
CAPSTONE PROJECT

SECURE DATA HIDING IN IMAGES USING STEGANOGRAPHY

Presented By: Aditri

Student Name :

ADITRI B RAY

College Name & Department :

MS RAMAIAH INSTITUTE OF TECHNOLOGY(MSRIT)

CSE(CORE)

BANGALORE

OUTLINE

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

PROBLEM STATEMENT

- With the rise of digital communication, securing sensitive data has become crucial.
- Traditional encryption methods are effective but often raise suspicion.
- Steganography provides a means to **hide information within images** in a way that is undetectable to the human eye, ensuring **covert data transmission**.
- However, existing steganography solutions lack **user-friendly interfaces, strong password protection, and web-based accessibility**.
- This project addresses these issues by developing a **secure, intuitive, and efficient image steganography tool**.

TECHNOLOGY USED

■ Frontend:

- HTML, CSS (Dark/Light theme), JavaScript – Interactive and accessible UI with theme toggling.

■ Backend:

- Python (Flask) – Handles encoding/decoding logic and user interactions.

■ Data Handling:

- OpenCV – Image processing for steganographic encoding/decoding.
- Pillow (PIL) – Image format handling and manipulation.

■ Security:

- AES Encryption – Ensures password-protected encoding and decoding.
- Salted Hashing – Used for securely storing passwords.

■ Security:

- **AES Encryption** – Ensures password-protected encoding and decoding.
- **Salted Hashing** – Used for securely storing passwords.

■ Storage:

- **File-based system** – Temporary storage for uploaded and processed images (can be extended to cloud storage).


■ Deployment:

- **Docker** – Containerized deployment for consistency across environments.
- **Google Cloud Run** – Serverless hosting for scalability and accessibility.

WOW FACTORS

- ✨ Interactive UI with Dark Mode & Theme Toggle
- ✨ Real-time Image Preview for selected images before encoding/decoding
- ✨ Password-Protected Encoding & Decoding for enhanced security
- ✨ Expanding Magic Smiley Animation in UI for an engaging experience
- ✨ Potential for Future AI-based Steganalysis Detection Countermeasures

END USERS

 **Cybersecurity Professionals** – Securely transmit sensitive data

 **Journalists & Activists** – Share confidential information under censorship

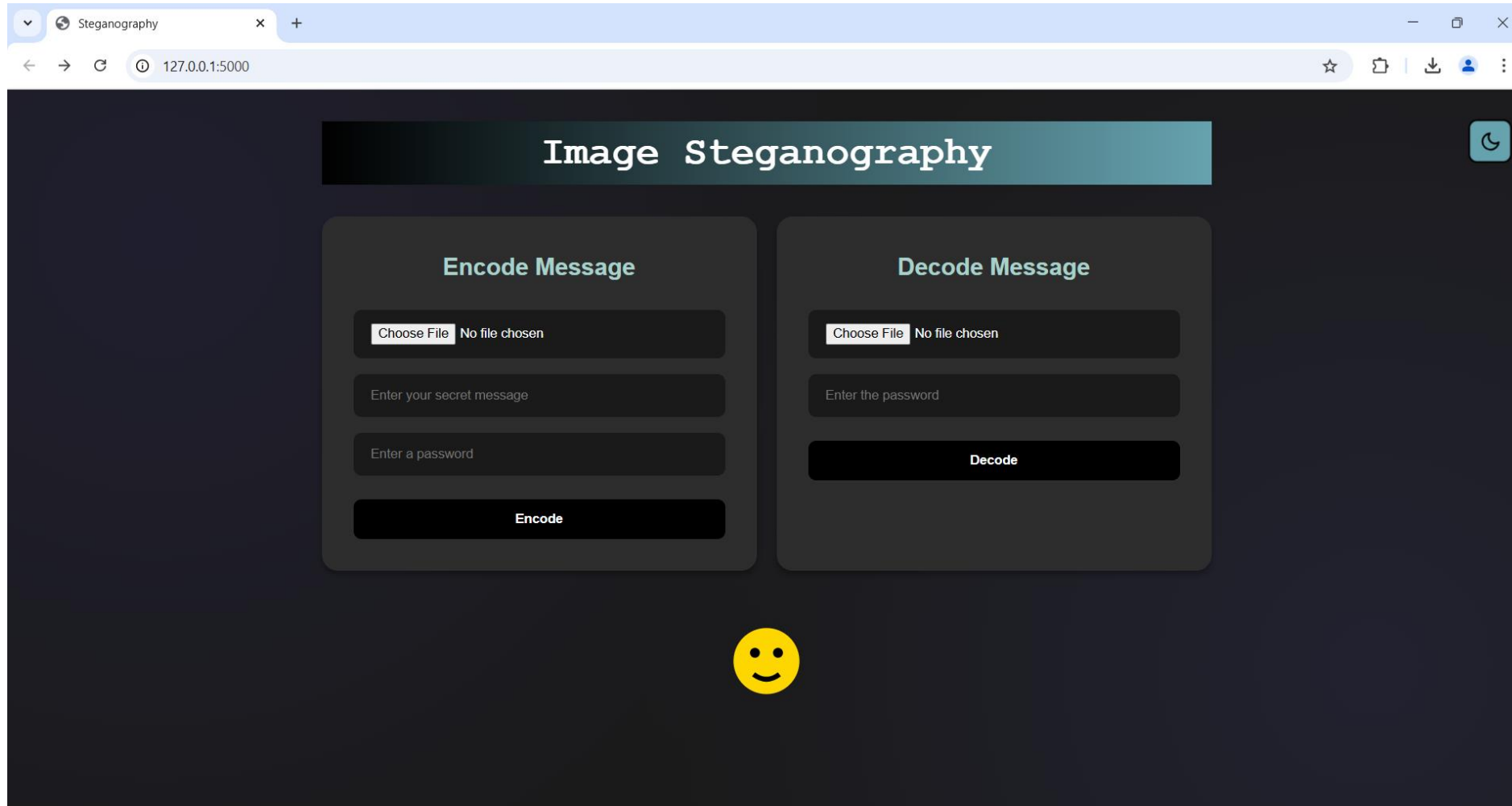
 **Privacy Enthusiasts** – Hide personal notes or data in images

 **Digital Artists** – Conceal copyright information or easter eggs in art

 **Corporations** – Secure internal communication without suspicion

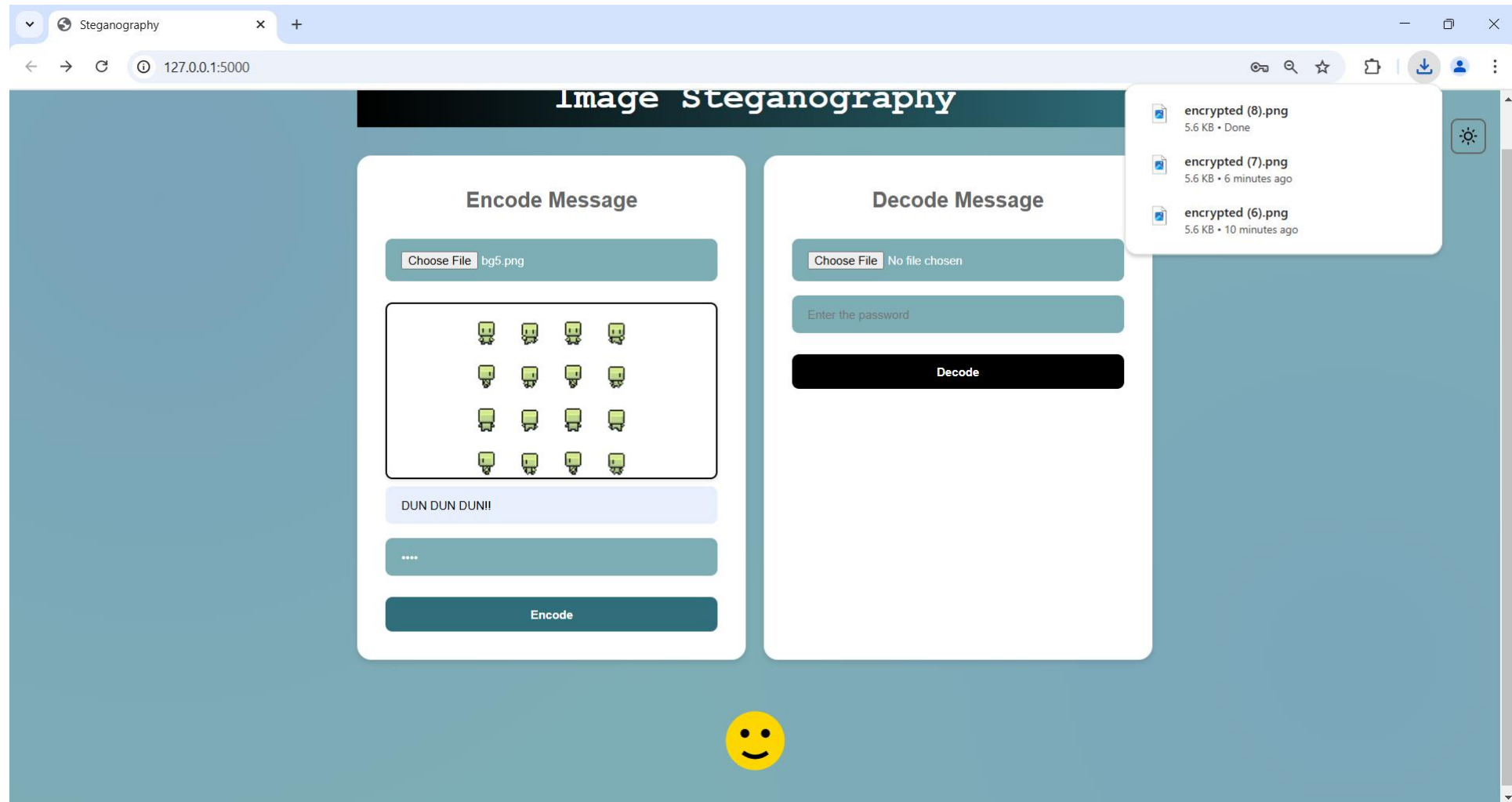
RESULTS

LIGHT/DARK THEME:



The screenshot shows a web browser window with a single tab titled 'Steganography'. The address bar displays '127.0.0.1:5000'. The application interface is dark-themed and features a header 'Image Steganography' with a light blue gradient bar. Below the header, there are two main sections: 'Encode Message' and 'Decode Message'. The 'Encode Message' section contains a file selection button labeled 'Choose File' with the text 'No file chosen' next to it, a text input field labeled 'Enter your secret message', another text input field labeled 'Enter a password', and a large black button labeled 'Encode'. The 'Decode Message' section contains a similar file selection button labeled 'Choose File' with 'No file chosen', a text input field labeled 'Enter the password', and a large black button labeled 'Decode'. At the bottom center of the application area, there is a yellow smiley face emoji. A small light blue icon with a moon symbol is visible in the top right corner of the application area.

ENCODE:



DECODE:

Steganography

127.0.0.1:5000

Image Steganography

Encode Message

Choose File

bg5.png

DUN DUN DUN!!

....

Encode

Decode Message

Choose File

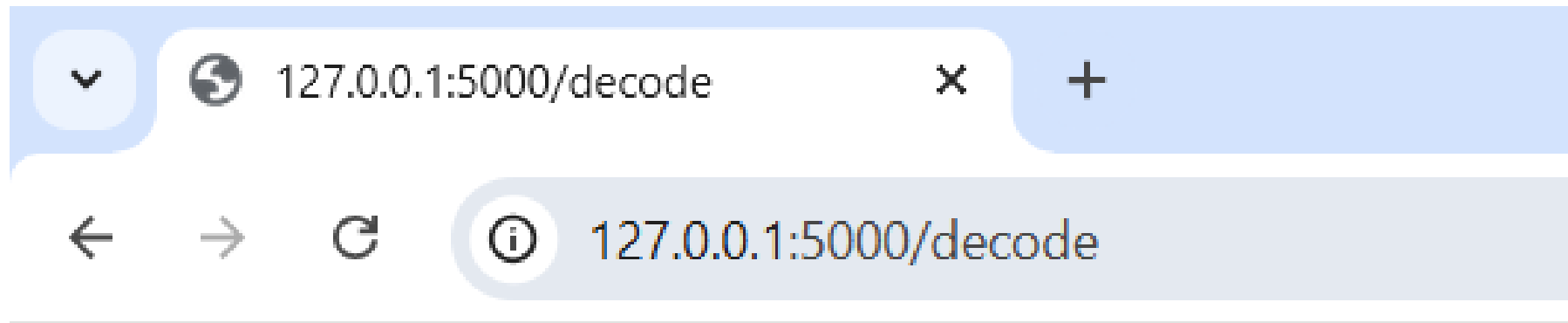
encrypted (8).png

....

Decode

edunet
foundation

OUTPUT:



Decrypted Message: DUN DUN DUN!!

CONCLUSION

- This project provides a modern, intuitive, and secure solution for digital steganography.
- By combining image processing, encryption, and a user-friendly UI, it enhances data security while remaining accessible.
- With future improvements like cloud storage, AI-driven security enhancements, and mobile integration, it can become a mainstream solution for private communication.

LINKS

GitHub Link:

- <https://github.com/AditriRay/Steganography>

Service URL:

- <https://steg-aditri-ibmskillsbuild-999019699834.asia-south1.run.app>

FUTURE SCOPE(OPTIONAL)

- Implement more advanced encryption techniques like AES with steganography.
- Support larger file types beyond images (e.g., audio, video).
- Mobile & Cloud Integration: Develop a mobile app with steganography-based messaging.
- Enable cloud storage for encoded images for remote access.
- AI-Powered Steganography: Use machine learning to adaptively hide messages in different image regions.
- Detect and counter steganalysis techniques that try to crack hidden messages.

CONCEPT:

- A cryptic website where players solve a hidden puzzle by uncovering secret messages embedded in images.
- Players upload images they find throughout the game, and the system decodes hidden clues.
- Some images might require passwords (found through riddles in previous levels).
- Completing a challenge unlocks new encrypted messages or levels.
- Aesthetic: A dark, cyberpunk-themed interface with glowing text and glitch effects.
- Multi-player Mode: Players can hide messages inside images and challenge friends to decrypt them.

THANK YOU!