CAPSTONE PROJECT

SECURE DATA HIDING IN IMAGE USING STEGANOGRAPHY

Presented By:
Saket Chaudhary
Veer Bahadur Singh Purvanchal University
B.Tech. (CSE)

OUTLINE

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

PROBLEM STATEMENT

In today's digital era, secure communication is crucial to prevent unauthorized access to sensitive information. Traditional encryption methods are easily detectable, making them a target for attackers. Steganography offers a solution by hiding secret messages within images, ensuring covert data transmission. This project aims to develop a user-friendly, password-protected steganography tool that enables secure message encoding and decoding with minimal image distortion.

TECHNOLOGY USED

- **Programming Language:** Python
- **GUI Framework**: Tkinter (for user-friendly interface)
- **Image Processing**: OpenCV (cv2)
- **Numerical Computation**: NumPy (for pixel manipulation)
- **File Handling & OS Integration:** OS module
- **Version Control & Collaboration**: GitHub
- **Platform**: Windows/Linux/Mac (Cross-platform compatibility)

WOW FACTORS

◇ **LSB Steganography** – Uses the *Least Significant Bit (LSB)* method for seamless message hiding without noticeable image distortion.

◇ **Password Protection** – Ensures that only authorized users can decode the hidden message.

◇ **Graphical User Interface (GUI)** – User-friendly interface for encoding and decoding messages without needing coding knowledge.

◇ **Multiple Image Format Support** – Works with *.png, .jpg*, and *.bmp* files, making it flexible for different use cases.

◇ **Fast & Efficient Processing** – Optimized encoding/decoding ensures quick message hiding and retrieval.

◇ **Cross-Platform Compatibility** – Runs on Windows, Linux, and macOS without requiring complex setup.

◇ **Open-Source & Extensible** – Can be enhanced with additional security features like AES encryption or AI-based detection prevention in the future.

END USERS

- 👨‍💻 **Cybersecurity Professionals** – Secure confidential data transmission.
- 📧 **Journalists & Activists** – Hide sensitive information to ensure privacy.
- 🔐 **Military & Intelligence Agencies** – Enable covert communication.
- 📊 **Business Organizations** – Protect confidential corporate data.
- 🎓 **Students & Researchers** – Learn and explore steganography techniques.
- 📱 **Individuals & Privacy Enthusiasts** – Secure personal messages from unauthorized access.

RESULTS

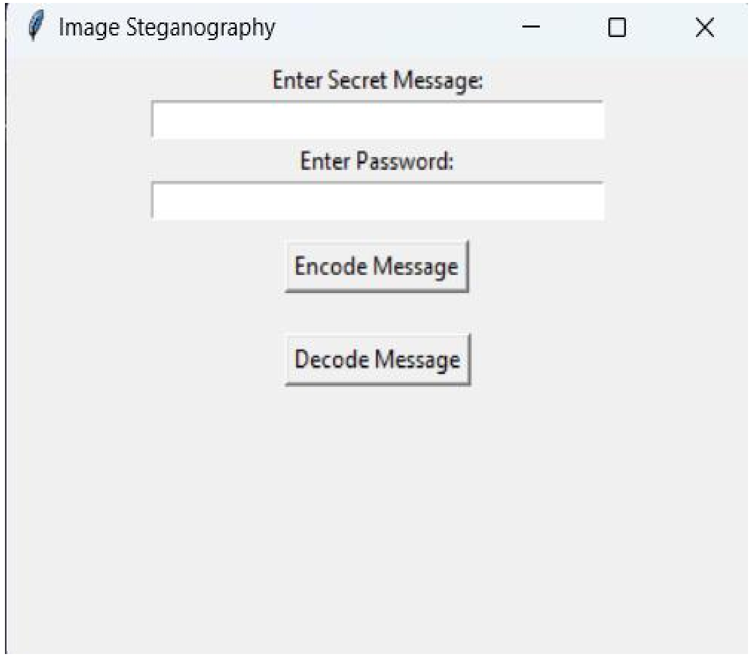
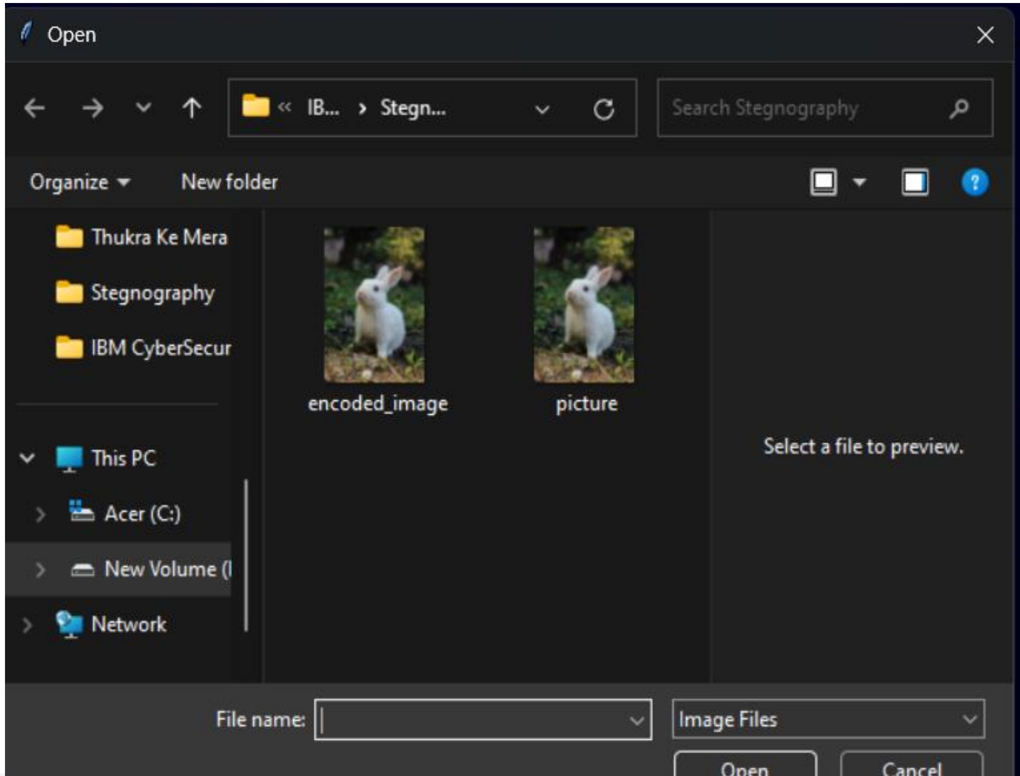


Image Steganography

Enter Secret Message:

Enter Password:



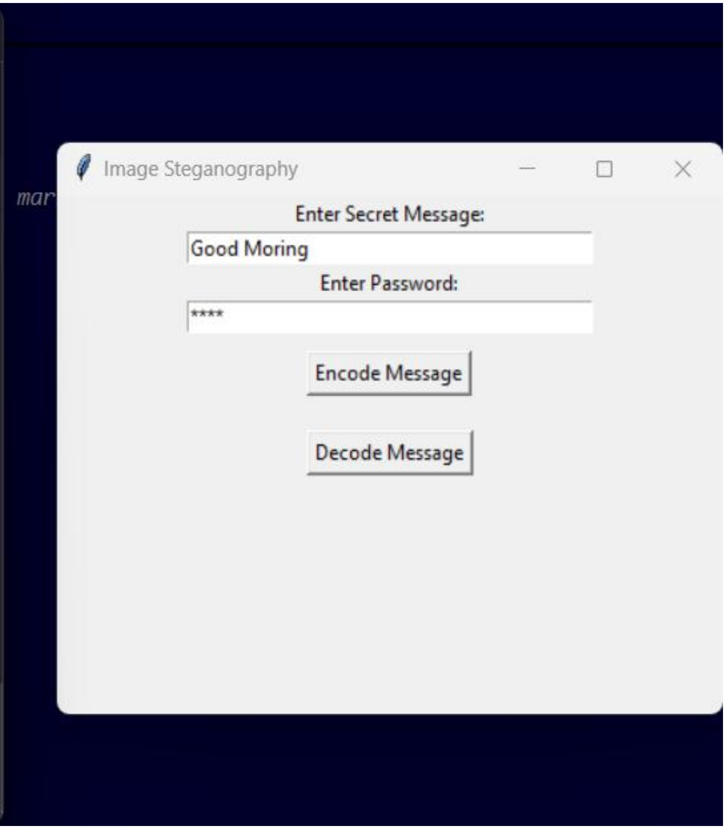
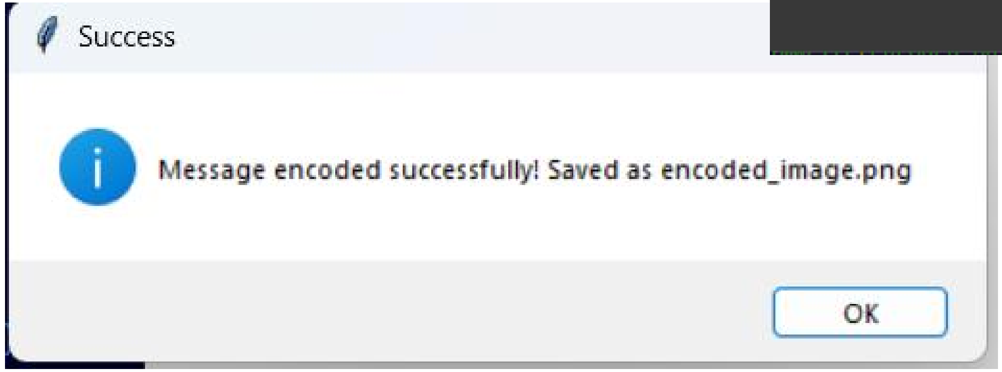


Image Steganography

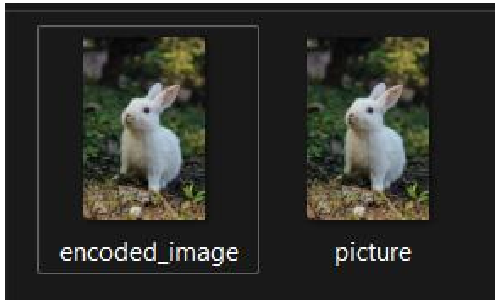
Enter Secret Message: Good Moring

Enter Password: ****



Success

Message encoded successfully! Saved as encoded_image.png



edunet foundation

CONCLUSION

StegoShield successfully addresses the challenge of *secure and covert data transmission* by utilizing *LSB Steganography* to hide messages within images without noticeable distortion. The *password-protected GUI-based tool* ensures that only authorized users can access hidden information, enhancing *data security and privacy*.

This project demonstrates the effectiveness of steganography in real-world secure communication, making it valuable for *cybersecurity, intelligence, and personal data protectio*n. With future enhancements like *encryption and AI-based detection prevention*, StegoShield has the potential to become a robust solution for next-generation digital security. 🚀

GITHUB LINK

🔗 StegoShield GitHub Repository

https://github.com/Saket22-CS/StegoShield.git

My Repository includes:

✓ **README.md** (Already provided—add it if not done yet)

✓ **Source Code** (`*stegoshield.py*` and other necessary files)

✓ **requirements.txt** (List of dependencies for easy setup)

✓ **Screenshots Folder** (Add images to showcase results)

FUTURE SCOPE

◇ **Advanced Encryption** – Integrate AES or RSA encryption to further secure hidden messages.

◇ **Audio & Video Steganography** – Expand beyond images to hide data in audio and video files.

◇ **Cloud Integration** – Enable secure storage and retrieval of stego-images on cloud platforms.

◇ **Mobile App Development** – Create an Android/iOS app for on-the-go secure messaging.

◇ **AI-Powered Steganalysis Prevention** – Use deep learning to make hidden messages even harder to detect.

◇ **Batch Processing** – Allow encoding/decoding multiple images at once for efficiency.

◇ **Blockchain Integration** – Use blockchain for verifying stego-images' authenticity and ownership.

These enhancements will make **StegoShield a more powerful and versatile tool for next-generation digital security!** 🔐🚀

THANK YOU

edunet
foundation