CRYPTIC CANVAS GENERATOR USING IMAGE STEGANOGRAPHY

Team Details

1. M.AkshayKumar(20EG105236)
2. B. Mahendar (20EG105254)
3. P. Maheshwari (20EG105725)

Project Supervisor

Name: Mrs. Rama Mrudula
Designation: Asst. professor

Introduction

Steganography is like a digital secret code-it hides messages within everyday things like pictures or audio files. You need two things for it to work: something to hide the message in (like a picture) and the message itself. People use it to keep messages safe when sending them online. It's like a digital spy trick! Besides keeping messages secret, it's also used to protect copyrights on pictures and for secret communication in things like spy stories. So, it's like a hidden language for the digital world.

Problem Statement

Explore hiding information in digital media through steanography focusing on image steanography and the efficient LSB algorithm. Evaluate applications across file formats, analyzing image based steanography methods with added cryptography for security.

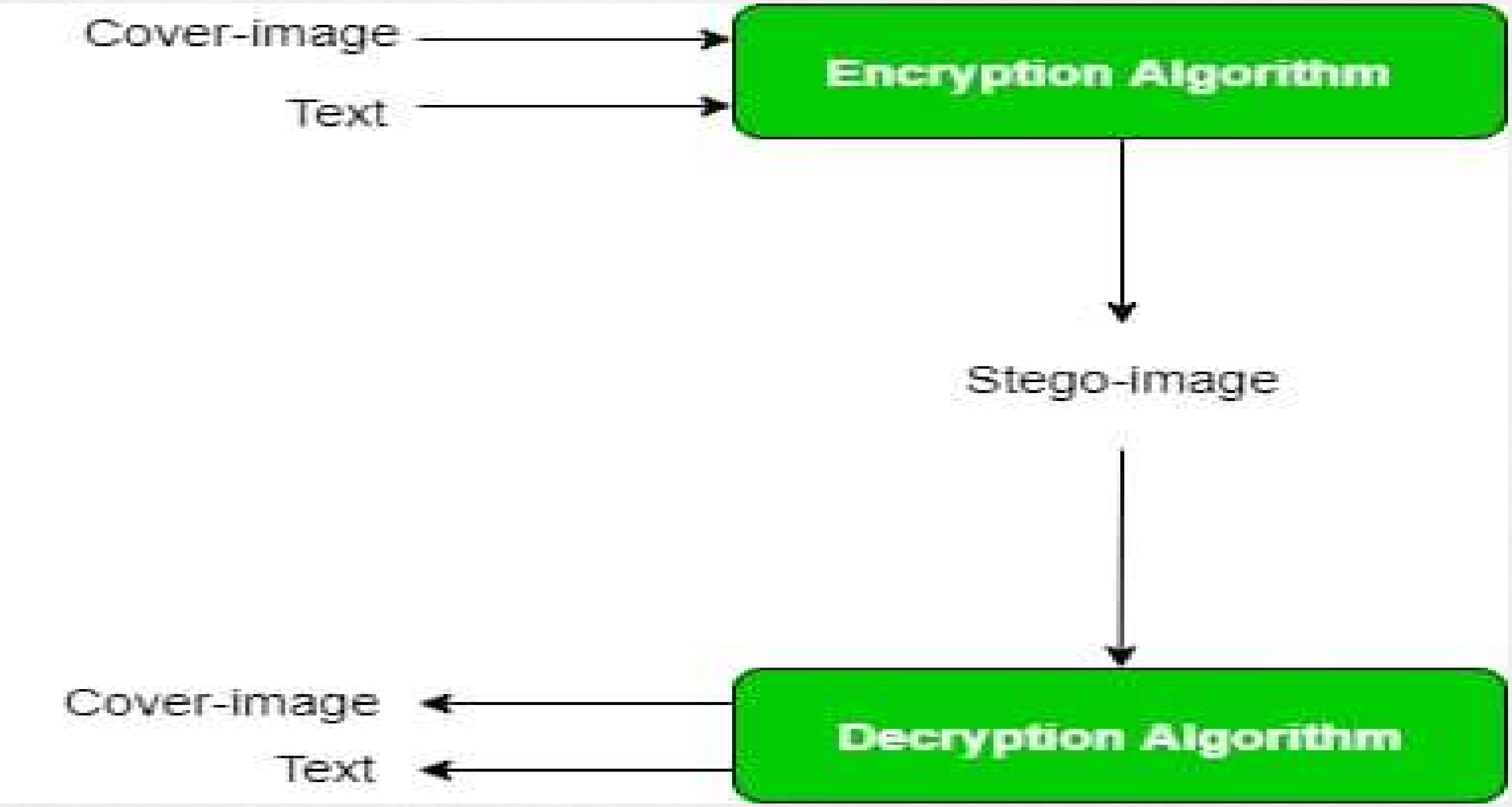
Illustrate the problem:

The aim is to address the detectability issue in steganography. We propose solving this problem by employing the method of Least Significant Bit (LSB) substitution. The key parameters to be improved include enhancing the capacity for data concealment, refining imperceptibility to minimize noticeable changes, and bolstering robustness to withstand potential detection threats. The objective is to develop a steganography technique that excels in these aspects, offering an effective and secure means of covert information transmission.

Proposed Method

- **Explanation Select Cover Image:** Begin by choosing a cover image as the carrier for the secret data. This image will be the vessel for hiding information .
- **Binary Representation:** Convert the pixel values of the cover image into their binary representations. This involves breaking down each pixel's color information into its constituent binary bits.
- **Secret Data Embedding:** Apply the Least Significant Bit (LSB) substitution technique. Replace the least significant bits of selected pixels with the bits of the secret data. This ensures minimal impact on the overall appearance of the cover image.
- **Imperceptibility Enhancement:** To improve imperceptibility, consider applying algorithms or methods that reduce the visual impact of changes introduced during the embedding process.
- **Testing and Validation:** Evaluate the steganographic method through testing to ensure that the embedded data is successfully concealed, the cover image retains its original appearance, and the method withstands various detection attempts.

Proposed Method



Cover-image

Text

Encryption Algorithm

Stego-image

Decryption Algorithm

Cover-image

Text

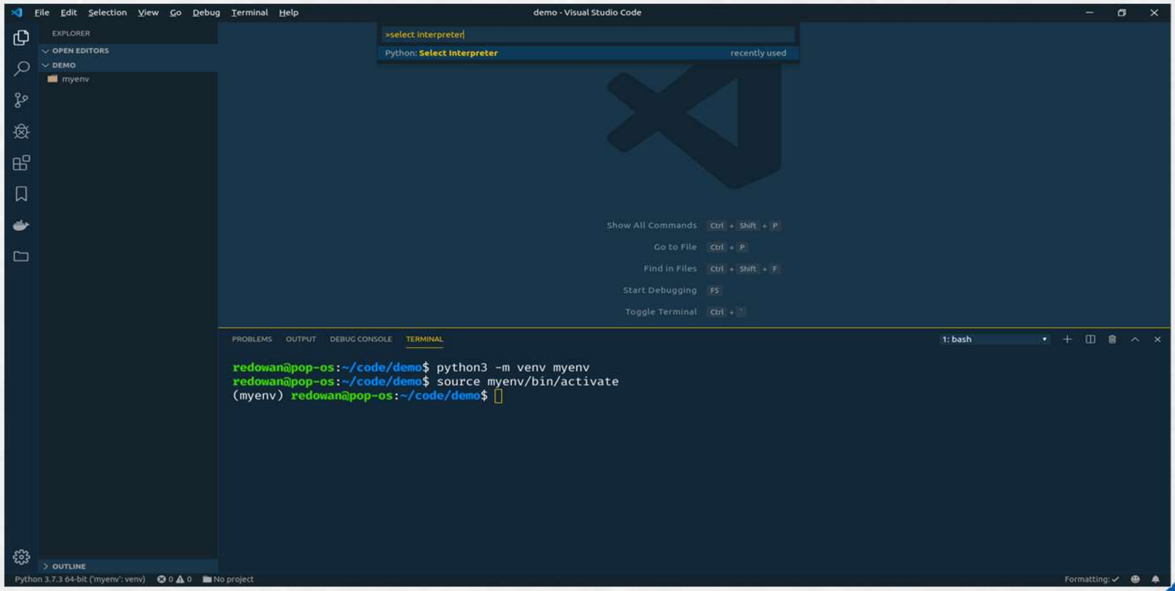
Proposed Method

Illustration :

In an era of heightened digital threats, ensuring the secure transmission of sensitive information has become paramount. Image steganography, a technique used to conceal data within images, offers a promising solution to this challenge. This study aims to evaluate the effectiveness of image steganography techniques, specifically focusing on Least Significant Bit (LSB) and Advanced Encryption Standard (AES), in achieving secure data concealment. By assessing the capabilities of these techniques, the research seeks to minimize detection risks while enhancing data protection in digital channels. Through rigorous analysis and experimentation, the study endeavors to contribute to the development of robust methodologies for safeguarding sensitive information in the digital age.

Experiment Environment

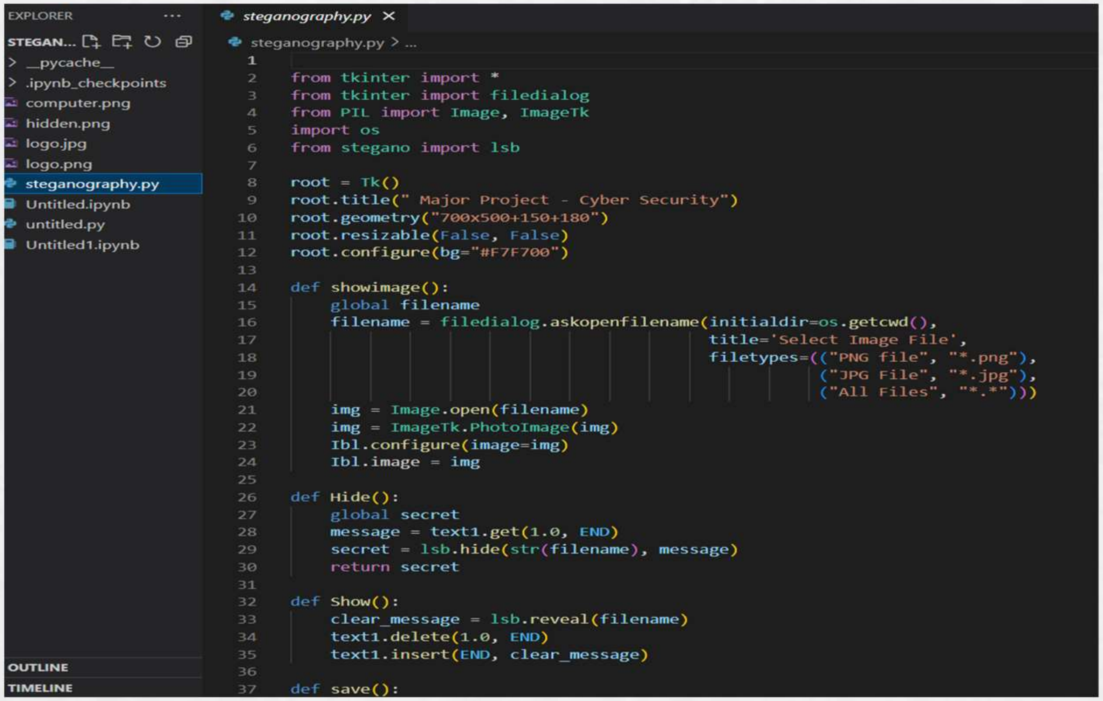
vscode


File Edit Selection View Go Debug Terminal Help
demo - Visual Studio Code
EXPLORER
OPEN EDITORS
DEMO
myenv
Show All Commands Ctrl + Shift + P
Go to File Ctrl + P
Find in Files Ctrl + Shift + F
Start Debugging F5
Toggle Terminal Ctrl + `
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL
1: bash
OUTLINE
Python 3.7.3 64-bit ('myenv': venv) ⊗ 0 ⚠ 0 No project
Formatting: ✓

```
>select interpreter
Python: Select Interpreter                                   recently used
```

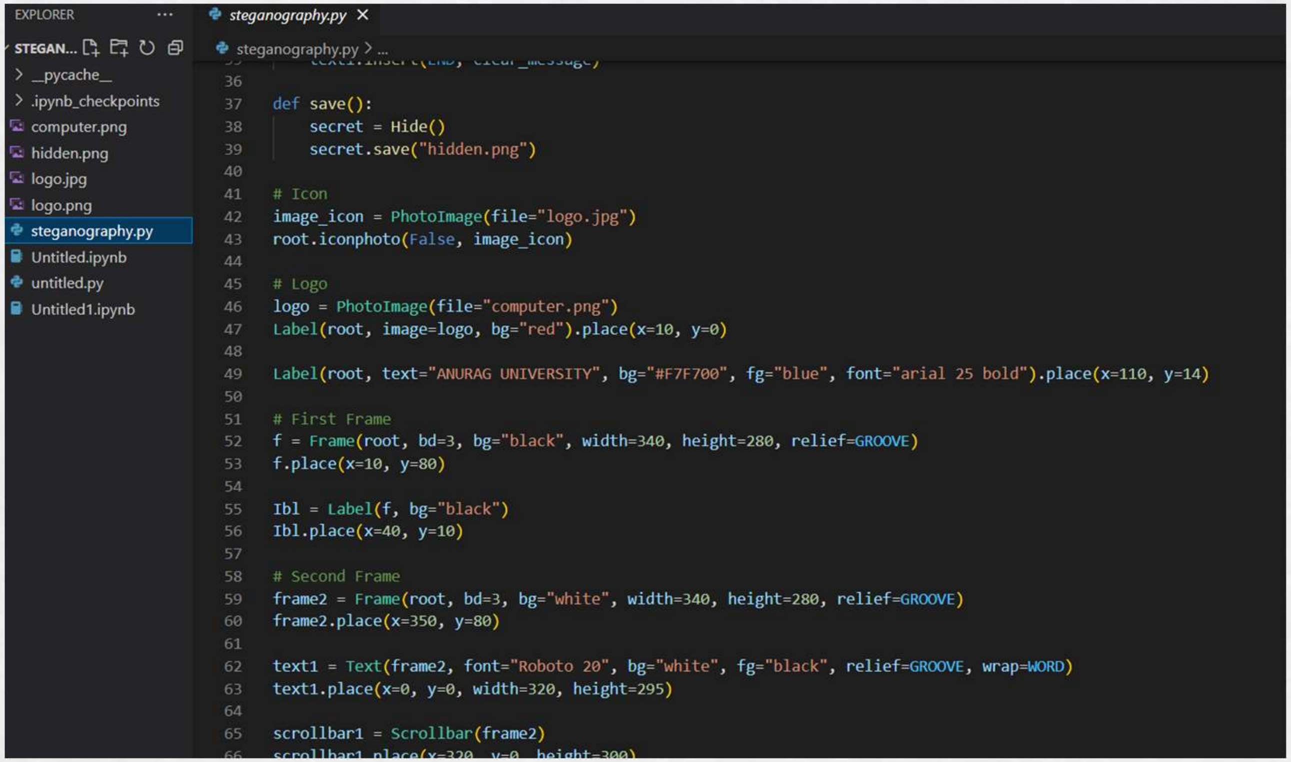
```
redowan@pop-os:~/code/demo$ python3 -m venv myenv
redowan@pop-os:~/code/demo$ source myenv/bin/activate
(myenv) redowan@pop-os:~/code/demo$ 
```

Experiment Screen shorts



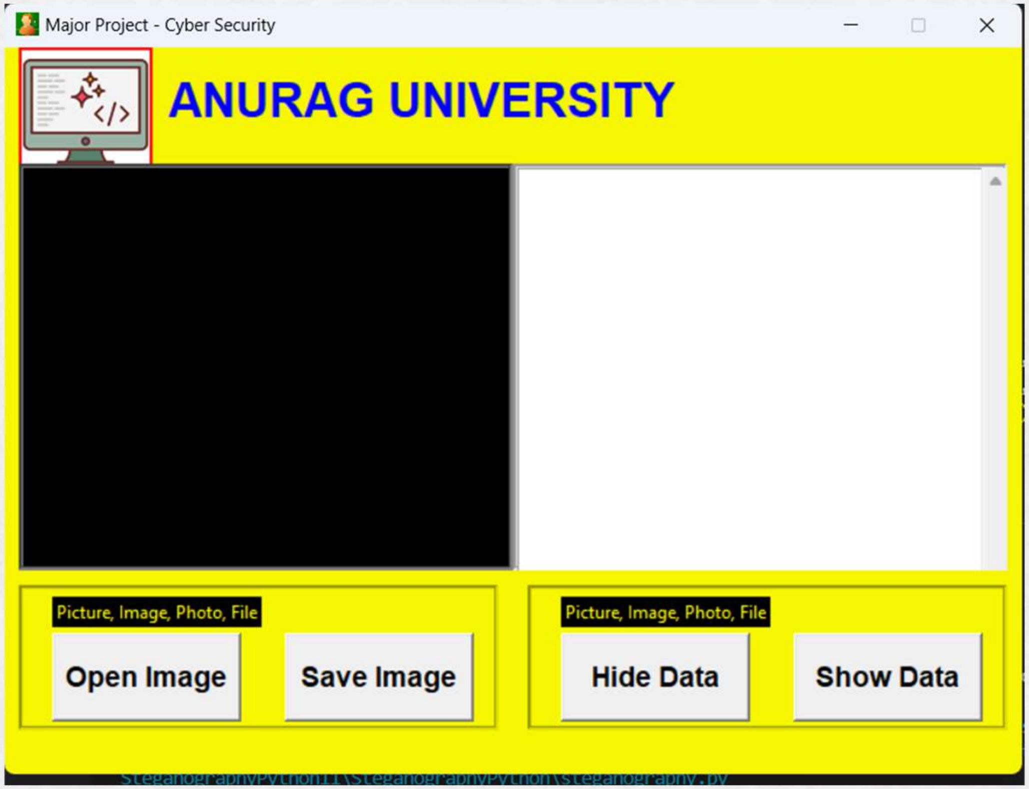
```python

from tkinter import *
from tkinter import filedialog
from PIL import Image, ImageTk
import os
from stegano import lsb

root = Tk()
root.title(" Major Project - Cyber Security")
root.geometry("700x500+150+180")
root.resizable(False, False)
root.configure(bg="#F7F700")

def showimage():
    global filename
    filename = filedialog.askopenfilename(initialdir=os.getcwd(),
                                          title='Select Image File',
                                          filetypes=(("PNG file", "*.png"),
                                                     ("JPG File", "*.jpg"),
                                                     ("All Files", "*.*")))
    img = Image.open(filename)
    img = ImageTk.PhotoImage(img)
    Ibl.configure(image=img)
    Ibl.image = img

def Hide():
    global secret
    message = text1.get(1.0, END)
    secret = lsb.hide(str(filename), message)
    return secret

def Show():
    clear_message = lsb.reveal(filename)
    text1.delete(1.0, END)
    text1.insert(END, clear_message)

def save():
```

Experiment Screen shorts



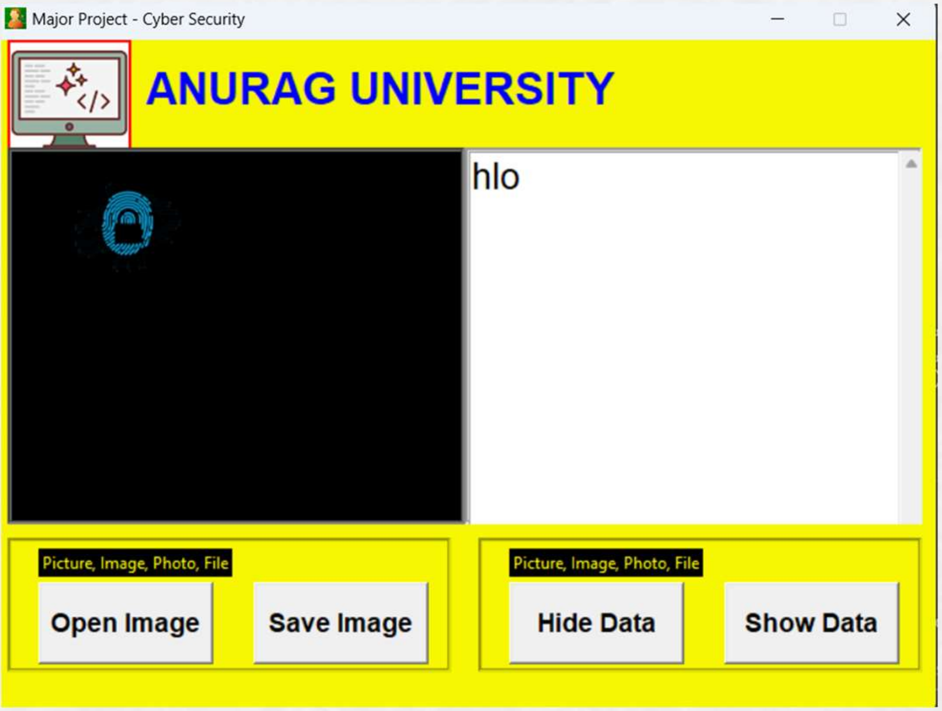
```python
    text1.insert(END, clear_message)

def save():
    secret = Hide()
    secret.save("hidden.png")

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

# Logo
logo = PhotoImage(file="computer.png")
Label(root, image=logo, bg="red").place(x=10, y=0)

Label(root, text="ANURAG UNIVERSITY", bg="#F7F700", fg="blue", font="arial 25 bold").place(x=110, y=14)

# First Frame
f = Frame(root, bd=3, bg="black", width=340, height=280, relief=GROOVE)
f.place(x=10, y=80)

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

# Second Frame
frame2 = Frame(root, bd=3, bg="white", width=340, height=280, relief=GROOVE)
frame2.place(x=350, y=80)

text1 = Text(frame2, font="Roboto 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)
```

Experiment Results


Major Project - Cyber Security
ANURAG UNIVERSITY
Picture, Image, Photo, File
Open Image
Save Image
Picture, Image, Photo, File
Hide Data
Show Data

SteganographyPython11\SteganographyPython\steganography.py

Experiment Results



Major Project - Cyber Security
ANURAG UNIVERSITY
Picture, Image, Photo, File
Open Image
Save Image
Picture, Image, Photo, File
Hide Data
Show Data

hlo

Finding

original

embedded

Justification

1.What are parameters improved by your method

Improved user experience and error handling through input validation, feedback mechanisms, and responsiveness optimization. Enhanced security awareness and guidance provided to users, along with performance optimization for efficient image processing.

2.Mathametic formulas for calculating parameter values

Peak Signal-to-Noise Ratio (PSNR):

$$PSNR = 10\log_{10}\frac{256^2}{MSE}$$

3.why your parameter values improved?

The parameter values improved in this project by enhancing user experience, security, and performance through robust input validation, optimized responsiveness, and heightened security awareness.