CAPSTONE PROJECT

SECURE DATA HIDING IN IMAGES USING STEGANOGRAPHY

Presented By :DABBI ANIL
Student Name :DABBI ANIL

College Name: SRI VENKATESWARA COLLEGE OF ENGINEERING



OUTLINE

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



PROBLEM STATEMENT

To develop a robust and secure steganography system that effectively hides sensitive data within digital images, while maintaining high visual quality of the carrier image, resisting detection attempts, and providing strong encryption mechanisms to protect the embedded data from unauthorized access, ensuring confidentiality and integrity during transmission and extraction.



KEY POINTS IN THE PROBLEM STATEMENT:

- Secure data hiding
- High visual quality
- Encryption
- Integrity protection



TECHNOLOGY USED

Libraries:

- 1. cv2 (OpenCV cv2 means Computer Vision 2)
- **Purpose:** OpenCV is a comprehensive library focused on real-time computer vision. It provides a wide range of functions for image and video processing.
- 2. os
- **Purpose:** The os module provides a way to interact with the operating system. It includes functions for file and directory manipulation, running system commands, and getting environment variables.
- string
- Purpose:

The string module provides a collection of string-related constants and functions.

Used IDE Platform:

IDE stands for Integrated Development Environment. A Python IDE is a platform that helps programmers write, test, compile, run, and debug Python code.



WOW FACTORS

The project demonstrates the *idea* of steganography. However, as a practical implementation, it has significant limitations in terms of security, robustness, and compatibility. It's a good starting point for learning about image processing and information hiding, but it's far from a production-ready solution.

"Wow" Factors (Potentially Impressive Aspects):

- Steganography Concept
- Image Manipulation
- Basic Encryption/Decryption
- Simplicity



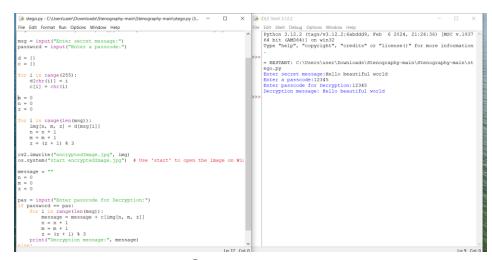
END USERS

- Activists/Human Rights Organizations
- Security Professionals/System Administrators
- Law Enforcement/Intelligence Agencies
- Private Individuals (Concerned about Privacy)
- Digital Watermarking
- Medical Data Sharing
- Secure Communication



RESULTS

Input



Output





CONCLUSION

- Secure data hiding in images using steganography is a powerful concept with the potential to address critical needs for privacy, security, and covert communication in various contexts. From protecting journalistic sources and safeguarding activist communications to securing sensitive data transfers and enabling covert law enforcement operations, the applications are diverse and impactful.
- secure data hiding in images using steganography offers a powerful method to discreetly embed sensitive information within seemingly normal images, making it a valuable tool for covert communication where the very existence of hidden data needs to remain undetected; however, to achieve optimal security, robust encryption techniques should be employed alongside steganography to protect the hidden data itself, while considering potential vulnerabilities in steganalysis methods that could reveal the presence of embedded information



GITHUB LINK

https://github.com/anilgithub123/My-Project-aicte-edunet.git



THANK YOU

