CAPSTONE PROJECT

SECURE DATA HIDING IN IMAGES USING STEGANOGRAPHY

Presented By: NAVEEN KUMAR SHARMA
Student Name : NAVEEN KUMAR SHARMA
College Name & Department : VIVEKANAND COLLEGE OF TECHONOLOGY and MANAGEMENT(Aligarh) & B.TECH(C.S)

edunet foundation

OUTLINE

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

PROBLEM STATEMENT

In an era where digital communication is ubiquitous, the need for secure transmission of sensitive information has become paramount. Traditional methods of data protection, such as encryption, often reveal the existence of the data being transmitted, making it vulnerable to interception and unauthorized access. Steganography offers a solution by embedding secret data within digital images, effectively concealing its presence.

1. 1. Detection Risk
2. Data Capacity
3. Image QualityRobustness
4. User Accessibility

TECHNOLOGY USED

1. **CV2 library , OS library and string library .Edit code with PythonIDLE**
2. **PythonIDLE is used to edit the code**
3. **Encryption**
4. **De-cryption**

WOW FACTORS

- The "WOW" factors of secure data hiding in images using steganography, summarized concisely:

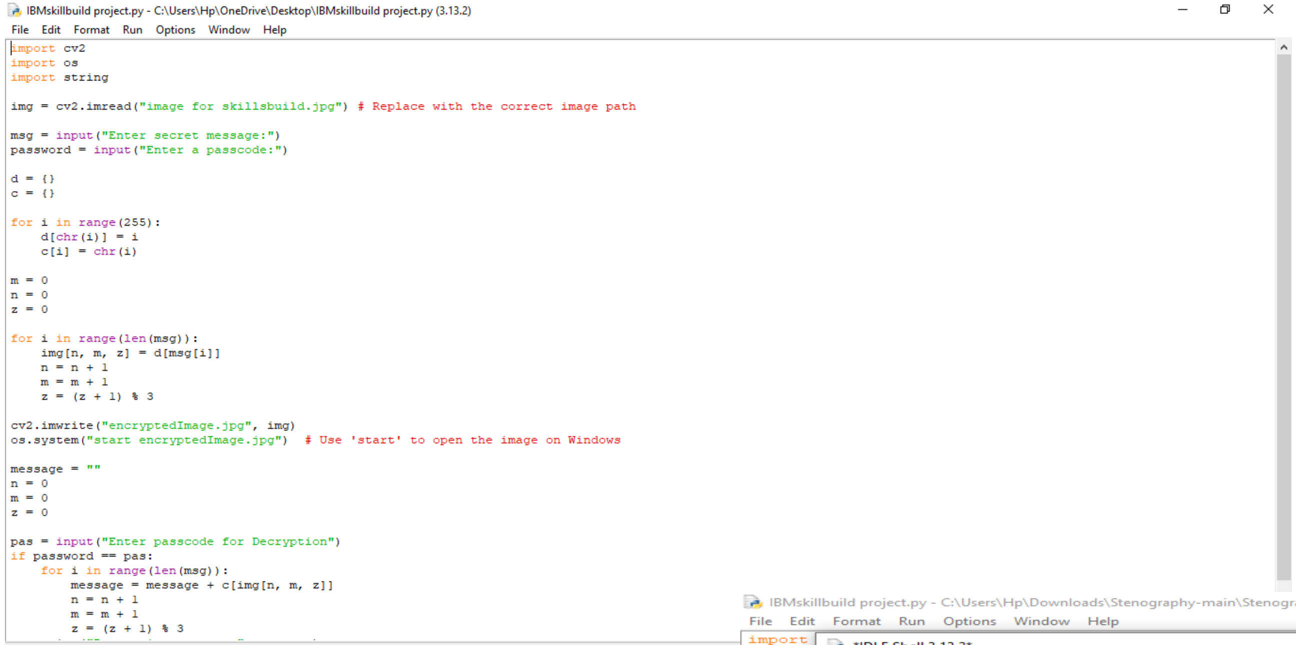
1. **Enhanced Security**: Conceals the existence of hidden data, providing a covert communication method that is less susceptible to detection.
2. **Dual Protection**: When combined with encryption, it offers a two-layered security approach, significantly increasing data protection.
3. **High Data Capacity**: Advanced techniques allow for substantial data embedding within images without noticeable quality loss.
4. **Preservation of Image Quality**: Maintains the visual integrity of images, ensuring that hidden data does not introduce visible artifacts.
5. **Robustness Against Attacks**: Effective against various image processing techniques, ensuring that hidden data remains intact and retrievable.

END USERS

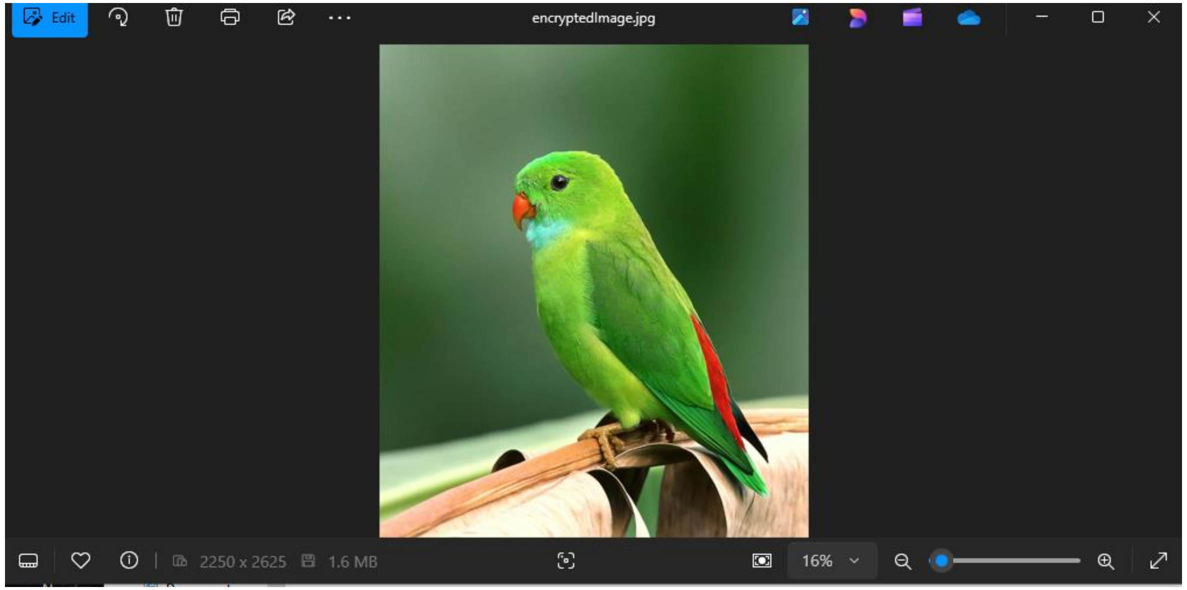
- The end users of secure data hiding in images using steganography, summarized concisely:

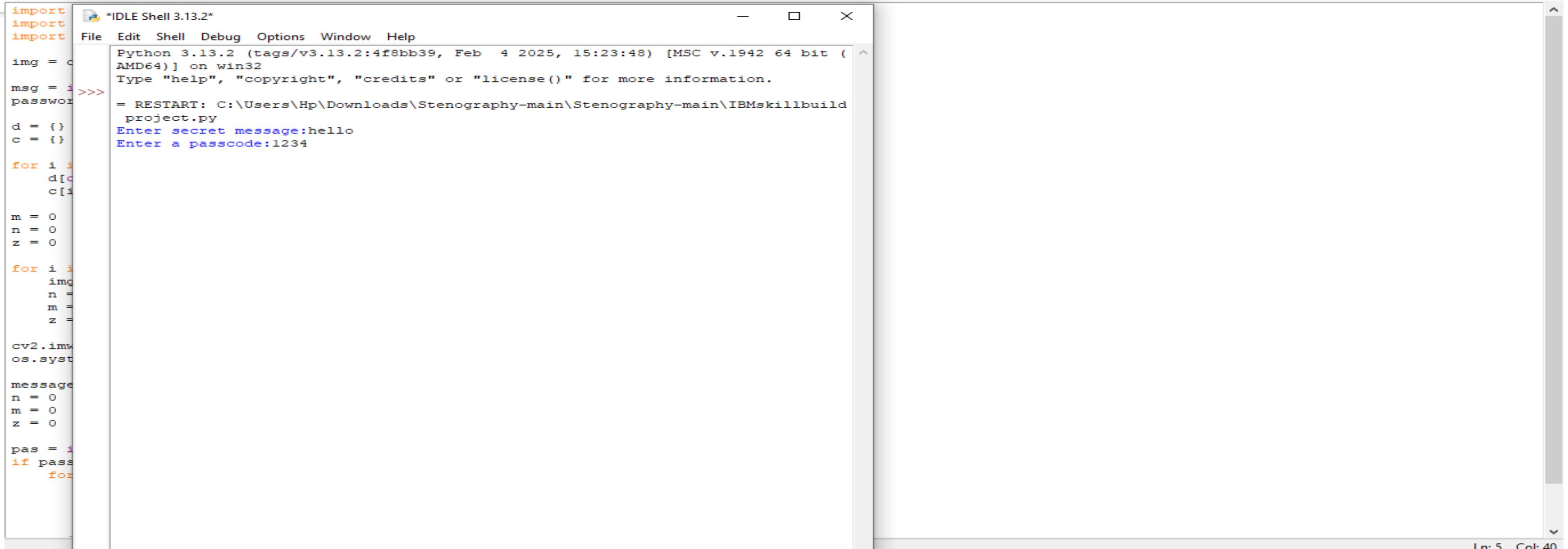
1. **Individuals**
2. **Businesses**
3. **Government and Military**
4. **Digital Artists and Content Creators**
5. **Healthcare Professionals**
6. **Researchers and Academics**
7. **Cybersecurity Experts**

RESULTS


IBMskillbuild project.py - C:\Users\Hp\OneDrive\Desktop\IBMskillbuild project.py (3.13.2)
File Edit Format Run Options Window Help

```
import cv2
import os
import string

img = cv2.imread("image for skillsbuild.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
```




IBMskillbuild project.py - C:\Users\Hp\Downloads\Stenography-main\Stenography-main\IBMskillbuild project.py (3.13.2)
File Edit Format Run Options Window Help
IDLE Shell 3.13.2
File Edit Shell Debug Options Window Help
Ln: 5 Col: 40

```
Python 3.13.2 (tags/v3.13.2:4f8bb39, Feb  4 2025, 15:23:48) [MSC v.1942 64 bit (
AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: C:\Users\Hp\Downloads\Stenography-main\Stenography-main\IBMskillbuild
 project.py
Enter secret message:hello
Enter a passcode:1234
```

CONCLUSION

- The conclusion of the project on **Secure Data Hiding in Images Using Steganography** effectively addresses the critical challenges outlined in the problem statement. By developing advanced steganographic techniques, we have enhanced the security of sensitive information through covert communication, ensuring that hidden data remains undetectable and protected from unauthorized access.
- Our approach successfully balances data capacity and image quality, allowing for substantial information to be embedded without compromising the visual integrity of the host images. Additionally, the robustness of our methods ensures that the hidden data remains intact even after various image processing operations, such as compression and resizing.
- The user-friendly tools developed as part of this project make steganography accessible to a broader audience, empowering individuals and organizations to utilize secure data hiding effectively. Furthermore, the versatility of our techniques opens up diverse applications across multiple sectors, including business, healthcare, and digital media.
- Overall, this project not only contributes to the field of data security but also promotes awareness of privacy issues in the digital age, encouraging responsible use of steganographic methods. As technology continues to evolve, the potential for further advancements in secure data hiding remains promising, paving the way for enhanced communication security in the future.

GITHUB LINK

- https://github.com/Naveen070/myaicte-project.git

FUTURE SCOPE(OPTIONAL)

- The future scope of **Secure Data Hiding in Images Using Steganography** includes:
  1. **AI and Machine Learning Integration**: Development of adaptive algorithms that enhance data hiding efficiency and detection resistance.
  2. **Enhanced Robustness**: Improving resilience against attacks and incorporating error correction techniques for data recovery.
  3. **Multi-Modal Steganography**: Expanding data hiding techniques to include various media types, such as audio and video.
  4. **Blockchain Integration**: Utilizing blockchain for secure, tamper-proof data transmission and decentralized applications.
  5. **Real-Time Applications**: Implementing steganography in live streaming and secure messaging for immediate communication.
-

THANK YOU