CAPSTONE PROJECT

SECURE DATA HIDING IN IMAGE USING STEGANOGRAPHY

Presented By: Sharlene Anna Pereira
Student Name : Sharlene Anna Pereira
College Name & Department : CHRIST (Deemed To Be University),
Computer Science And Engineering

OUTLINE

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

PROBLEM STATEMENT

- Traditional encryption produces visible ciphertext, making it susceptible to interception.
- Attackers can detect encrypted messages and attempt decryption.
- This project **hides AES-256 encrypted messages inside images** using steganography.
- The encrypted text remains **invisible** and **undetectable** to unauthorized users.
- Even if extracted, the message cannot be read without the correct password.

TECHNOLOGY USED

- Programming Language

  Python: Used for implementing encryption, image processing, and user interface.

- Development Environment

  Google Colab: A cloud-based platform for running Python scripts.

  GitHub: Version control and project hosting.

- Libraries Used

  OpenCV: Image processing and manipulation.

  Gradio: Creating a user-friendly interface for encryption and decryption.

  Cryptography: Implementing AES-256 encryption and password-based key derivation.

  NumPy: Handling numerical operations and image data processing.

WOW FACTORS

- ✓ **AES-256 Encryption:** The highest level of encryption used to secure sensitive data.
- ✓ **Steganography Integration:** Hides encrypted messages inside images, making them invisible to unauthorized users.
- ✓ **Dual-Layer Security:** Even if the image is extracted, the encrypted message remains protected with AES encryption.
- ✓ **Gradio Web Interface:** Provides an interactive and easy-to-use interface for encryption and decryption.
- ✓ **Cross-Platform Compatibility:** Works on any operating system that supports Python.
- ✓ **Small File Size Impact:** The encryption and embedding process does not significantly alter the size or quality of the image.

END USERS

- **Individuals:** Protect private messages from unauthorized access.
- **Organizations:** Securely share sensitive business communications.
- **Journalists and Activists:** Safeguard confidential information in high-risk environments.
- **Cybersecurity Professionals:** Study encryption and steganography techniques.
- **Law Enforcement Agencies:** Use steganography for undercover communications.

RESULTS

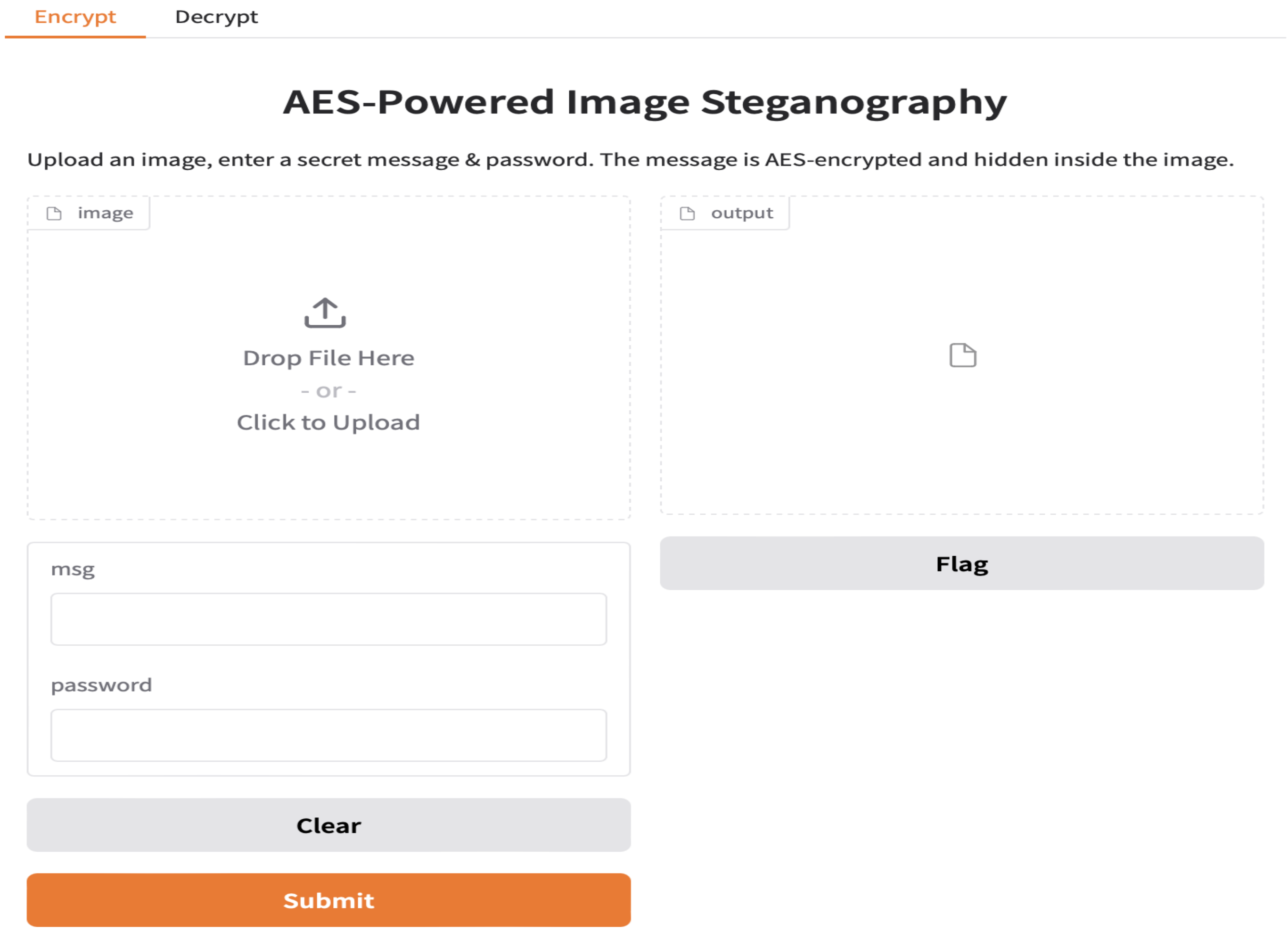
- **Encryption Process**

1. The user **uploads an image** and enters a secret message.
2. The message is **encrypted using AES-256.**
3. The encrypted text is **embedded into the image pixels.**
4. The **modified image is saved**, appearing unchanged to the naked eye.

- **Decryption Process**

1. The encrypted image is **uploaded back into the system.**
2. The correct **password must be provided** for decryption.
3. The **hidden encrypted message is extracted** from the image.
4. The **message is decrypted** and displayed in its original form.

RESULTS

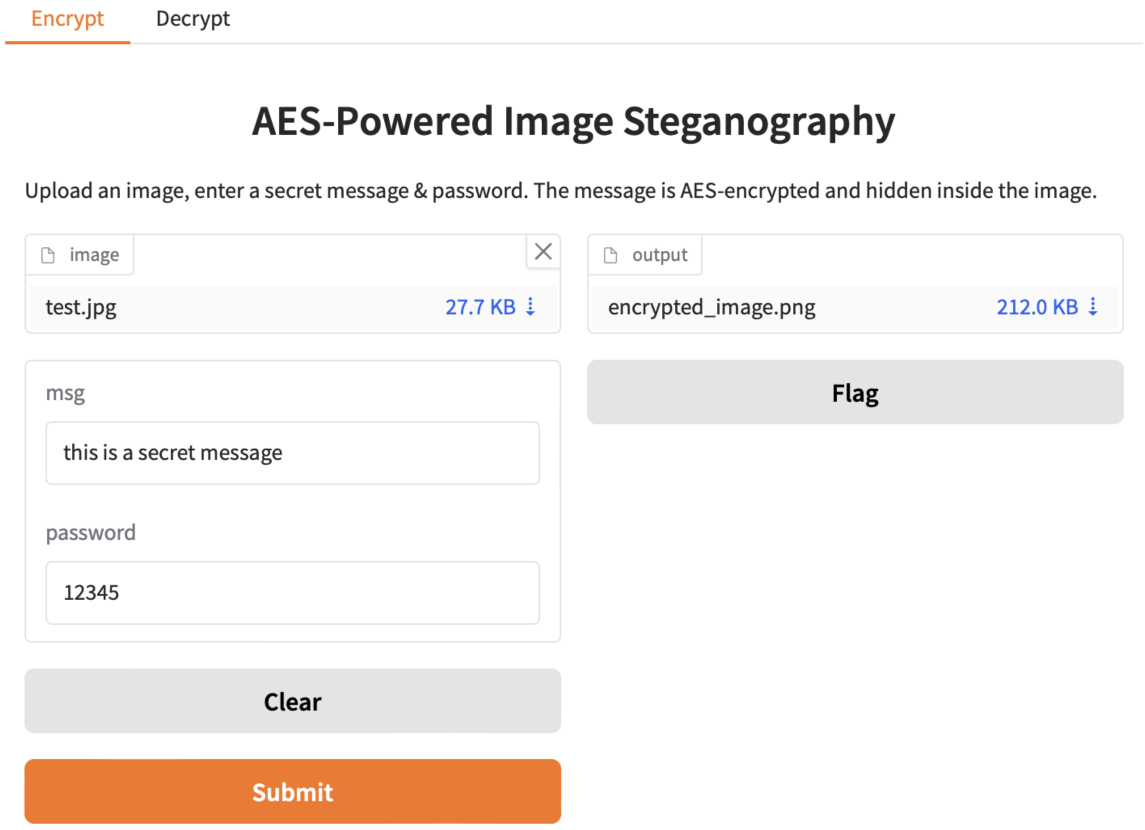


AES-Powered Image Steganography

Upload an image, enter a secret message & password. The message is AES-encrypted and hidden inside the image.

Fig: AES-Powered Image Steganography Interface

RESULTS



AES-Powered Image Steganography

Upload an image, enter a secret message & password. The message is AES-encrypted and hidden inside the image.

image: test.jpg 27.7 KB

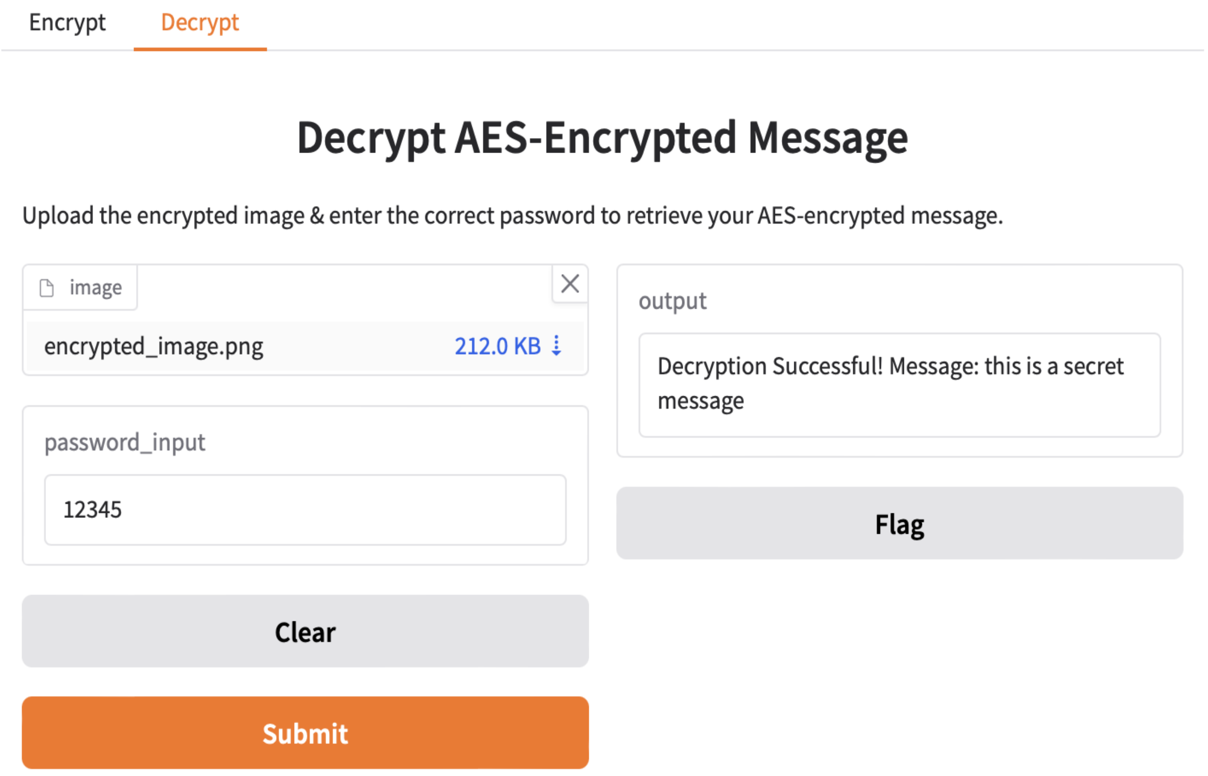
output: encrypted_image.png 212.0 KB

msg: this is a secret message

password: 12345

Fig: Encryption Interface

Designed to hide AES-encrypted messages inside images.



Decrypt AES-Encrypted Message

Upload the encrypted image & enter the correct password to retrieve your AES-encrypted message.

image: encrypted_image.png 212.0 KB

password_input: 12345

output: Decryption Successful! Message: this is a secret message

Fig: Decryption Interface

Retrieves hidden messages using the correct password.

CONCLUSION

- <u>**Project Achievements**</u>

✓ Successfully combined **AES-256 encryption** with **steganography** for secure message hiding.

✓ Developed a **user-friendly interface** using Gradio for accessibility.

✓ Ensured messages remain **undetectable and protected** from attacks.

✓ The project demonstrates a **practical approach to secure communication**.

- <u>**Key Takeaways**</u>

✓ **Encryption alone is not enough**—steganography adds an extra layer of security.

✓ **Even if the image is intercepted**, the encrypted message remains unreadable without the correct password.

✓ **This technique can be applied to secure messaging, watermarking, and digital forensics.**

GITHUB LINK

https://github.com/sharleneanna/Image-Steganography-AES.git

FUTURE SCOPE

- **Quantum-Secure Encryption:** Implement post-quantum cryptography for even stronger security.
- **Video Steganography:** Extend the project to hide encrypted messages inside video files.
- **AI-Powered Steganography:** Use machine learning to optimize embedding techniques and improve resistance against detection.
- **Blockchain Integration:** Store encrypted messages securely using decentralized technology.
- **Multi-Layer Steganography:** Hide messages in multiple layers of an image for enhanced security.

THANK YOU