CAPSTONE PROJECT

SECURE DATA HIDING IN IMAGE USING STENOGRAPHY

Presented By : SAIBA SRI MAHALAKSHMI
Student Name : SAIBA SRI MAHALAKSHMI
College Name : GEETHANJALI INSTUTION OF PG STUDIES
Department : MASTER OF COMPUTER APPLICATION

edunet foundation

OUTLINE

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

PROBLEM STATEMENT

With the increasing need for secure communication and data protection, traditional encryption methods may attract unwanted attention. Stenography, the practice of concealing information within digital media, offers a covert way to transmit sensitive data without raising suspicion. The challenge is to develop a stenography-based system that can efficiently hide and extract text within images, audio, or video files while maintaining the original quality and ensuring minimal detectability. The system should be user-friendly, support various file formats, and provide a robust mechanism for data security and retrieval.

TECHNOLOGY USED

- **Programming Language :** Python Development Environment: Python IDLE Libraries & Modules : PIL (Pillow) – For image processing (hiding and extracting data in images)
- **OpenCV** – If working with advanced image processing
- **NumPy** – For handling image data in arrays
- **Wave (built-in Python module)** – If implementing audio stenography
- **Cryptography** – For encrypting the hidden message

WOW FACTORS

- 1.Invisible Data Hiding

  The message is hidden inside an image or audio without changing its appearance or quality, making it undetectable.

- 2. Encryption for Extra Security

  Uses encryption (e.g., AES or simple XOR cipher) to add an extra layer of protection before hiding the message.

- 3. Multiple File Format Support

  Can work with JPEG, PNG, BMP for images or WAV for audio files.

- 4. Easy Message Extraction

  With a simple Python script, the hidden message can be extracted instantly.

- 5. Minimal Image Distortion

  The algorithm ensures that image quality remains unchanged, preventing detection by the human eye.

- 6. Lightweight & Fast Processing

  The program runs quickly and efficiently, even on low-end systems.

- 7. User-Friendly & Customizable

  Simple GUI (if implemented using Tkinter or PyQt) makes it easy to use, or a CLI for power users.

END USERS

- 1. Cybersecurity Professionals

  To securely transmit sensitive data without attracting attention.

- 2. Journalists & Whistleblowers

  To communicate confidential information without detection.

- 3. Government & Defense Organizations

  For covert communication and data protection.

- 4. Digital Forensics Experts

  To uncover hidden messages in digital evidence.

- 5. Ethical Hackers & Penetration Testers

  To test security measures against hidden data transmission.

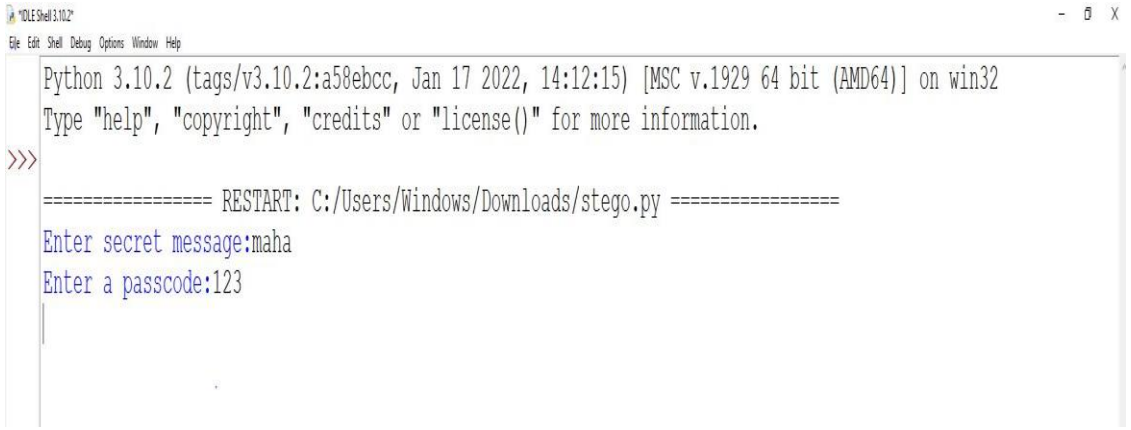
- 6. Individuals Concerned About Privacy

  For personal data security in images or audio files.

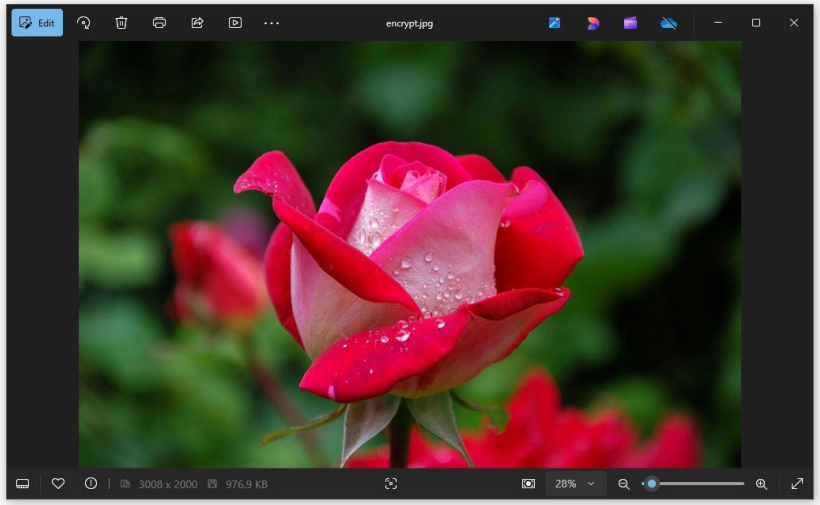
- 7. Software Developers & Researchers

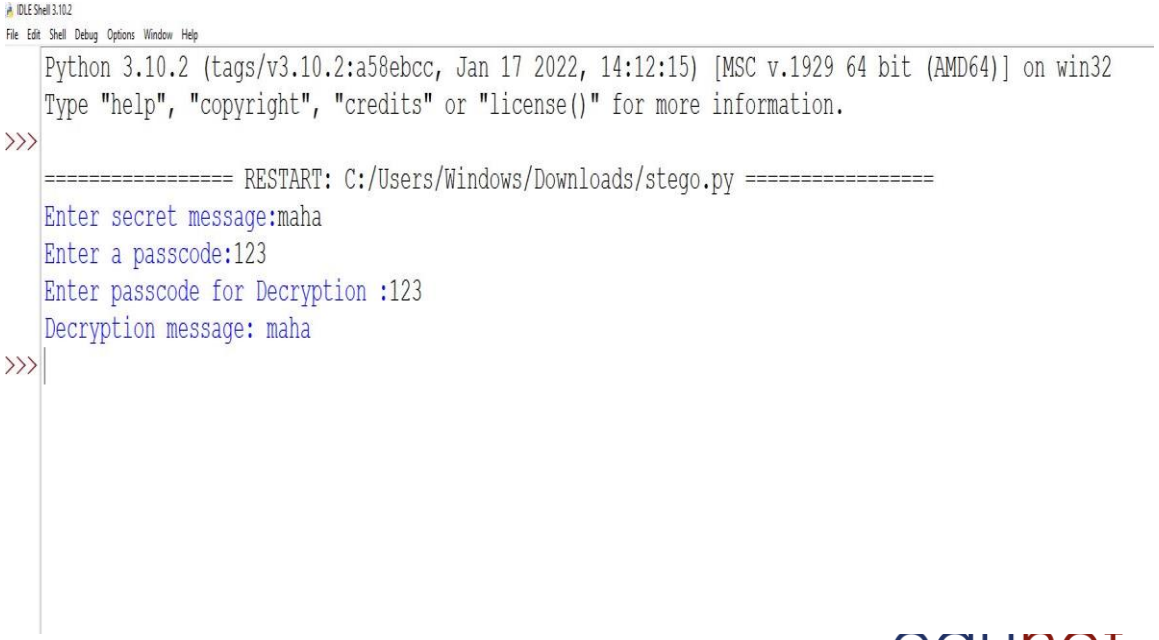
  To explore data hiding techniques and improve security algorithms.

RESULTS




```
========== RESTART: C:\Users\Windows\Downloads\stego.py ==========
Enter secret message:maha
Enter a passcode:123
Enter passcode for Decryption :
```





CONCLUSION

- Stenography is a powerful technique for hiding sensitive information within digital media, ensuring covert communication without raising suspicion. This project successfully implements image-based stenography using Python IDLE, allowing users to embed and extract hidden messages while preserving the original quality.
- With features like encryption, multiple file format support, and minimal image distortion, the project enhances data security and privacy. It has practical applications in cybersecurity, journalism, digital forensics, and personal data protection.
- Future improvements could include audio and video stenography, a user-friendly GUI, and advanced encryption techniques for enhanced security. This project demonstrates the potential of steganography in modern cybersecurity while maintaining simplicity and efficiency.

GITHUB LINK

- https://github.com/sri0099/steno.git

FUTURE SCOPE(OPTIONAL)

- 1.**Support for Audio & Video Stenography**

  Extend the project to hide messages in audio (WAV, MP3) and video (MP4, AVI) files for enhanced versatility.

- 2.**Improved Encryption Techniques**

  Integrate AES, RSA, or SHA encryption to make hidden messages even more secure.

- 3.**AI-Based Steganalysis Resistance**

  Implement machine learning techniques to make hidden data harder to detect by AI-based forensic tools.

- 4.**Lossless Data Compression**

  Use compression algorithms (e.g., Huffman coding, LZW) to reduce message size while maintaining quality.

- 5.**Cloud Integration**

  Enable secure cloud storage and retrieval of steganographic images/audio for remote access.

THANK YOU

edunet foundation