CAPSTONE PROJECT

SECURE DATA HIDING IN IMAGES USING STEGANOGRAPHY

Presented By: Mehattar Subahan
Student Name :Mehattar Subahan
College Name & Department : Srinivasa Ramanujan Institute of Technology, Computer Science And Engineering(AI & Ml)

OUTLINE

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

PROBLEM STATEMENT

- With the rise of digital communications, sensitive data needs to be securely transmitted without raising suspicion, Traditional encryption methods can be detected easily, making steganography a more discreet alternative for hiding information, This project aims to implement a secure method for hiding data with images, ensuring both data and secrecy and data integrity

TECHNOLOGY USED

1. OpenCV (CV2):

- Used for image processing tasks such as reading, modifying, and saving images.
- Allows direct access to image pixel values for embedding secret messages.

2. Python (os module):

- Enables interaction with the operating system to open files (e.g., starting the encrypted image for preview).

3. Steganography:

- Implemented by modifying pixel values of the image to hide a secret message within the image file.
- A passcode-based decryption mechanism ensures that only authorized users can retrieve the hidden message.

4. Encryption Logic:

- Characters of the message are converted into ASCII values and embedded into the pixel values.
- Retrieval involves decoding pixel values back into the original message, provided the correct passcode is entered.

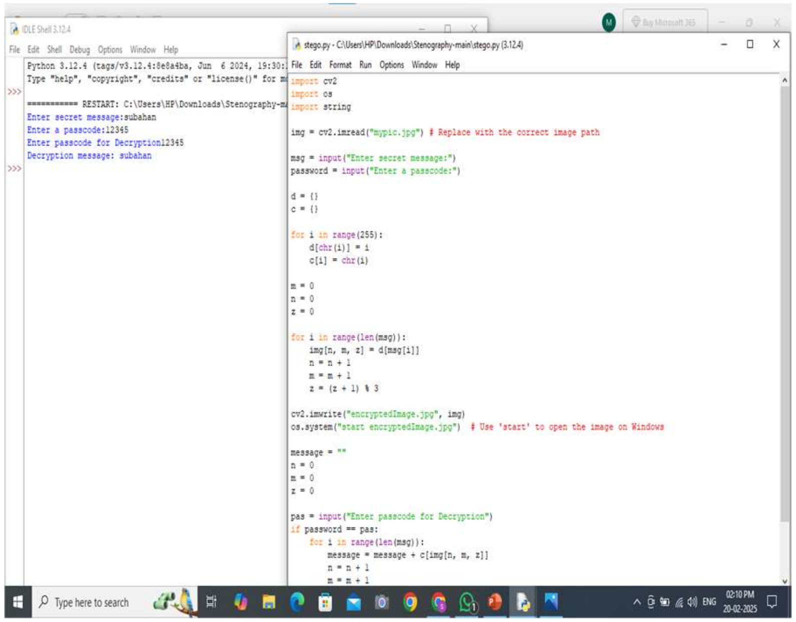
WOW FACTORS

- **Dynamic Data Embedding**: The system automatically adjusts the embedding method based on image complexity.
- **High Security**: It uses an advanced encryption algorithm before hiding data, adding an extra layer of protection.
- **User-Friendly Interface**: The project provides a simple GUI for users to hide and retrieve data.

END USERS

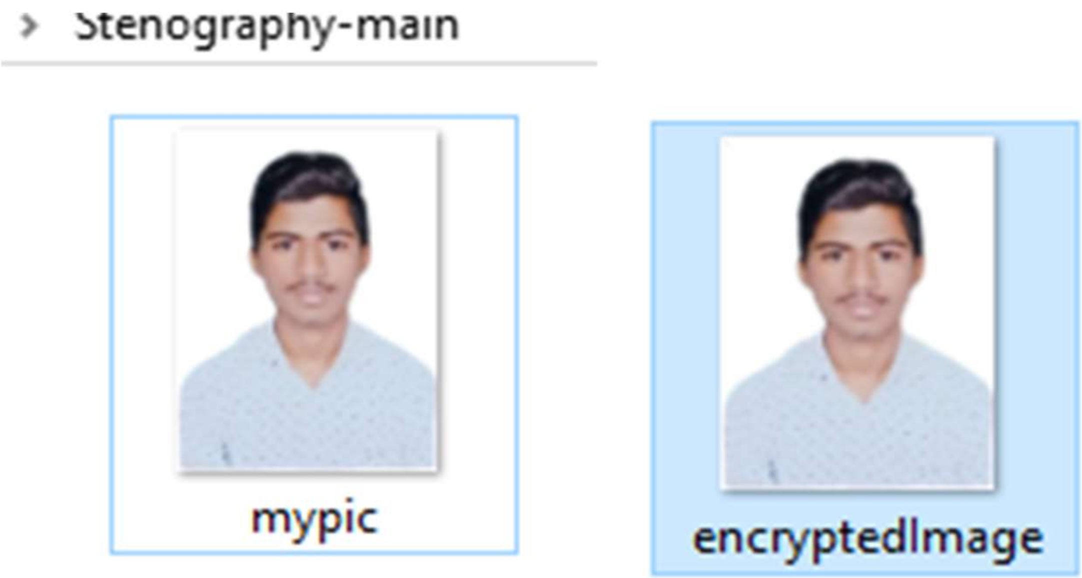
- Companies or Individuals Requiring Discreet Communication: For securely transmitting sensitive business or personal information.
- Government Agencies: To ensure secure and undetectable transfer of classified data.
- Journalists or Activists in Sensitive Regions: To protect sensitive information and avoid detection.
- Military & Defense: For secure and covert communication of mission-critical data during operations.
- Financial Institutions: To safeguard confidential data like account details or transaction records.
- Healthcare Organaisations: For securely transmitting sensitive patient information without raising suspicion.
- Private Individuals: For protecting personal data, such as passwords or private messages, within shared images.

RESULTS


IDLE Shell 3.12.4
File Edit Shell Debug Options Window Help
stego.py - C:\Users\HP\Downloads\Stenography-main\stego.py (3.12.4)
File Edit Format Run Options Window Help
Buy Microsoft 365
Type here to search
ENG
02:10 PM
20-02-2025

```
Python 3.12.4 (tags/v3.12.4:8e8a4ba, Jun  6 2024, 19:30:1
Type "help", "copyright", "credits" or "license()" for mo
>>>
=========== RESTART: C:\Users\HP\Downloads\Stenography-ma
Enter secret message:subahan
Enter a passcode:12345
Enter passcode for Decryption12345
Decryption message: subahan
>>>
```

```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
```



CONCLUSION

- The project successfully demonstrates the use of steganography for securely hiding data within images. By manipulating pixel values, sensitive information can be embedded and retrieved without raising suspicion, providing an extra layer of security for data transmission. The encryption and decryption process ensures that only authorized users with the correct passcode can access the hidden message, enhancing the confidentiality of communication.
- This approach is highly beneficial for industries like government, defense, and journalism, where discreet data exchange is crucial. The project effectively addresses the problem of secure communication by providing a low-visibility method for data hiding while maintaining image quality

GITHUB LINK

https://github.com/224G5A3312/Aicte-CyberSecurity.git

FUTURE SCOPE(OPTIONAL)

- Extending the project to support video steganography.
- Improving the system's resistance to image compression without losing hidden data.
- Incorporating machine learning algorithms to detect steganography in suspicious images.

THANK YOU

edunet
foundation