CAPSTONE PROJECT

SECURE DATA HIDING IN IMAGES USING STEGANOGRAPHY

Presented By:M Venkata Chandra Sena Reddy

Student Name : M Venkata Chandra Sena Reddy

College Name : BHARATH INSTITUTE OF HIGHER EDUCATION AND RESEARCH

Department : B.TECH CSE-IBM

OUTLINE

- **Problem Statement**

- **Technology used**

- **Wow factor**

- **End users**

- **Result**

- **Conclusion**

- **Git-hub Link**

- **Future scope**

edunet
foundation

PROBLEM STATEMENT

- Ensuring data security while maintaining the integrity of the cover image.

- Making encryption and decryption accessible to non-technical users through a simple interface.

- Traditional encryption methods are easily detectable and can raise suspicion.

- Need for a secure way to hide confidential messages within images.

edunet
foundation

TECHNOLOGY USED

- **Programming Language**: Python3

- **Image Processing Library**: OpenCV

- **File Handling & Security**: Basic encryption logic for password protection

- **Platform**: Linux

edunet
foundation

WOW FACTORS

- Uses steganography to embed a message into an image without noticeable changes.

- User-friendly GUI for easy encryption and decryption.

- Lossless data hiding using pixel value manipulation instead of traditional cryptographic techniques.

- Works on any standard image file format (PNG , JPG, JPEG).

END USERS

- **Software Developers** – Learning steganography concepts and their applications.

- **Cybersecurity Enthusiasts** – Exploring secure communication techniques.

- **Government & Defense** – Secure message transmission without raising suspicion.

- **Journalists & Activists** – Concealing sensitive information in images to avoid surveillance.

edunet
foundation

RESULTS

Initial image:

Encrypted image:

```
1 import cv2
2 import os
3 import string
4
5 img = cv2.imread("Image.jpg") # Replace with the correct image path
6 password = input("Enter a passcode:")
7 msg = input("Enter secret message:")
8
9
10 d = {}
11 c = {}
12
13 for i in range(255):
14     d[chr(i)] = 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, z]= d[msg[i]]
23     n = n + 1
24     m = m + 1
25     z = (z + 1) % 3
26
27 cv2.imwrite("encryptedImage.jpg", img)
28
29
30 message = ""
31 n = 0
32 m = 0
33 z = 0
34
35 pas = input("\nEnter passcode for Decryption : ")
36 if password == pas:
37     for i in range(len(msg)):
38         message = message + c[img[n, m, z]]
39         n = n + 1
40         m = m + 1
41         z = (z + 1) % 3
42     print("Decryption message : ", message)
43 else:
44     print("YOU ARE NOT auth")
45
```

```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ cd Downloads

┌──(kali㉿kali)-[~/Downloads]
└─$ cd stegoproj

┌──(kali㉿kali)-[~/Downloads/stegoproj]
└─$ python3 stego_code.py
Enter a passcode:123
Enter secret message:This is my pic

Enter passcode for Decryption : 000
YOU ARE NOT auth

┌──(kali㉿kali)-[~/Downloads/stegoproj]
└─$ python3 stego_code.py
Enter a passcode:123
Enter secret message:This is my pic

Enter passcode for Decryption : 123
Decryption message :  This is my pic

┌──(kali㉿kali)-[~/Downloads/stegoproj]
└─$
```

CONCLUSION

- Steganography provides a covert way of communicating sensitive information.

- This project showcases a simple yet effective implementation of message hiding in images.

- The GUI makes encryption and decryption accessible even to non-technical users.

- Future improvements can make it more robust, secure, and scalable.

edunet
foundation

GITHUB LINK

https://github.com/chandrasenaredy/stegoproject1.git

FUTURE SCOPE

- **Advanced Encryption Techniques** – Integrate AES encryption before embedding text in images.

- **Support for Audio & Video Steganography** – Expanding beyond images.

- **AI-based Detection Prevention** – Ensuring messages stay undetectable from modern forensic tools.

- **Mobile App & Web Version** – Expanding accessibility beyond desktops.

- **Multi-Layer Security** – Combining steganography with blockchain for ultra-secure communication.

edunet
foundation

THANK YOU