

---

# **CAPSTONE PROJECT**

## **SECURE DATA HIDING IN IMAGE USING STEGANOGRAPHY**

**Presented By: Edunet IBM Skill Build (AICTE)**  
**Student Name : Yesaswi Madabattula**  
**College Name & Department : MVGR College (CSM)**

# 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

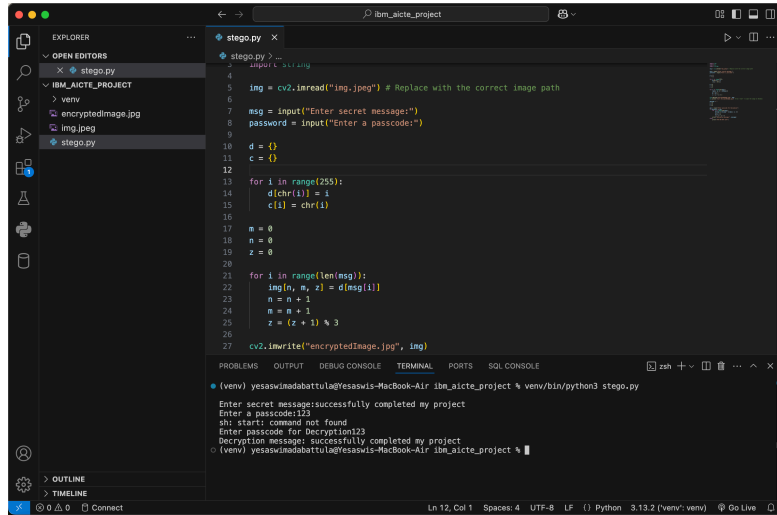
- Invisible data hiding without altering the image quality significantly.
- Efficient extraction of hidden data using minimal computational resources.
- Enhanced security by applying additional encryption techniques before hiding data.

---

## END USERS

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

# RESULTS

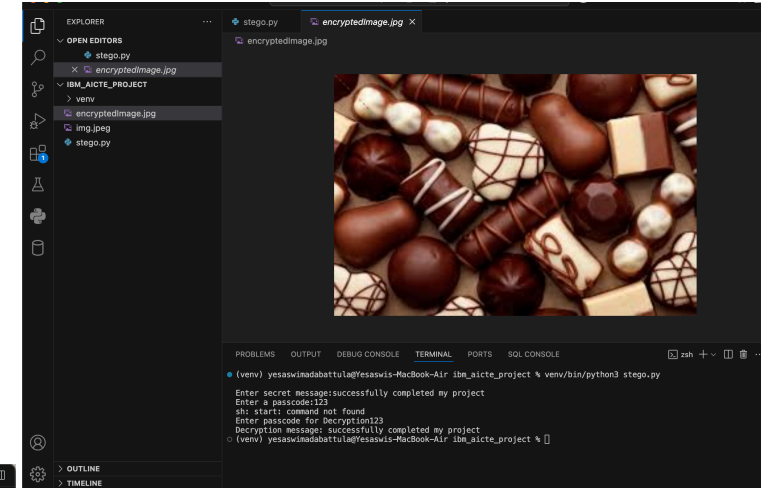
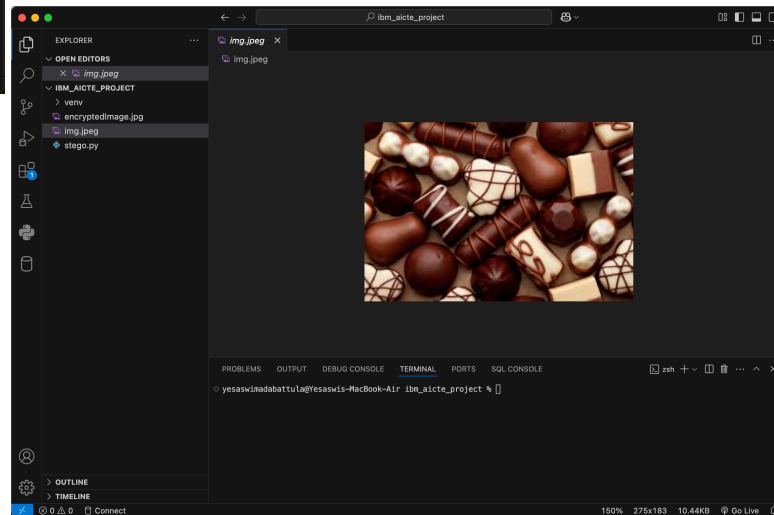


The screenshot shows the VS Code editor with the `stego.py` file open. The script uses `cv2.imread` to load an image, takes user input for a secret message and password, and then performs XOR encryption on the image data. The terminal output shows the script being executed, the secret message "successfully completed my project" being entered, and the password "123" being entered for decryption.

```
1 import cv2
2
3
4
5 img = cv2.imread("img.jpg") # Replace with the correct image path
6
7 msg = input("Enter secret message:")
8 password = input("Enter a password:")
9
10 d = 0
11 e = 0
12
13 for i in range(255):
14     d = chr(i)
15     c[i] = chr(i)
16
17 n = 0
18 m = 0
19 z = 0
20
21 for i in range(len(msg)):
22     img[n, m, 2] = d[msg[i]]
23     n = n + 1
24     m = m + 1
25     z = (z + 1) % 3
26
27 cv2.imwrite("encryptedImage.jpg", img)
```

Terminal Output:

```
(venv) yesaswinadabattula@yesaswis-MacBook-Air ibm_aicte_project % venv/bin/python3 stego.py
Enter secret message:successfully completed my project
Enter a password:123
sh: start: command not found
Enter password for Decryption:123
Decryption message: successfully completed my project
(venv) yesaswinadabattula@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/Yesaswi33/IBM\\_AICTE\\_CS\\_Project.git](https://github.com/Yesaswi33/IBM_AICTE_CS_Project.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**