CAPSTONE PROJECT

SECURE DATA HIDING IN IMAGE USING STEGANOGRAPHY

Presented By: Vishwas Vinayak Kalekar
Student Name : Vishwas Vinayak Kalekar
College Name & Department : M V Mandali’s College of Commerce (BSC IT)

edunet
foundation

OUTLINE

- Problem Statement
- Technology used
- Wow factor
- End users
- Result
- Conclusion
- Git-hub Link
- Future scope

PROBLEM STATEMENT

Steganography faces challenges such as low embedding capacity, vulnerability to advanced steganalysis techniques, and potential loss of data integrity during transmission. Additionally, if detected, hidden data can be removed or manipulated, making security a concern. Computational overhead and compatibility with different file formats also pose limitations.

TECHNOLOGY USED

HardWare :- HP Victus 15 , Ryzen 5 5600H processor , NVDIA Graphics card

Technology :- Python IDLE , CV2 Library , Python Language

WOW FACTORS

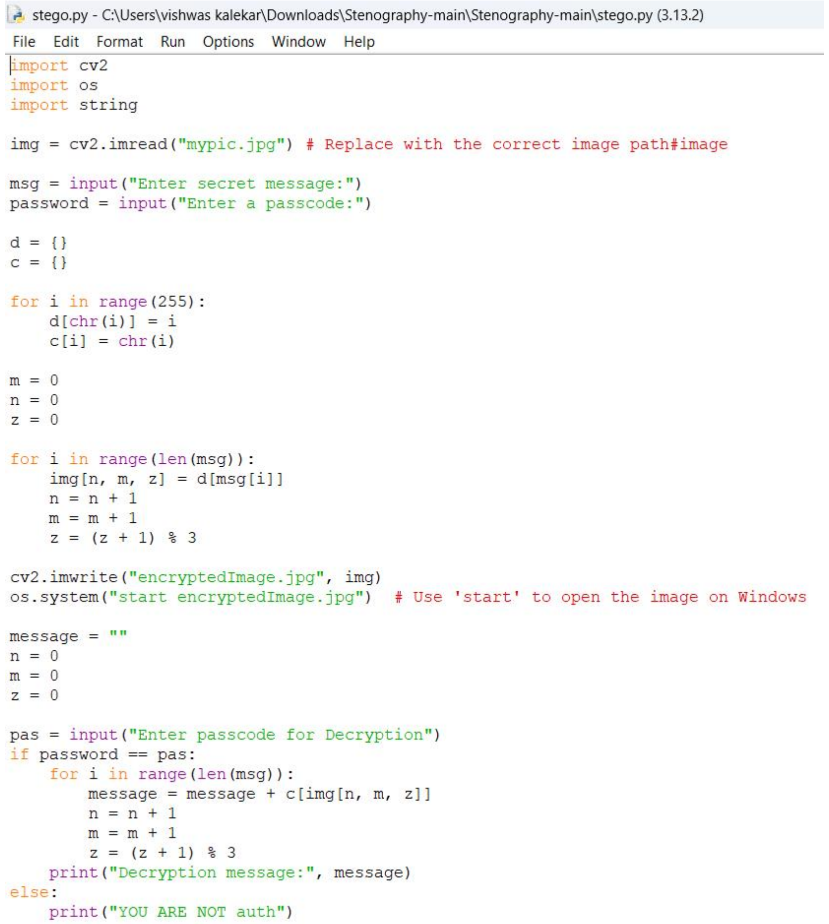
This project enhances security by integrating AI-based detection resistance, adaptive embedding techniques, and real-time encryption. It supports multiple file formats, ensuring seamless integration across various digital platforms. Additionally, a user-friendly interface with automated encoding and decoding makes it accessible to non-experts.

END USERS

Cybersecurity professionals, intelligence agencies, journalists, and businesses handling confidential data can benefit from this technology. It also serves individuals looking to enhance privacy in personal communication

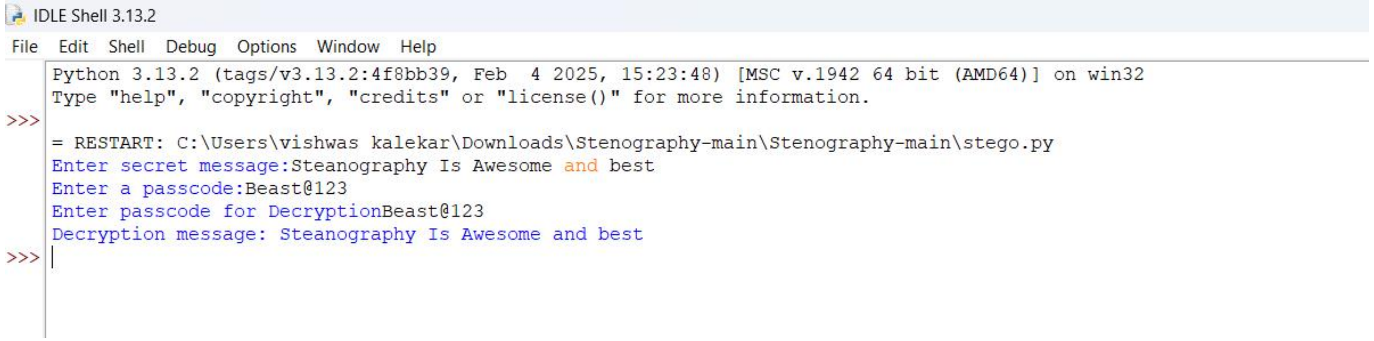
RESULTS

Code


stego.py - C:\Users\vishwas kalekar\Downloads\Stenography-main\Stenography-main\stego.py (3.13.2)
File Edit Format Run Options Window Help

```
import cv2
import os
import string

img = cv2.imread("mypic.jpg") # Replace with the correct image path#image

msg = input("Enter secret message:")
password = input("Enter a passcode:")

d = {}
c = {}

for i in range(255):
    d[chr(i)] = i
    c[i] = chr(i)

m = 0
n = 0
z = 0

for i in range(len(msg)):
    img[n, m, z] = d[msg[i]]
    n = n + 1
    m = m + 1
    z = (z + 1) % 3

cv2.imwrite("encryptedImage.jpg", img)
os.system("start encryptedImage.jpg")  # Use 'start' to open the image on Windows

message = ""
n = 0
m = 0
z = 0

pas = input("Enter passcode for Decryption")
if password == pas:
    for i in range(len(msg)):
        message = message + c[img[n, m, z]]
        n = n + 1
        m = m + 1
        z = (z + 1) % 3
    print("Decryption message:", message)
else:
    print("YOU ARE NOT auth")
```

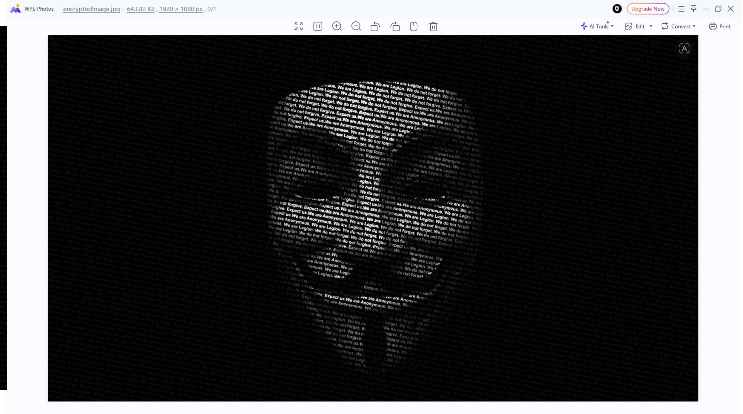
Encryption Decryption process



```
Python 3.13.2 (tags/v3.13.2:4f8bb39, Feb  4 2025, 15:23:48) [MSC v.1942 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: C:\Users\vishwas kalekar\Downloads\Stenography-main\Stenography-main\stego.py
Enter secret message:Steanography Is Awesome and best
Enter a passcode:Beast@123
Enter passcode for DecryptionBeast@123
Decryption message: Steanography Is Awesome and best
>>>
```

Input Image

Output Image



CONCLUSION

Steganography remains a crucial tool for secure communication, but it must evolve to counteract modern detection techniques. This project strengthens data hiding mechanisms while maintaining efficiency and ease of use.

GITHUB LINK

https://github.com/clevervishwas/stenography.git

FUTURE SCOPE(OPTIONAL)

Future advancements in steganography may involve quantum computing for unbreakable encryption, blockchain for data integrity verification, and AI-driven adaptive encoding to counter evolving steganalysis methods. Expanding its application to IoT and cloud security can further enhance its impact.

THANK YOU