STEGANOGRAPHY

Project Advisor:

Dr.Salwa Osama

What is steganography?

Steganography is the practice of hiding information within other, non-secret, information or files, so that the hidden data is not apparent to someone who casually observes the carrier file. Unlike encryption, where the presence of a secret message is obvious (though the content is hidden), steganography conceals the fact that any message is present at all.

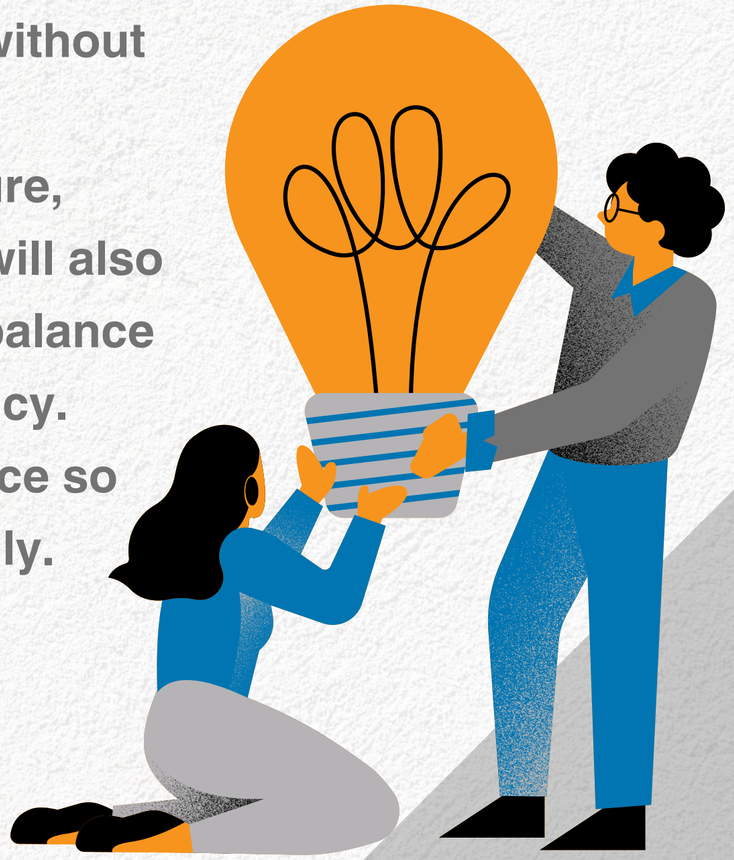
“steganography means hiding one peace of data within another”

Importance of stegnoghraphy in real words

- Securing Sensitive Information
  - Covert Communication
  - Preventing Detection
- Digital Rights Management
  - Copyright Protection
- Data Integrity
  - Tamper Detection:
- Military and Intelligence Operations
  - Classified Communication
- Secure Data Storage
  - Embedding in Media Files
- Preventing Censorship
  - Circumventing Restrictions

Objective

- Our project aims to create a system that can hide and extract messages in images and audio without affecting their quality. We will use efficient algorithms to ensure the hidden data is secure, hard to detect, and resistant to attacks. We will also compare different methods to find the best balance between data capacity, security, and efficiency. Finally, we will design an easy-to-use interface so anyone can hide and retrieve messages easily.



History of Steganography

Steganography has a long history, evolving from ancient techniques to sophisticated digital methods

- Ancient Times
  - Greek Wax Tablets: Messages were inscribed on wood and covered with wax, giving the appearance of a blank tablet.
  - Body Tattoos: Hidden messages were tattooed on messengers' shaved heads and concealed as the hair grew back.
  - Herodotus' Accounts: Documented innovative uses of steganography during wars.

History of Steganography

Steganography has a long history, evolving from ancient techniques to sophisticated digital methods

- Middle Ages
  - Invisible Ink: Natural substances like lemon juice or milk were used to write messages visible only under heat.
  - Secret Symbols: Hidden messages were embedded in religious texts, artworks, and everyday items.

History of Steganography

Steganography has a long history, evolving from ancient techniques to sophisticated digital methods

- Renaissance Era
  - Advanced Concealment: Steganography grew more sophisticated, with messages hidden in music scores or paintings.
  - Scientific Exploration: Scholars experimented with more reliable and complex methods.

History of Steganography

Steganography has a long history, evolving from ancient techniques to sophisticated digital methods

- Modern Era
  - World Wars: Steganography played a vital role in espionage, using techniques like microdots to conceal information.
  - Digital Steganography: With the advent of computers, data hiding evolved into embedding information in images, audio, and videos using techniques like the Least Significant Bit (LSB) method.

History of Steganography

Steganography has a long history, evolving from ancient techniques to sophisticated digital methods

- Contemporary Use
  - Steganography is now widely used in cybersecurity, digital watermarking, and covert communication. It works alongside cryptography to enhance data security and integrity.

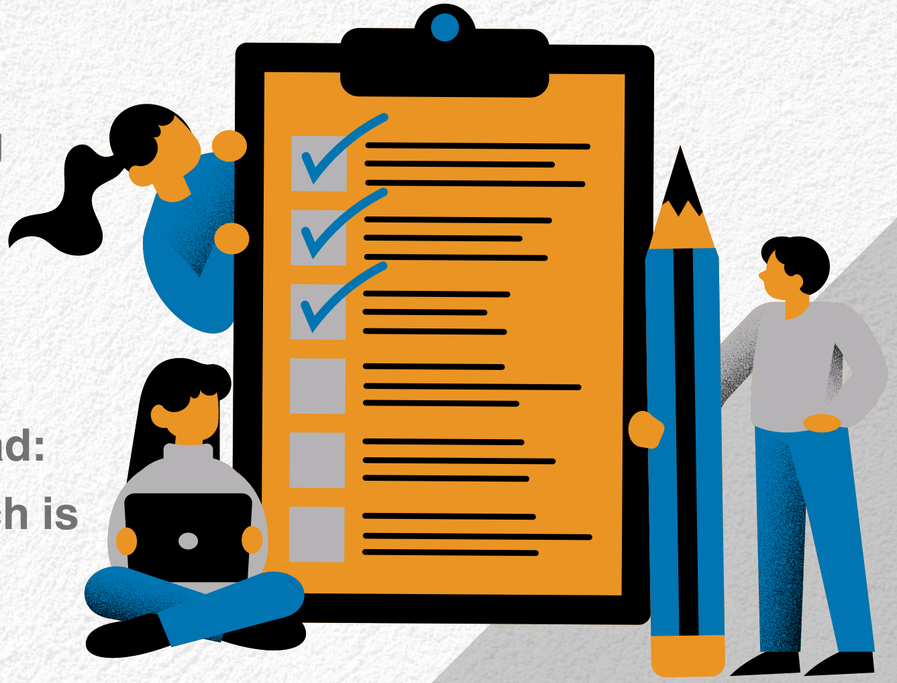
Steganography vs Cryptography

- unknown message passing
- little known technology
- technology still being develop for certain formats
- steganography does not alter the structure of the secret message

- known message passing
- common technology
- most of algorithms known by all
- cryptography alter the structure of the secret data

Steganography terms

- carrier or cover file: an original message or a file in which hidden information will be stored inside of it
- stego-medium: the medium in which the information is hidden
- steganalysis: the process of detecting hidden information inside a file.
- embedded or payload: the information which is to be hidden or concealed



Types of steganography

01

PURE STEGANOGRAPHY

02

TEXT STEGANOGRAPHY

03

IMAGE STEGANOGRAPHY

04

AUDIO STEGANOGRAPHY

Pure Steganography

Does not require the exchange of secret information before sending a message, relying solely on secrecy for security. It is defined by a quadruple (C, M, D, E), where C is the set of possible covers, M is the set of secret messages, and E is the embedding function. The extraction function D ensures that the hidden message can be retrieved from the cover.

While Pure Steganography is preferred for its simplicity and lack of stego-key exchange, it offers no security if the embedding method is known to attackers.

Text Steganography

Involves hiding secret messages within text documents without altering the document's visible appearance. This technique uses various methods such as modifying whitespace, altering characters' case, or embedding messages in seemingly random data.

Text steganography is often used to transmit covert information through seemingly innocent or routine communications, making detection difficult. It relies on the fact that the human eye may not detect subtle changes in text, especially in large volumes of data. Advanced techniques may use natural language processing to hide messages in grammatically correct sentences.

Image Steganography

Involves hiding secret data within an image file without altering itsvisual appearance significantly. This technique is used to securely transmit hidden information, such as text or another image, within the pixels of an image. The process typically involves encoding the secret data into the least significant bits of the pixel values. The recipient can extract the hidden information using the same steganographic algorithm and a secret key or password.

Image steganography is commonly used for secure communication and watermarking.

Audio Steganography

Technique used to hide secret information within audio files. It involves embedding the secret data into the audio signal in a way that is imperceptible to human listeners. This can be achieved by modifying certain properties of the audio signal, such as amplitude or frequency, to encode the hidden information. The process of embedding the data is typically reversible, allowing the hidden information to be extracted later.

Audio steganography is often used for covert communication or for watermarking audio files to protect intellectual property.

Techniques of Steganography

1) Text Steganography

Line-Shift Coding:

- **This method involves vertically shifting the positions of text lines within a document to encode information uniquely. Decoding may be done from either the format file or the bitmap image, particularly feasible when the original image has uniform line spacing.**

Techniques of Steganography

1) Text Steganography

Word-Shift Coding:

- **In this technique, the positions of words within text lines are horizontally shifted to encode the document uniquely. Decoding can be performed from the format file or the bitmap image, but the original image is necessary due to variable spacing between words, commonly used for text justification.**

Techniques of Steganography

1) Text Steganography

Feature Coding:

- **This approach alters selected text features within a document, such as vertical endlines (tops of letters like b, d, h, etc.), based on codewords. Decoding requires the original image, specifically noting changes in pixel dimensions at a given feature point.**

Techniques of Steganography

2) Image Steganography

Least Significant Bit (LSB) Embedding:

- **This straightforward approach involves embedding bits of a message directly into the least significant bit plane of the cover image. Since the changes are minimal and imperceptible to the human eye, LSB modification ensures effective hiding of information within the image. It's crucial to use lossless compression formats to prevent loss of hidden data during transformations.**

Techniques of Steganography

2) Image Steganography

Masking and Filtering:

- **Masking and filtering methods are commonly applied to 24-bit and grayscale images. They operate akin to watermarking physical paper, serving as digital counterparts. Masking involves altering the brightness of the masked portion. The smaller the change in brightness, the lower the likelihood of detection. While these methods may subtly change the image's visible properties, they are less susceptible to compression and other image processing compared to LSB modification.**

Techniques of Steganography

2) Image Steganography

Discrete Cosine Transformations (DCT):

- **More complex than LSB embedding, this method involves modifying discrete transformations used cosine in JPEG compression. By manipulating DCT coefficients, data can be concealed within the image. This approach provides robust hiding capabilities, particularly suitable for images compressed using lossy algorithms like JPEG.**

Techniques of Steganography

3) Audio Steganography

LSB Coding:

- **In LSB coding, the least significant bit of the binary sequence of each sample in the digitized audio file is replaced with the binary equivalent of the secret message. This technique exploits the fact that small alterations in the least significant bit are imperceptible to human ear**

Techniques of Steganography

3) Audio Steganography

Phase Coding:

- **Phase coding takes advantage of the fact that the Human Auditory System(HAS) is less sensitive to phase changes than to noise in audio signals. Secret message bits are encoded as phase shifts in the phase spectrum of the digital signal, achieving inaudible encoding in terms of signal-to noise ratio.**

Techniques of Steganography

3) Audio Steganography

Spread Spectrum:

- Spread spectrum techniques encompass two approaches: direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS). DSSS multiplies the transmitted signal by a pseudorandom noise sequence, spreading the signal's energy over a wider bandwidth. FHSS, on the other hand, pseudo-randomly returns the carrier frequency, resulting in a uniform frequency distribution.

Techniques of Steganography

3) Audio Steganography

Echo Hiding:

- **Echo hiding involves embedding the secret message as an echo within the cover audio signal. Parameters such as amplitude, decay rate, and offset from the original signal are adjusted to represent the encoded binary message, ensuring that the echo remains below the threshold of human auditory perception**

Factor Affecting Steganography

- Capacity refers to the total number of bits successfully hidden and recovered by the steganographic system.

- Robustness: Robustness denotes the ability of embedded data to remain intact despite transformations undergone by the stego-system, such as filtering, noise addition, and compression.

- Undetectable: An algorithm is considered undetectable if the image with the embedded message aligns with the source model, without making statistical changes to the carrier's noise component.

Factor Affecting Steganography

- **Invisibility (Perceptual Transparency): Invisibility relies on properties of the human visual or audio system. Embedded information should be imperceptible to an average observer, without significant degradation in perceptual quality.**

- **Security: Security entails ensuring embedded information remains resistant to removal after discovery by an attacker, relying on the secrecy of the algorithm and the secret key.**

Steganography Algorithms

1) Spatial Domain

- LSB (Least Significant Bit):
  - Capacity: High
  - Security: Low
  - Complexity: Simple
  - Resistance to Changes: Weak
  - Best Use Case: Quick data hiding in images.
- Pixel Value Differencing:
  - Capacity: Moderate
  - Security: Moderate
  - Complexity: Simple to Moderate
  - Resistance to Changes: Moderate
  - Best Use Case: Subtle embedding in image edges.

Steganography Algorithms

1) Spatial Domain

- Edge-based Steganography:
  - Capacity: Moderate
  - Security: Moderate
  - Complexity: Simple to Moderate
  - Resistance to Changes: Moderate
  - Best Use Case: Hiding data in image edge details.

Steganography Algorithms

2)Transform Domain

- Discrete Cosine Transform:
  - Capacity: Moderate
  - Security: High
  - Complexity: Moderate to Complex
  - Resistance to Changes: Strong
  - Best Use Case: Image/audio with frequent compression
- Discrete Wavelet Transform:
  - Capacity: Moderate
  - Security: High
  - Complexity: Complex
  - Resistance to Changes: Very Strong
  - Best Use Case: Resilient to noise and compression.

Steganography Algorithms

2)Transform Domain

- Singular Value Decomposition:
  - Capacity: Moderate
  - Security: High
  - Complexity: Complex
  - Resistance to Changes: Strong
  - Best Use Case: Robust watermarking applications.
- Fourier Transform:
  - Capacity: Low to Moderate
  - Security: High
  - Complexity: Complex
  - Resistance to Changes: Strong
  - Best Use Case: Signal processing applications.

Steganography Algorithms

3)Cryptographic Embedding

- Encryption-based methods:
  - Capacity:Moderate to High
  - Security:Very High
  - Complexity:Very Complex
  - Resistance to Changes:Very Strong
  - Best Use Case:High-security environments.

Steganography Algorithms

4)Text-based

- Formatting/Encoding:
  - Capacity:Low
  - Security:Low
  - Complexity:Simple
  - Resistance to Changes:Weak
  - Best Use Case:Embedding simple data in text files

Steganography Algorithms

5)Spread Spectrum

- Signal-based methods:
  - Capacity:Low
  - Security:High
  - Complexity:Moderate
  - Resistance to Changes:Very Strong
  - Best Use Case:Audio or noisy data environments.

Steganography Algorithms

6)Model-based

- Statistical modeling:
  - Capacity:Variable
  - Security:High
  - Complexity:Complex
  - Resistance to Changes:Strong
  - Best Use Case:Resistant to statistical detection.

Steganography Algorithms

7)Fractal-based

- Fractal patterns:
  - Capacity:High
  - Security:Moderate
  - Complexity:Complex
  - Resistance to Changes:Moderate
  - Best Use Case:Scalable images or pattern hiding.

Steganography Algorithms

8)AI-based

- GANs and neural networks:
  - Capacity:High
  - Security:Very High
  - Complexity:Very Complex
  - Resistance to Changes:Very Strong
  - Best Use Case:Adaptive methods robust against detection.

Steganography Algorithms

9)Quantum Steganography

- Quantum states:
  - Capacity:Variable
  - Security:Ultra-High
  - Complexity:Very Complex
  - Resistance to Changes:Ultra-Strong
  - Best Use Case:Cutting-edge quantum security

Steganography Algorithms

10)Cover Modification

- Histogram-based:
  - Capacity:Moderate
  - Security:High
  - Complexity:Moderate
  - Resistance to Changes:Strong
  - Best Use Case:Adjusting histograms for secure embedding

Detection of Steganography

Detection of steganography involves looking for patterns or anomalies in the cover media that might indicate hidden information

- **Text Steganography: Detection involves looking for patterns oralterations in the text, such as unusual language usage or excessive white space.**

- **Image Steganography: Statistical analysis can reveal discrepancies or patterns indicating modifications in stego-images, particularly focusing on LSB alterations.**

Detection of Steganography

Techniques such as frequency analysis or detecting statistical anomalies can aid in uncovering hidden messages.

- Audio and Video Steganography: Statistical analysis can be applied to detect LSB modifications in audio files.
- Other detection methods include scanning for high, inaudible frequencies, odd distortions, or patterns in sounds.
- For video steganography, special code signs or gestures may be used, which are difficult to detect with computer systems.

Steganalysis

Steganalysis is the process of detecting steganography by analyzing various parameters of a stego media to determine if it contains a hidden message

- This process involves identifying suspected media, reducing the set of suspected information streams using statistical methods, and employing techniques such as visual detection to identify unusual patterns or degradation in the media.

Steganalysis

Steganalysis is the process of detecting steganography by analyzing various parameters of a stego media to determine if it contains a hidden message

- Steganalysis attacks aim to detect, extract, and destroy hidden objects in stego media, and they can vary based on the information available for analysis, including known carrier attacks, steganography-only attacks, known message attacks, and known steganography attacks.

Steganalysis

Steganalysis is the process of detecting steganography by analyzing various parameters of a stego media to determine if it contains a hidden message

- Steganalysis helps in detecting and stopping the use of steganographic techniques by comparing cover objects, stego objects, and portions of the stego-key.

Future of Steganography

Increased Sophistication:

- Steganographic techniques will become more common and advanced.

Advances in Steganalysis:

- Tools for detection will improve but may lag behind steganographic developments.

Security Threats:

- Malicious software (Trojans, worms, viruses) could be hidden in media files, activated upon viewing or listening.

Enhanced Intrusion Detection Systems (IDS):

- IDS will incorporate steganographic signatures to detect threats in images and audio.

Future of Steganography

Anti-Virus Evolution:

- Antivirus software will develop steganalysis features to scan for hidden threats.

Dual Steganography:

- Combining steganography with cryptography could offer future solutions to security challenges.

Robust Watermarking:

- A strong, tamper-resistant digital watermark may emerge as a key innovation.

OUR PROJECT

Introduction to the Project

- **Goal: To develop a user-friendly tool that embeds and extracts hidden messages in images using advanced steganographic methods.**

- **Key Features:**
  - **Supports hiding text in both images and audio.**
  - **Uses *LSB (Least Significant Bit)* for simple embedding.**
  - **Uses *PVD (Pixel Value Differencing)* for higher security and imperceptibility.**

- **Objective:**
  - **To develop a steganography tool that securely hides and extracts secret messages in images and audio.**
  - **Focus on balancing imperceptibility, data capacity, and usability.**

Techniques Used

Image Steganography

- LSB (Least Significant Bit):
  - Embeds secret data by replacing the least significant bits of pixel values.
- Why LSB
  - Simple and efficient.
  - Minimal visual changes.
- Limitation:
  - Less secure for sensitive data due to vulnerability to steganalysis.

Techniques Used

Image Steganography

- PVD (Pixel Value Differencing):
  - Hides data by analyzing the difference between adjacent pixel values.
- Why PVD
  - Embeds more data in high-contrast areas.
  - Maintains better image quality compared to LSB..
- Advantage:
  - Higher capacity and imperceptibility than LSB.

Techniques Used

Audio Steganography

- LSB (Least Significant Bit):
  - Embeds data by modifying the least significant bits of audio samples..
- Why LSB
  - Quick and efficient for small-sized data.
  - Inaudible changes to audio quality.

Techniques Used

Audio Steganography

- LSB (Least Significant Bit):
  - Embeds data by modifying the least significant bits of audio samples..
- Why LSB
  - Quick and efficient for small-sized data.
  - Inaudible changes to audio quality.

Implementation Overview

Features

- Graphical User Interface (GUI)* for user-friendly interaction using tkinter
- Separate tabs for:
  - Hide: Embed secret messages.
  - Unhide: Extract hidden messages..

- File Format Support:
  - Image: .png, .jpg, .jpeg, .bmp
  - Audio: .wav, .mp3

Workflow

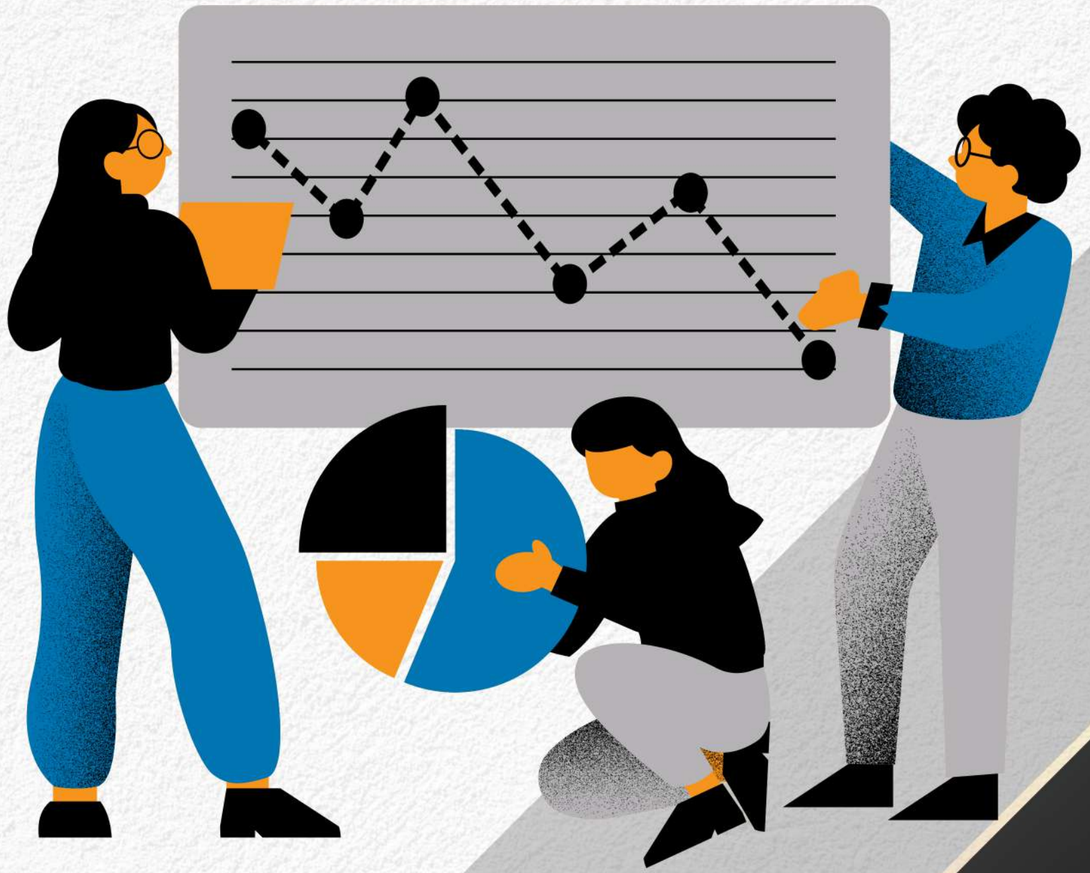
- Hide:
  - User uploads an image or audio file.
  - Enters a secret message.
  - Selects the output file location.
  - The tool processes the file using the selected steganography technique.

- Unhide:
  - User uploads a stego file.
  - The tool extracts and displays the hidden message.

Results and Analysis

- Image Results:
  - LSB: Minimal quality loss, suitable for small messages.
  - PVD: Higher capacity and better quality retention, ideal for larger messages.

- Audio Results:
  - LSB: Data embedding has negligible impact on audio quality, ensuring inaudibility.



Challenges and Solutions

- Challenge:
  - Maintaining balance between capacity and imperceptibility.
- Solution:
  - Used PVD for higher data capacity with minimal visual artifacts.

- Challenge:
  - Simplifying user interaction.
- Solution:
  - Designed a GUI for seamless navigation and functionality.

Conclusion

- Your project successfully demonstrates the potential of *LSB* and *PVD* techniques in image steganography and *LSB* in audio steganography for secure and efficient data hiding.
- The combination of advanced techniques and a user-friendly GUI makes it a practical tool for multimedia steganography.

Future Scope

- Focus on Images and Audio: Avoid exploring video steganography and instead refine and expand techniques for image and audio steganography.
- Detection Tab Addition: Add a detection tab to identify steganographic content for testing and evaluation purposes.
- Adaptive Techniques with Machine Learning: Implement adaptive steganography techniques powered by machine learning to improve robustness and efficiency.

THANK YOU