CAPSTONE PROJECT

SECURE DATA HIDING IN IMAGE USING STEGANOGRAPHY

Presented By: Edunet IBM Skill Build (AICTE)
Student Name : Pavan Manepalli
College Name & Department : MVGR College (CSM)

edunet
foundation

OUTLINE

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

PROBLEM STATEMENT

With the rise of cyber threats, securing sensitive information is crucial. Traditional encryption methods can attract attackers' attention. Steganography offers a way to conceal data within images, making it nearly undetectable. This project implements secure data hiding techniques to enhance information security.

TECHNOLOGY USED

Programming Language: Python

Libraries: OpenCV, NumPy, PIL (Pillow)

Concepts: LSB (Least Significant Bit) Steganography

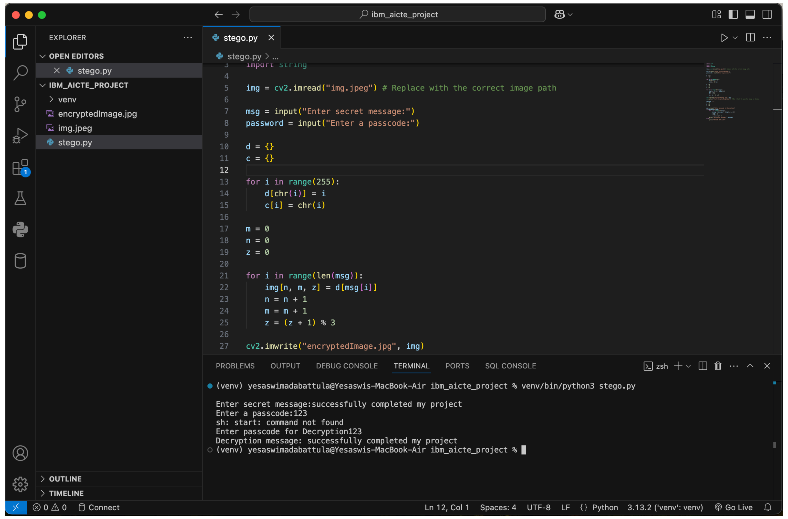
WOW FACTORS

- Invisible data hiding without altering the image quality significantly.
- Efficient extraction of hidden data using minimal computational resources.
- Enhanced security by applying additional encryption techniques before hiding data.

END USERS

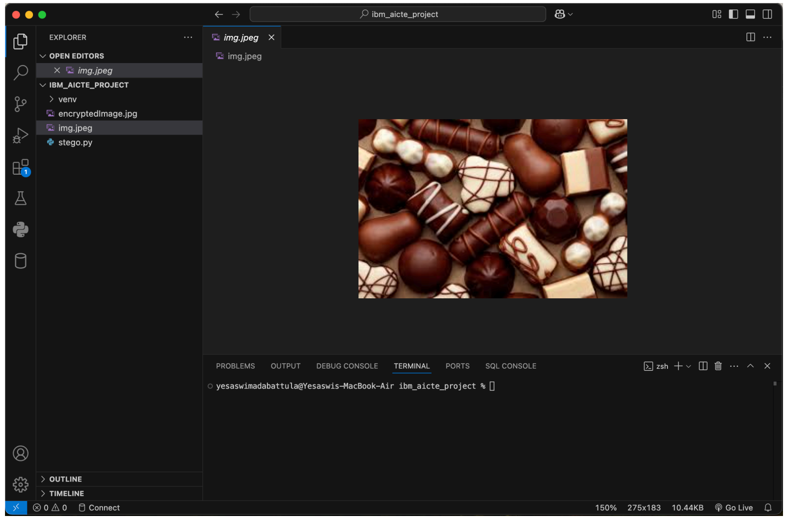
- Government agencies for secure communication.
- Journalists and whistleblowers for confidential information transfer.
- Corporate sectors for data protection

RESULTS

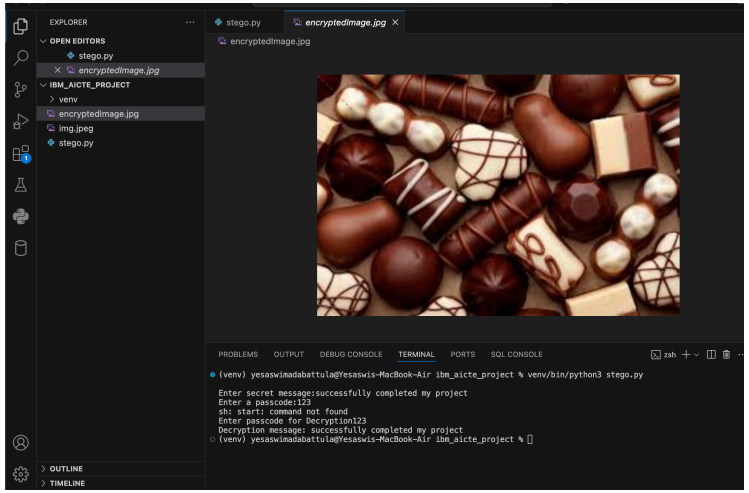


```python
import string

img = cv2.imread("img.jpeg") # 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)
```

```
(venv) yesaswimadabattula@Yesaswis-MacBook-Air ibm_aicte_project % venv/bin/python3 stego.py

Enter secret message:successfully completed my project
Enter a passcode:123
sh: start: command not found
Enter passcode for Decryption123
Decryption message: successfully completed my project
(venv) yesaswimadabattula@Yesaswis-MacBook-Air ibm_aicte_project %
```



```
yesaswimadabattula@Yesaswis-MacBook-Air ibm_aicte_project %
```



```
(venv) yesaswimadabattula@Yesaswis-MacBook-Air ibm_aicte_project % venv/bin/python3 stego.py

Enter secret message:successfully completed my project
Enter a passcode:123
sh: start: command not found
Enter passcode for Decryption123
Decryption message: successfully completed my project
(venv) yesaswimadabattula@Yesaswis-MacBook-Air ibm_aicte_project %
```

CONCLUSION

This project successfully demonstrates the application of steganography for secure data transmission. By embedding sensitive information into images, it provides an additional security layer without raising suspicion.

GITHUB LINK

- https://github.com/pavan-0615/IBM_AICTE_CYBER.git

FUTURE SCOPE(OPTIONAL)

Implementing AI-driven steganography for dynamic data embedding.
Extending to video steganography for larger data concealment.
Enhancing security with advanced cryptographic techniques before hiding data.

THANK YOU

edunet
foundation