CAPSTONE PROJECT

SECURE DATA HIDING IN IMAGES USING STEGANOGRAPHY

Presented By:

Student Name : PRATIK DHAGE

College Name & Department :

D Y Patil College of engineering and technology, Kolhapur

edunet foundation

OUTLINE

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

PROBLEM STATEMENT

Data security is a paramount issue in the digital era, particularly when handling sensitive information. Conventional encryption techniques can be complicated and often require additional storage for encrypted files. This project presents an innovative image-based encryption and decryption system, enabling users to securely embed secret messages within images. Access to the decrypted message is safeguarded by a password, ensuring only authorized individuals can retrieve the information.

TECHNOLOGY USED

Programming Language:

- **Python –** Used for building encryption and decryption logic.

Libraries & Frameworks:

- **OpenCV –** Handles image processing and manipulation.
- **Numpy –** Supports array-based operations for embedding messages.
- **PyQt6 –** Creates a user-friendly GUI for encryption and decryption.

Platforms:

- Runs on **Windows, Linux and macOS** with python installed.

WOW FACTORS

What Makes This Project Unique?

•**Image-based Steganography** – Unlike conventional encryption, the message is concealed within the pixel values of an image.

•**Intuitive GUI** – Users can interact through a graphical interface without relying on command-line operations.

•**Secure Access** – Decryption requires the correct password, ensuring an extra layer of protection.

•**Storage-Free Encryption** – The message remains embedded within the image, removing the need for separate encrypted files.

END USERS

- **Cybersecurity Enthusiasts** – Dive into encryption and steganography techniques.
- **Journalists & Activists** – Share sensitive information discreetly and securely.
- **Students & Researchers** – Gain insights into cryptography and image processing.
- **Photographers & Designers** – Embed copyright details to safeguard intellectual property.
- **General Users** – Conceal private messages or sensitive data within images effortlessly.

RESULTS

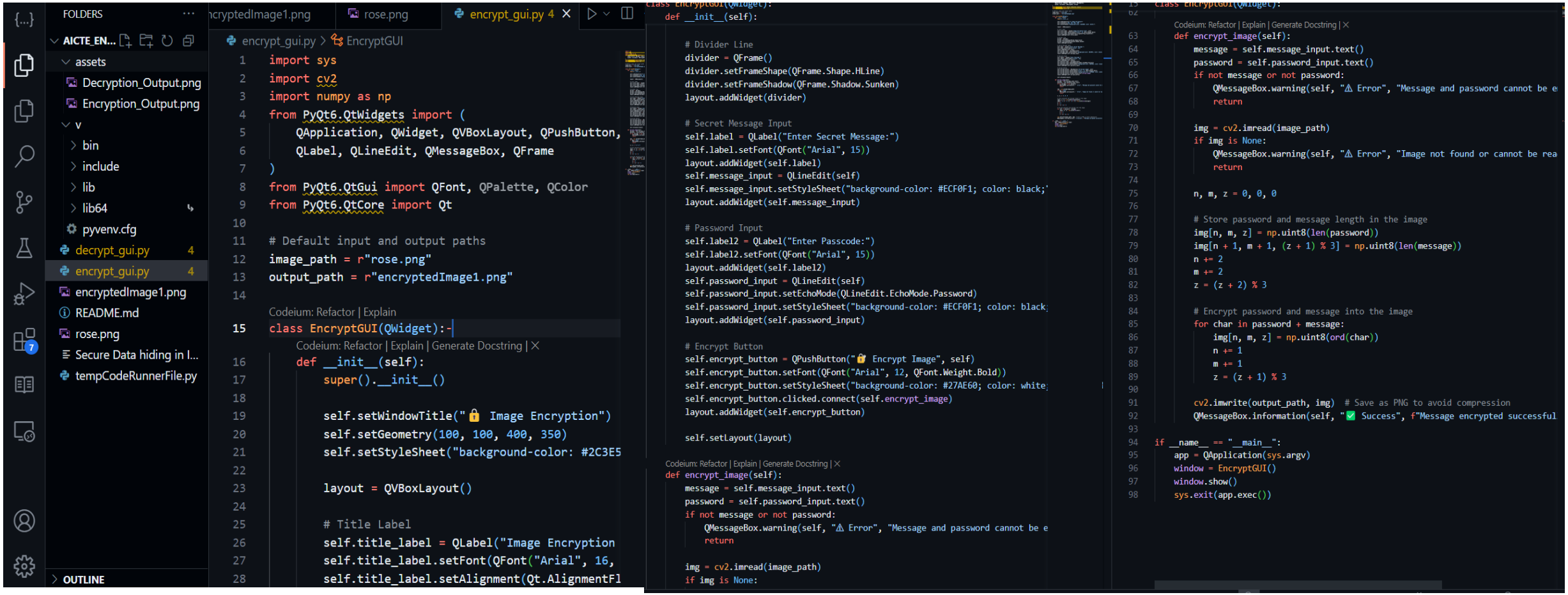
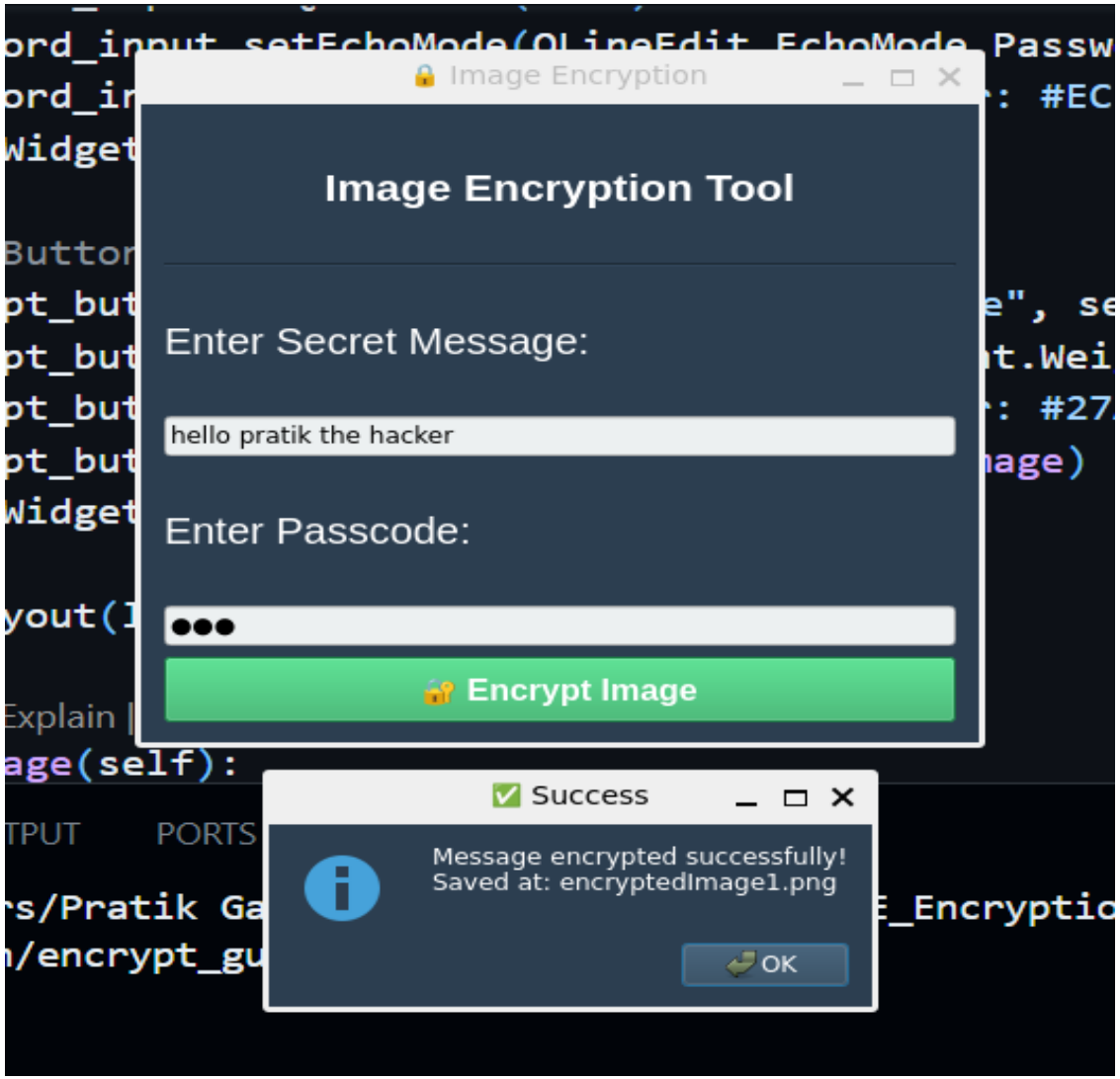


Figure 1: Encryption Code

edunet foundation

Figure 2: Encryption Output



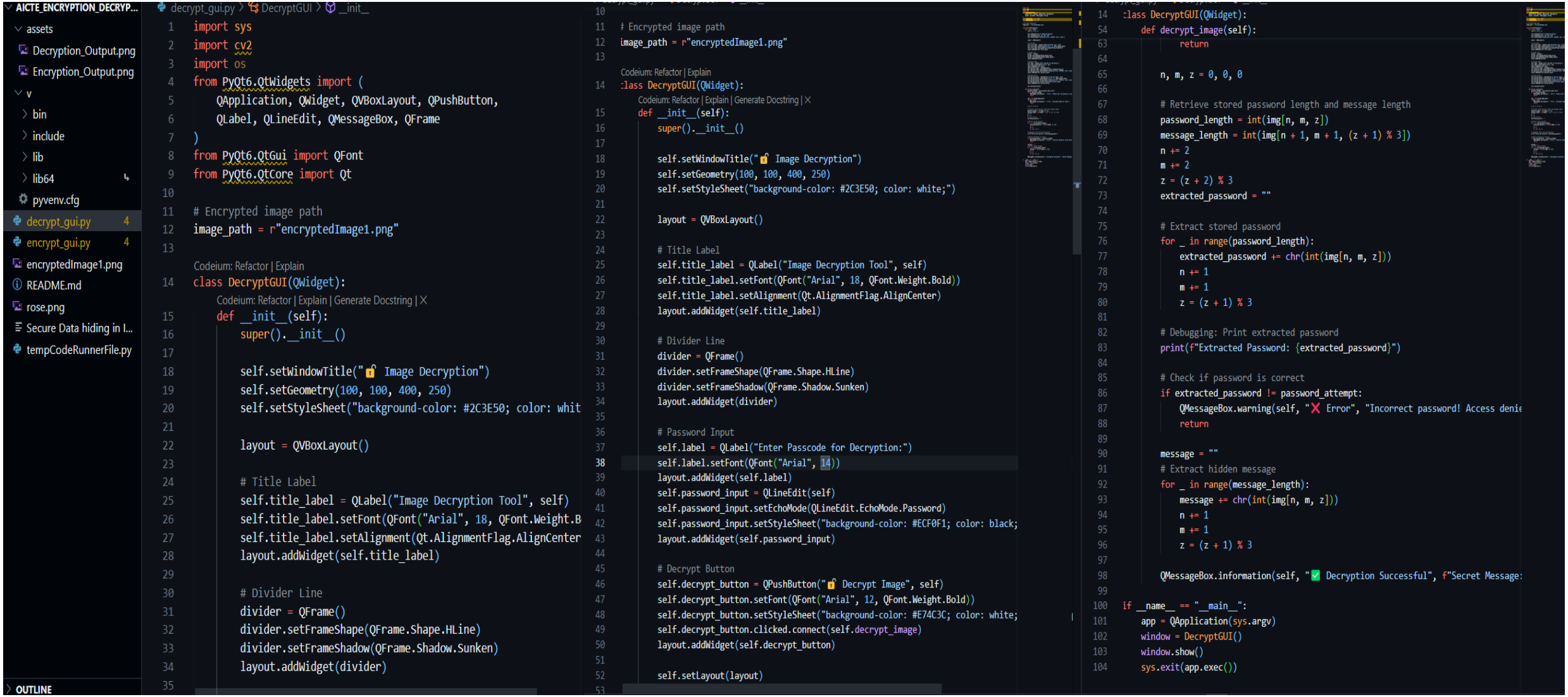


Figure 3: Decryption code

Figure 4: Decryption Output

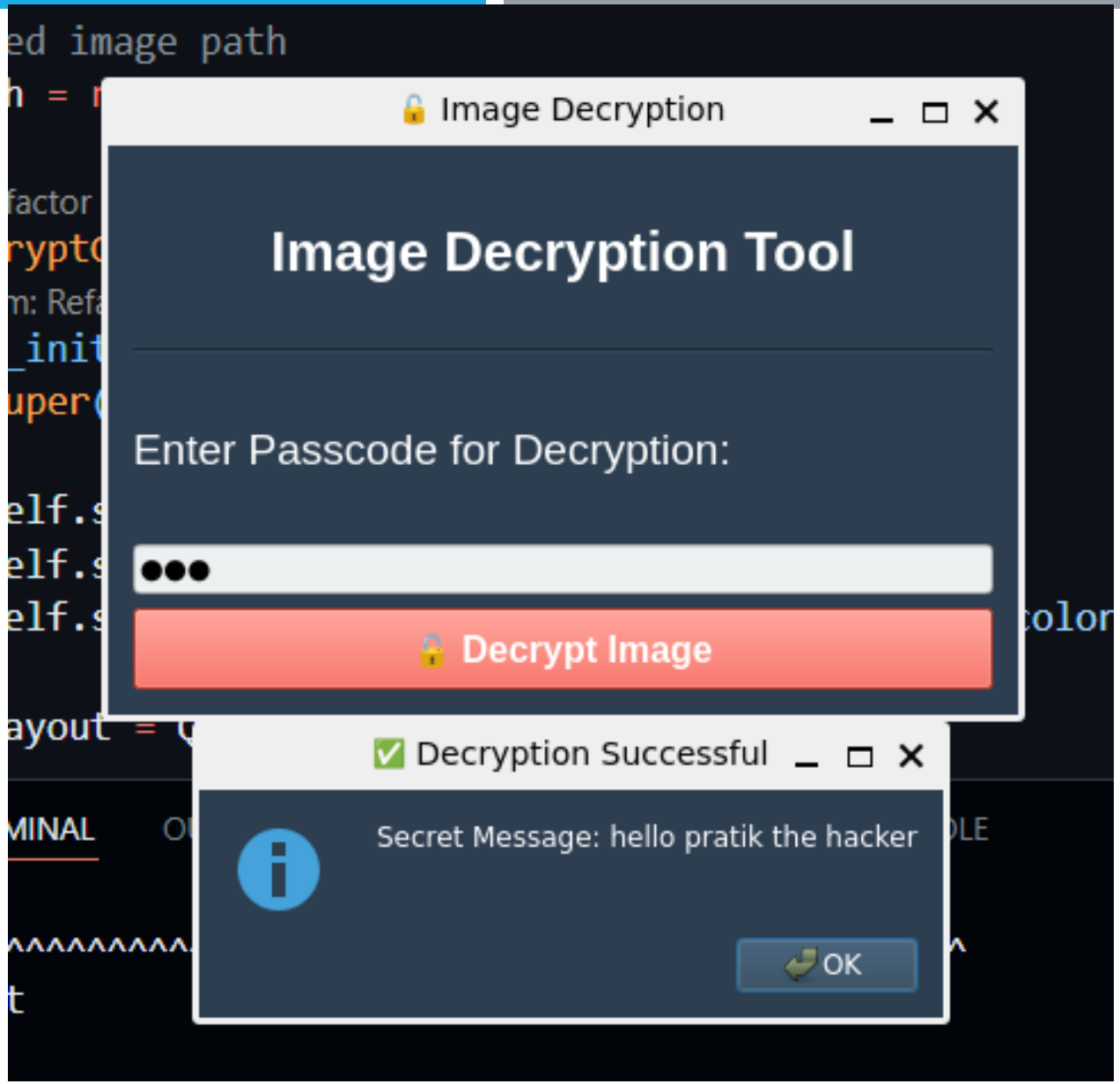


Figure 5 : Encrypted Image

CONCLUSION

Project Summary:

- This project offers a straightforward yet powerful method for encrypting messages within images using steganography and password protection.
- With an intuitive graphical user interface (GUI), it ensures accessibility for both technical and non-technical users.
- Leveraging OpenCV and NumPy, the system enables fast and efficient message embedding and extraction while preserving image integrity.
- Ultimately, this project showcases a practical implementation of image-based cryptography, enhancing secure communication.

GITHUB LINK

- https://github.com/CodeSmithPratik/IBM_AICTE_CYBERSECURITY_INTERNSHIP_PROJECT.git

FUTURE SCOPE(OPTIONAL)

- **Stronger Security Measures** – Integrate AES or RSA encryption with steganography for a dual-layer protection system.
- **Expanded Format Support** – Enable compatibility with multiple image formats, including JPG, BMP, and TIFF.
- **Cross-Platform Availability** – Develop mobile and web-based versions for broader accessibility.
- **AI-Powered Security** – Utilize deep learning to detect tampered images and enhance security mechanisms.

THANK YOU 

edunet foundation