



www.hexart.in

Enhancing communication security with
imperceptible audio embedding in image

P. M. S. S. Phani Teja
L. Mouli Sai Babu

HEXART.IN INNOVATION COHORT PROGRAM

Image Steganography: Hiding Audio Data in Images

ABSTRACT

In a world where securing sensitive data is paramount, traditional encryption methods can raise suspicion and cloud storage introduces vulnerability.

- Our project explores a covert solution: hiding audio files within seemingly innocent image files using image steganography.
- Our objective is to demonstrate the effectiveness of image steganography for secure and discreet audio transmission.
- This project's findings will not only contribute to developing robust and reliable steganographic methods but also illuminate potential applications of this intriguing technique in real-world scenarios.

Hiding audio files within
seemingly innocent
image files

Demonstrate the
effectiveness for secure
and discreet audio
transmission

INTRODUCTION

In the realm of secure data transmission and covert communication, there is a growing need for innovative techniques that go beyond traditional encryption methods.

- This project aims to explore and develop an advanced image steganography solution capable of concealing images within audio files for secure and discreet information exchange.

Objective

- Image steganography for covert audio transmission - designing and implementing an image steganography system that seamlessly embeds audio files into images, ensuring imperceptibility of the hidden content while maintaining robustness against detection.

MOTIVATION

Audio Embedding for Environmental Data:

Utilizes the auditory spectrum to embed environmental information covertly, ensuring secure transmission.

Benefits of Combining Audio and Image Steganography:

Enhances data security by leveraging both visual and auditory domains, providing a robust and multifaceted covert communication approach.

Environmental Impact of Secure Communication Methods:

Promotes sustainable practices in data transmission, minimizing ecological footprint while safeguarding sensitive environmental information.

POTENTIAL CHALLENGES

Traditional Data Transmission:

- Bandwidth limitations, interception risks, and data corruption challenges.

Secure Communication Importance:

- Safeguarding sensitive environmental data is crucial.
- Covert communication prevents unauthorized access, ensuring data integrity.

Resource Efficiency:

- Efficient utilization of resources is essential in environmental monitoring.
- Secure communication methods optimize resource allocation and reduce wastage.

OTHER ASPECTS

ECO-FRIENDLY ASPECTS	SECURITY AND PRIVACY CONSIDERATIONS
Eco-Friendly Discussion: Audio embedding in image steganography minimizes environmental impact by optimizing data transmission methods.	Concerns Addressed: Ensures secure transmission of sensitive environmental data to prevent unauthorized access.
Comparisons with Traditional Methods: Reduced energy consumption and lower electronic waste compared to resource-intensive traditional transmission methods.	Privacy Preservation: Incorporates measures to protect the privacy of individuals and organizations involved in environmental monitoring.
Sustainable Practices: Aligns with global efforts for eco-friendly technologies in information security.	Security Measures: Integration of encryption techniques to fortify data against potential threats.

OTHER ASPECTS

CHALLENGES AND LIMITATIONS	ONGOING RESEARCH AND IMPROVEMENTS
Challenges Faced: Limited capacity for data storage within images may restrict the amount of embedded audio information.	Continuous Research: Ongoing efforts to address challenges and enhance the efficiency of audio embedding in image steganography.
Detection Risks: Developing countermeasures for potential detection of steganographic techniques.	Advancements in Techniques: Exploration of innovative methods for improved concealment and increased data capacity.
Legal and Ethical Concerns: Addressing legal implications and ethical considerations associated with covert communication.	Collaborative Initiatives: Collaboration with researchers and industry experts to overcome existing limitations and contribute to the evolution of steganographic technologies.

EXISTING TECHNIQUES

Least Significant Bit Substitution (LSB)

- LSB substitution is a technique used in image steganography to hide secret messages within an image.
- It involves replacing the least significant bits (LSBs) of each pixel with a secret message, making it difficult to detect without knowledge of the technique.

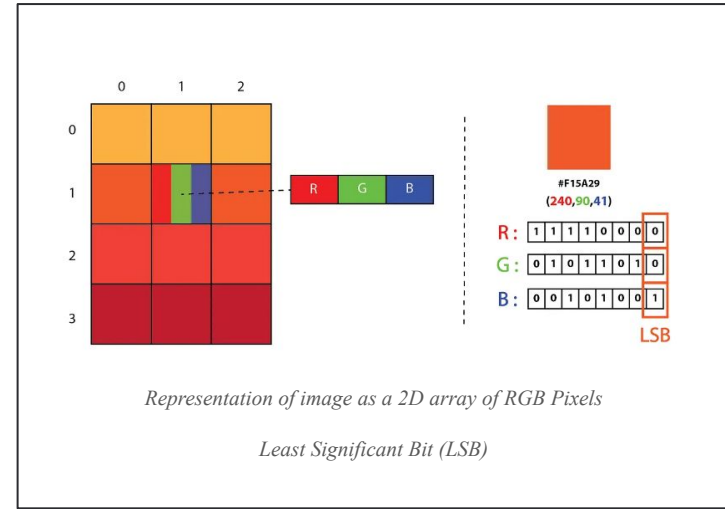
Steganography in Noise

- Image steganography in noise involves embedding information within the subtle variations of noise in digital images.
- By exploiting imperceptible changes in noise patterns, this technique enables covert communication without visibly altering the image itself.

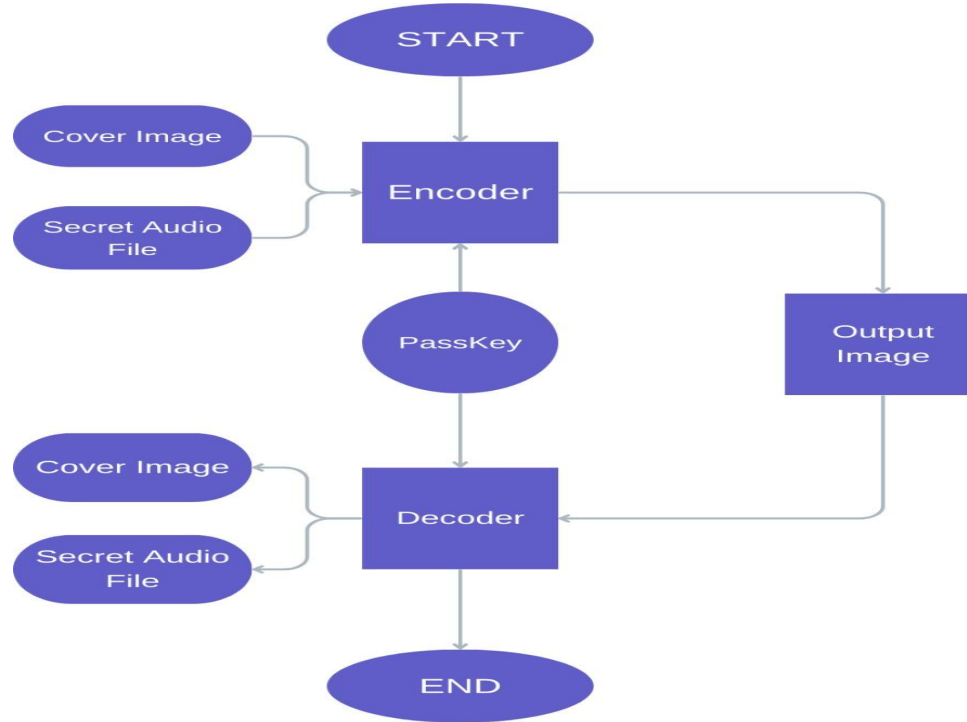
PROPOSED SYSTEM

The proposed system utilizes the Least Significant Bit (LSB) technique for audio steganography in images.

- This technique involves converting the audio data into binary bits and then embedding these bits into the least significant bits of the image. By replacing the least significant bits of the image with the audio bits, the audio can be effectively hidden within the image.
- This approach enables the secure and covert transmission of audio data within images, making it suitable for various applications requiring data hiding and transmission security.



WORKFLOW



INTEGRATION OF AUDIO AND IMAGE STEGANOGRAPHY

Step 1 : Audio Encoding

- Convert audio message into a suitable format (e.g., binary).

Step 2 : Image Selection

- Choose an image as the carrier for embedding audio data.

Step 3 : Pixel Modification

- Modify selected image pixels to encode audio information (e.g., LSB substitution).

Step 4 : Combined Output

- Obtain a hybrid image with embedded audio, visually indistinguishable from the original.

Step 5 : Extraction

- Decode audio from the hybrid image to retrieve the original message.

TECH STACK

- Python
- Pillow
- Numpy
- Scipy

APPLICATIONS

Security &
Confidentiality

Digital
Forensics

Data
Hiding

Digital
Watermarking

CONCLUSION

Key Points Recap:

- Audio embedding in image steganography provides a dual-layered approach to secure communication in environmental monitoring.
- Challenges include limited data capacity, quality preservation, and legal/ethical considerations.
- Ongoing research aims to overcome limitations and advance steganographic techniques.

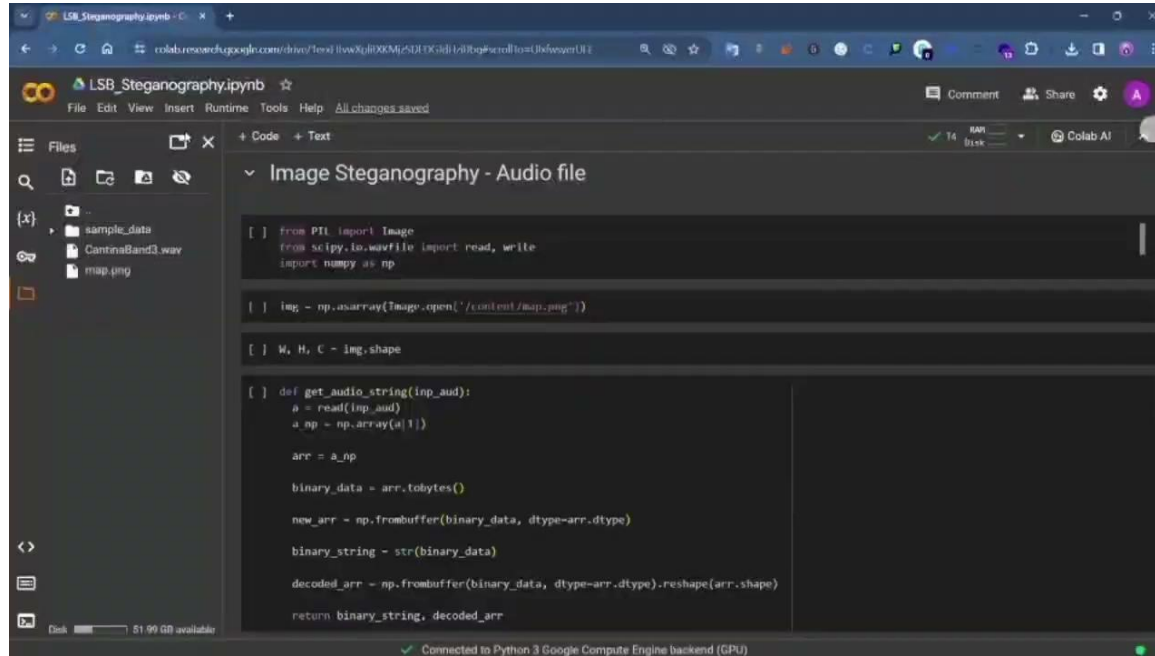
Emphasis on Eco-Friendly Data Transmission:

- Integration of audio embedding aligns with eco-friendly practices, reducing electronic waste and energy consumption compared to traditional methods.
- Promotes sustainability in data transmission, contributing to a greener approach in environmental monitoring.

FINAL THOUGHTS

The fusion of security, covert communication and eco-friendly practices in audio embedding showcases a promising avenue for the future of environmental data transmission.

OUTCOME



The screenshot shows a Google Colab notebook interface. The browser address bar displays a URL from colab.research.google.com. The notebook title is 'LSB_Steganography.ipynb'. The left sidebar shows a file explorer with a folder 'sample_data' containing 'CantinaBand3.wav' and 'map.png'. The main code area is titled 'Image Steganography - Audio file' and contains the following Python code:

```
[ ] from PIL import Image
    from scipy.io.wavfile import read, write
    import numpy as np

[ ] img = np.asarray(Image.open('/content/map.png'))

[ ] W, H, C = img.shape

[ ] def get_audio_string(inp_aud):
    a = read(inp_aud)
    a_np = np.array(a[1])

    arr = a_np

    binary_data = arr.tobytes()

    new_arr = np.frombuffer(binary_data, dtype=arr.dtype)

    binary_string = str(binary_data)

    decoded_arr = np.frombuffer(binary_data, dtype=arr.dtype).reshape(arr.shape)

    return binary_string, decoded_arr
```

At the bottom of the notebook, a status bar indicates 'Connected to Python 3 Google Compute Engine backend (GPU)'.

Thank You

Hexart.In...an opportunity like never before!



Sponsor



Implementation Partner



CSR Partner