CAPSTONE PROJECT

SECURE DATA HIDING IN IMAGES USING STEGANOGRAPHY

Presented By:
Student Name : Minnu Krishna A
College Name & Department : SCTCE, ECE

OUTLINE

- **Problem Statement**

- **Technology used**

- **Wow factor**

- **End users**

- **Result**

- **Conclusion**

- **Git-hub Link**

- **Future scope**

PROBLEM STATEMENT

The growing need for secure communication has made data privacy a critical concern. Steganography, which hides secret data within digital images, offers a potential solution. However, existing methods often struggle with balancing data security, image quality, and resistance to attacks like compression or manipulation.

This project aims to develop a secure and robust steganographic technique that ensures data confidentiality while maintaining high image quality and resistance to steganalysis.

TECHNOLOGY USED

CV2 Library
OS Library
String Library
IDLE (Python 3.13 64-bit)
Github

WOW FACTORS

This project combines advanced steganography and encryption techniques to provide a highly secure method for hiding sensitive data in images. It ensures both high data capacity and excellent image quality, making hidden information virtually undetectable. By integrating anti-forensic measures, the system resists various image manipulations and attacks, offering robust security for digital communication. The ability to securely transmit confidential data without compromising user experience sets this project apart.

END USERS

- **Individuals** who require privacy for personal communication and want to securely transmit sensitive information without detection.

- **Corporate organizations** needing to protect confidential business data during transmission, such as intellectual property or proprietary information.

- **Government agencies** and **military personnel** that require secure channels for confidential communication and to safeguard national security data.

- **Cybersecurity professionals** who can implement steganographic techniques for secure file sharing and to enhance data protection strategies.

- **Journalists and activists** in sensitive environments where secure, anonymous communication is critical for protecting sources and information from surveillance or censorship.

edu**net**
foundation

RESULTS- Encryption Code

Code->

```python
import cv2
import os
import string

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

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")
```
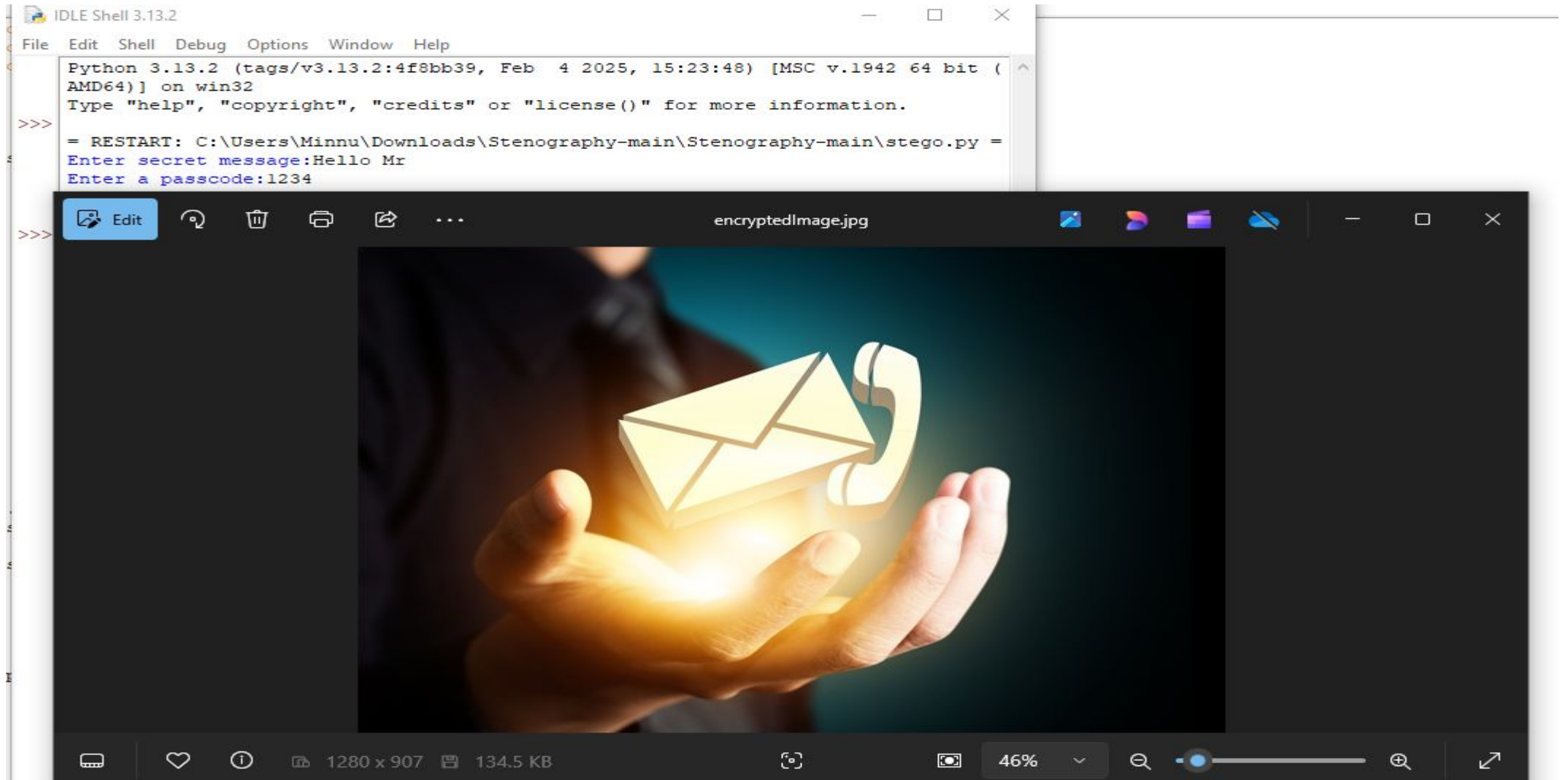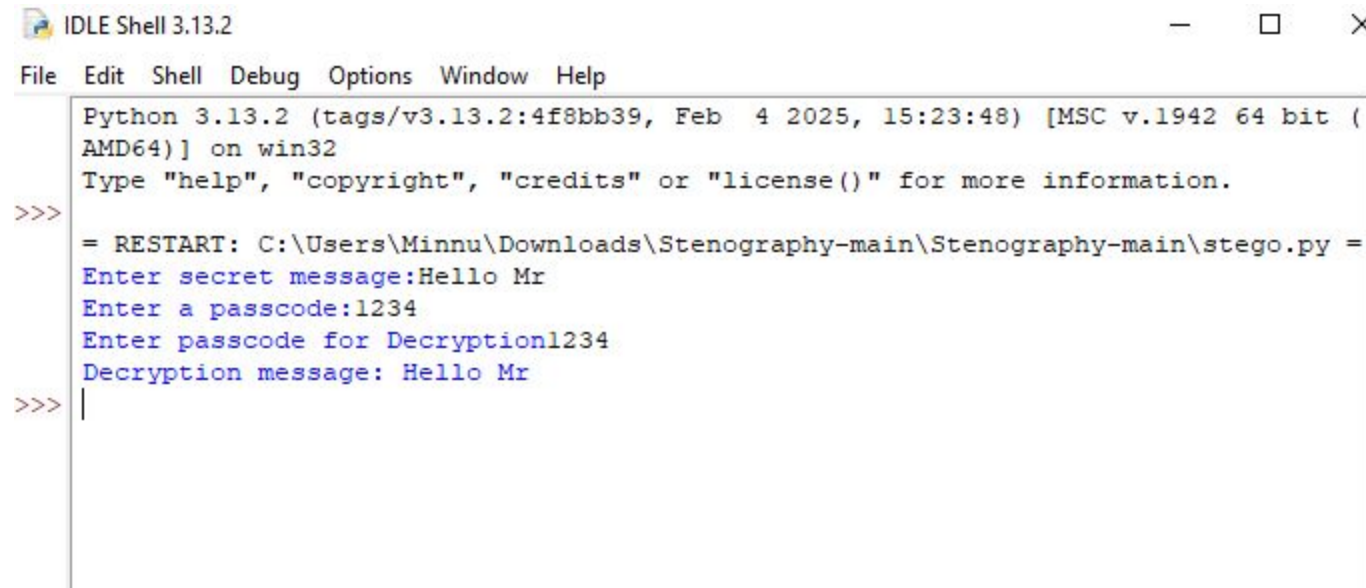
RESULTS- Encryption Output

Output->

RESULTS- Decryption

Output

CONCLUSION

■ In conclusion, the "Secure Data Hiding in Images Using Steganography" project successfully provides a robust solution for concealing sensitive information within digital images. By combining advanced steganographic techniques with encryption, the system ensures high data security, undetectability, and resistance to common attacks, such as image manipulation or compression. This approach offers a practical and efficient method for secure data transmission, making it ideal for individuals, organizations, and agencies seeking to protect confidential information in a digital environment.

GITHUB LINK

https://github.com/MINSU-TECH/MY-PROJECT-AICTE-EDUNET.git

FUTURE SCOPE

The future scope of the "Secure Data Hiding in Images Using Steganography" project includes enhancing the algorithm's efficiency for larger data payloads while maintaining image quality. Additionally, integrating machine learning techniques to improve resistance to advanced steganalysis and attacks, such as deep learning-based image processing, could further strengthen security. Exploring multi-layered encryption and cross-media steganography (e.g., audio, video) offers potential for broader applications in secure communications across diverse platforms.

THANK YOU