Audio Steganography with AES Encryption for Confidential Communication

AGENDA

- Abstract
- Introduction
- Literature Review
- Problem Statement
- Objectives
- Proposed Methodology
- Applications
- Results and Discussion
- Conclusion
- Future Enhancements
- References

ABSTRACT

- Cryptography secures information using mathematical algorithms.
- Steganography hides data within multimedia files like images, audio, and video.
- Audio steganography combined with AES encryption enhances security in digital communication.
- AES ensures cryptographic protection by converting data into an unreadable form.
- The encrypted data is embedded in audio using Least Significant Bit (LSB) techniques.
- This approach provides both confidentiality of information and imperceptibility within audio signals.

INTRODUCTION

- Steganography is the technique of hiding secret information within a non-secret medium in such a way that its presence remains undetectable.
- AES is a widely used symmetric encryption algorithm that secures data by converting it into an unreadable form using a secret key, ensuring confidentiality and protection against unauthorized access.
- AES provides strong encryption, while steganography conceals the existence of the message.
- Audio steganography conceals information within sound files without noticeable distortion.
- The integration of encryption and steganography creates a robust method for confidential communication.

LITERATURE REVIEW

- Existing works explore image-based steganography with various algorithms.
- Audio steganography methods include LSB modification, echo hiding, and phase coding.
- AES is widely used due to its efficiency and strong resistance to attacks.
- Few works combine AES with audio steganography for secure communication.

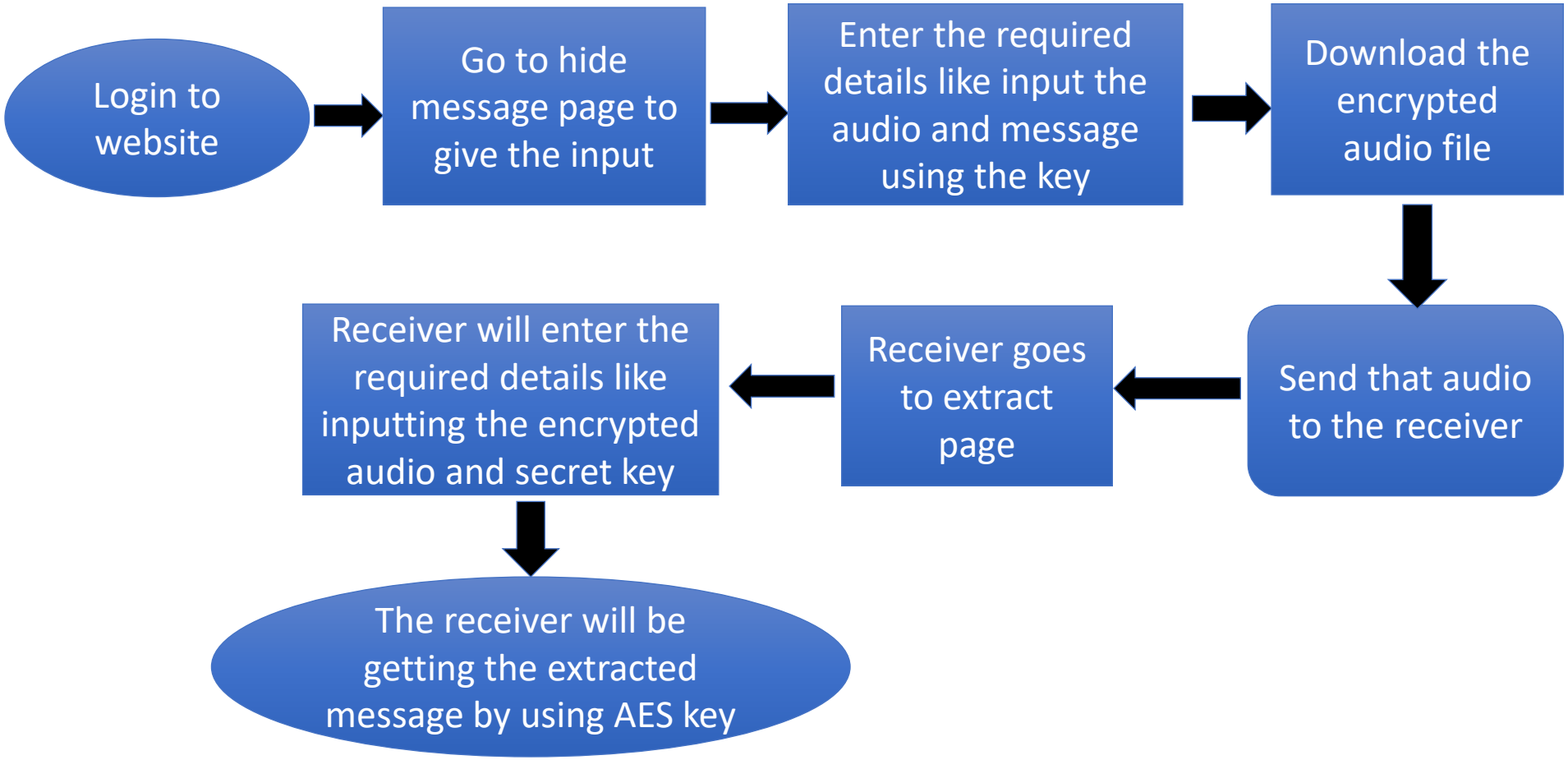
PROBLEM STATEMENT

- Traditional cryptography alone makes data visible as ciphertext.
- Steganography without encryption is vulnerable if detected.
- There is a need for a dual-layer security mechanism.
- Proposed system integrates AES with audio steganography for stronger confidentiality.

OBJECTIVES OF THE CAPSTONE PROJECT

- To design a secure system for embedding secret messages in audio files.
- To use AES encryption for protecting message confidentiality.
- To evaluate robustness against steganalysis attacks.
- To ensure minimal distortion in audio quality.

PROPOSED METHODOLOGY – ARCHITECTURE



APPLICATIONS OF THE RESEARCH

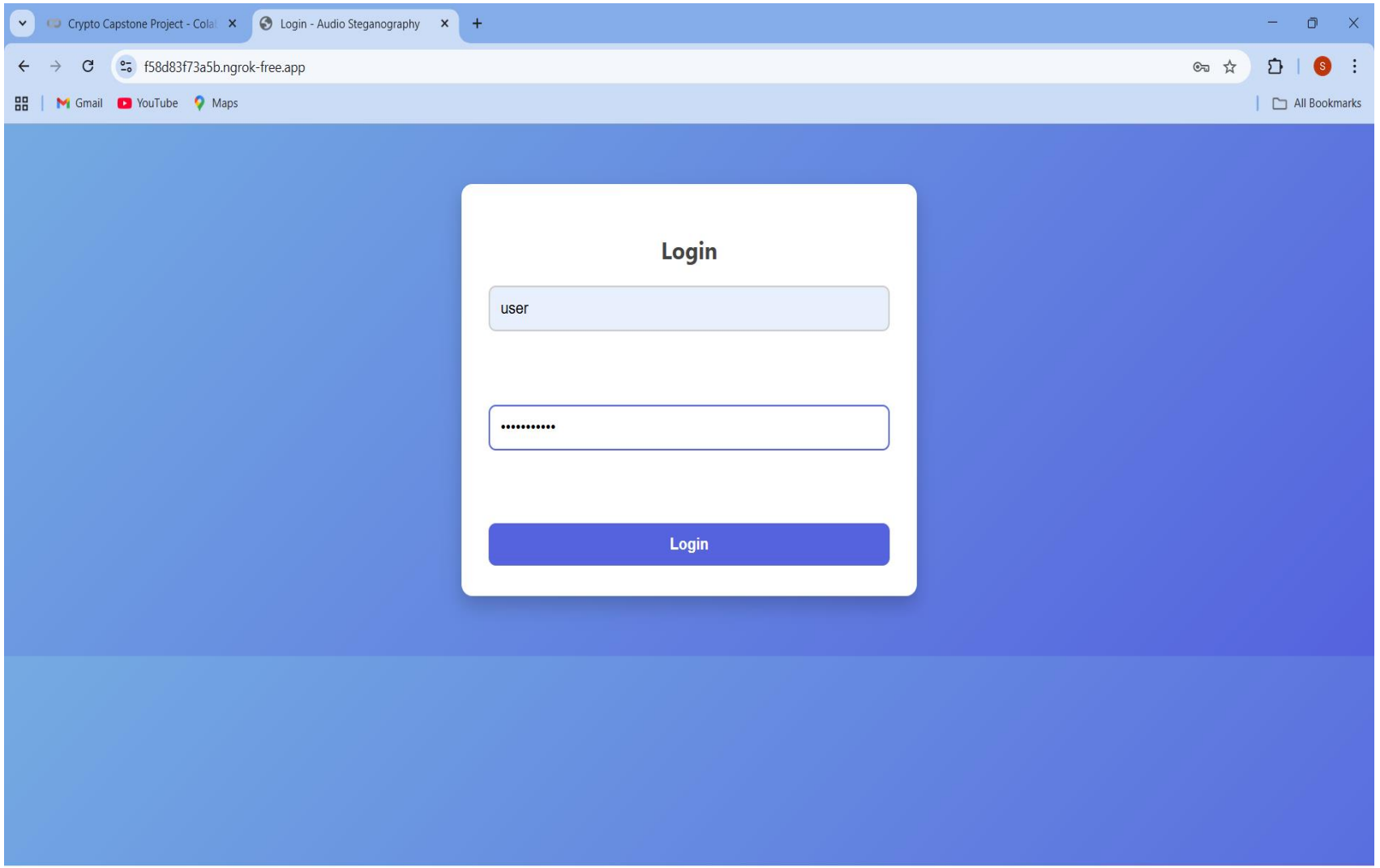
- Secure military and intelligence communications.
- Confidential corporate data exchange.
- Digital watermarking and copyright protection.
- Personal secure messaging applications.

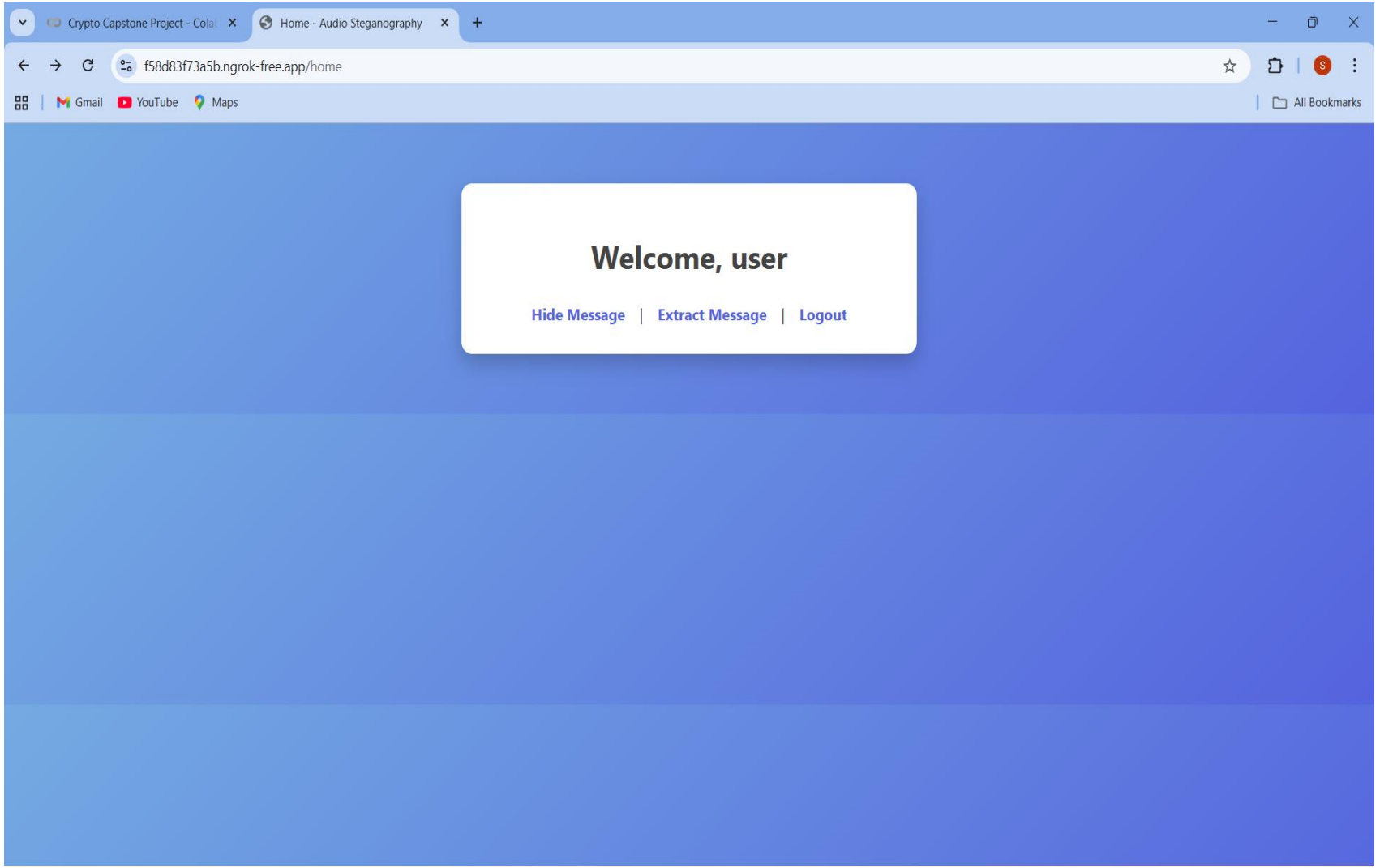
DESCRIPTION ABOUT THE DATASETS USED

- Publicly available audio samples used for embedding.
- WAV format files selected for lossless quality.
- No external dataset required for AES encryption process.
- Dataset size: Approx. 10–20 audio clips for testing.

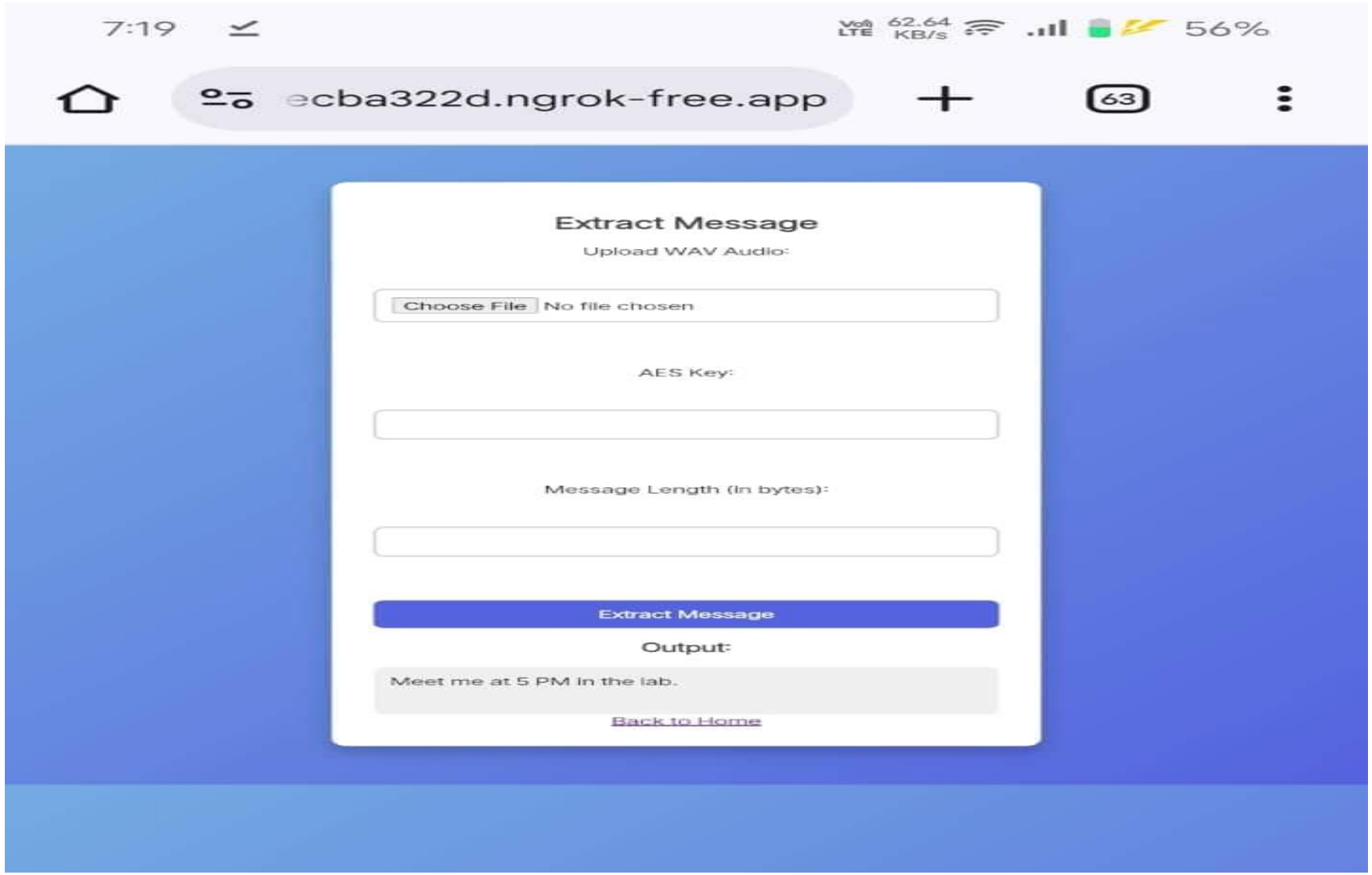
STEPS OF PROPOSED METHODOLOGY

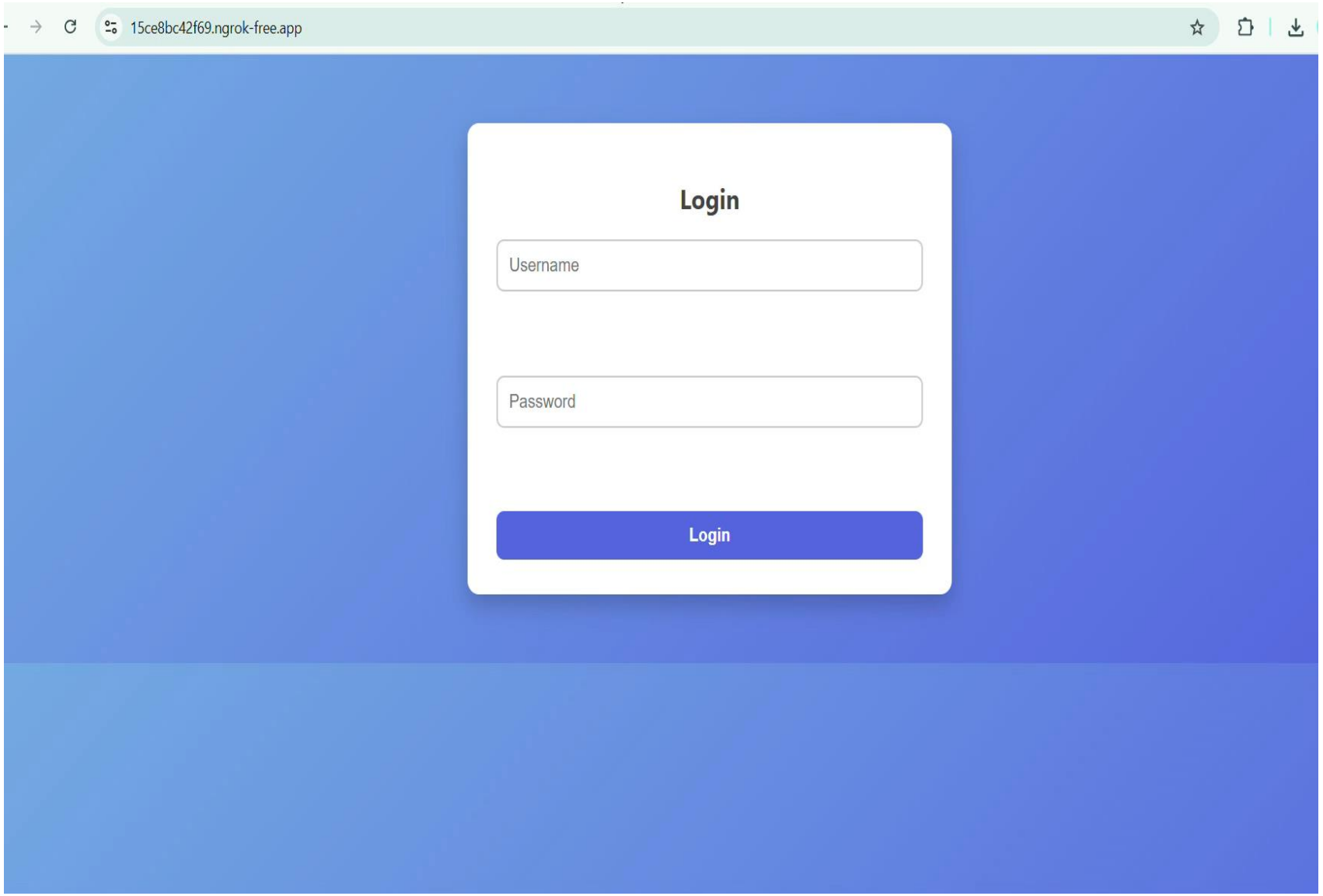
- Input plaintext message.
- Encrypt message using AES key.
- Embed encrypted data into audio file (LSB technique).
- Transmit stego-audio file.
- Receiver extracts encrypted message.
- Decrypt message using AES to obtain original plaintext.


Crypto Capstone Project - Colal
Login - Audio Steganography
f58d83f73a5b.ngrok-free.app
Gmail
YouTube
Maps
All Bookmarks
Login
user
Login


Crypto Capstone Project - Cola
Home - Audio Steganography
f58d83f73a5b.ngrok-free.app/home
Gmail
YouTube
Maps
All Bookmarks
Welcome, user
Hide Message | Extract Message | Logout


Hide Message
Upload WAV Audio:
Choose File
Pushpa Pushpa.wav
Message:
Meet me at 5 PM in the lab.
AES Key:
secretkey123
Hide Message
Back to Home


7:19
62.64 KB/s
56%
ecba322d.ngrok-free.app
63
Extract Message
Upload WAV Audio:
Choose File
No file chosen
AES Key:
Message Length (in bytes):
Extract Message
Output:
Meet me at 5 PM in the lab.
Back to Home


15ce8bc42f69.ngrok-free.app
Login
Username
Password
Login

RESULTS AND DISCUSSION

- Proposed method successfully embedded and retrieved secret messages.
- Audio quality maintained with negligible distortion.
- AES encryption ensured confidentiality even if hidden message is extracted.
- Performance evaluated with PSNR and MSE metrics.

COMPARISON AND ANALYSIS

- Compared with traditional cryptography-only approaches.
- Compared with image-based steganography.
- Our system shows improved confidentiality and imperceptibility.
- AES integration increases resilience against brute-force attacks.

CONCLUSION

- The system ensures highly confidential communication.
- AES provides strong encryption for sensitive data.
- Audio steganography conceals the presence of data.
- Combined approach enhances multimedia security.

FUTURE ENHANCEMENTS

- Extend method to video and image files.
- Use advanced steganography methods like phase coding.
- Optimize AES for faster performance in real-time communication.
- Develop mobile and web applications for secure communication.

REFERENCES

- William Stallings, Cryptography and Network Security.
- Research papers on AES and audio steganography.
- IEEE journals on multimedia security.
- Online resources for steganography techniques.

THANK YOU