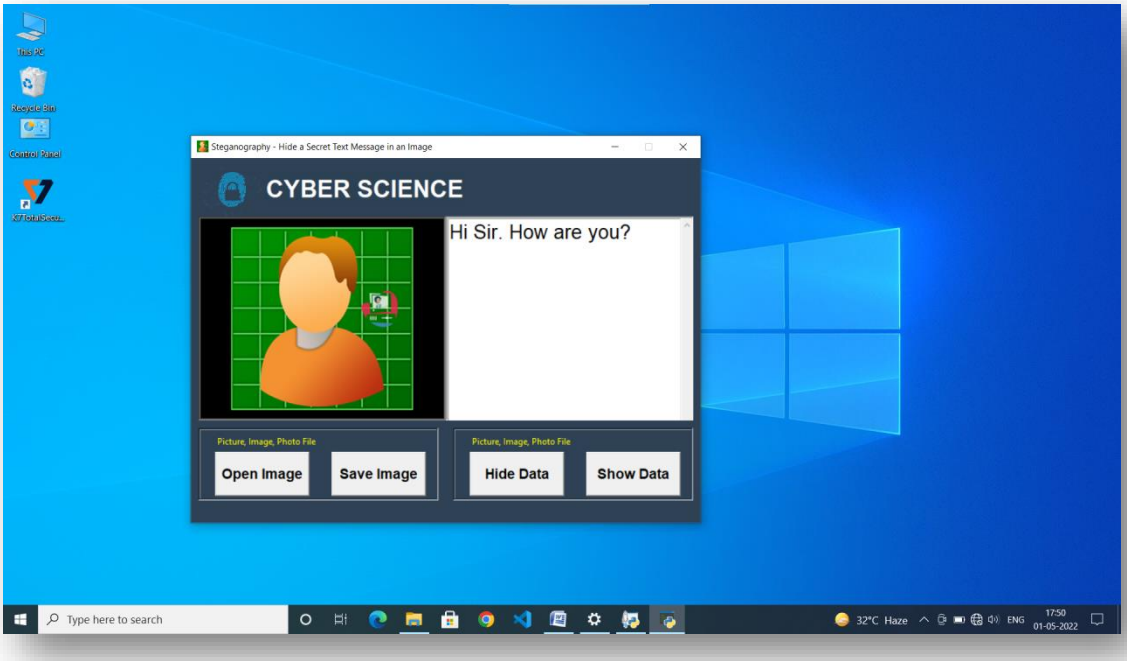

FIGURE:A.2.8 – DECRYPTION PROCESS

REFERENCES

1. WIKIPEDIA https://en.m.wikipedia.org/wiki/Steganography
2. W3Schools https://www.w3schools.com
3. Banerjee, & Indradip (2011). A survey of steganography and steganalysis technique in image, text, audio and video as cover carrier Journal of Global Research in Computer Science, 2(4), 116.
4. Bhagat, A., & Dhembhare, A. (2015). An efficient and secure data hiding techniqueSteganography. International Journal of Innovative Research in Computer and Communications Engineering, 3(2), 944-949.
5. Bhattacharyya, & Souvik (nd). ResearhGate Retrieved from ResearhGate:https://www.researchgate.net/figure/Universal-Steganalysis-method-Calibration-Base Feature-Fridrich-et-al-10 developed.
6. Bhattacharyya, S., Banerjee, I, & Sanyal, G. (2011). A Survey of steganography and steganalysis Technique in image, text, audio and video as cover carrier. Journal of Global Research in Computer Science, 2(4), 1-16.
7. Chan, C.-K. (2002). Hiding data in images by simple LSB substitution. Department of Engineering and Information Technology, City University of HongKong, https://www.kitploit.com/2018/02/1sbsteganography-python-program-to.html.