Steganoography PROJECT

Presented By

1. Student Name: Mahanthi Sowmya
2.College Name: KIET
3.Department: AI&DS

FINAL PROJECT

concepts:

- Introduction
- Features
- Advantages
- Disadvantages
- Purpose
- Image

::text hiding in an image using steganography::

Introduction

In text steganography, secret message is embedded into cover text using word mapping method. For image steganography, secret message is hided into cover
image with the help of stego key through the LSB technique using discrete logarithms. This method uses blank-space in the cover-text to embed original message.

Text steganography involves hiding information inside text files.

This includes changing the format of existing text, changing words within a text, using context-free grammars to generate readable texts, or generating random character sequences.steganography the solution uses the art **of** steganography to hide the inside the image

→LSB IN STEGANOGRAPHY

The most famous steganographic approach is the least significant bit (LSB) where LSB refers to the last or the right-most bit in a binary number. This approach replaces some LSBs of the cover image with the secret data bits of the hidden message. LSB is easy and simple in computations but the capacity is low.The two ways of LSB steganography are LSB replacement and LSB matching. The first is the LSB replacement, which is the most basic of the LSB. The end parts of a cover image are replaced with each bit of the message that has to be hidden using LSBreplacement steganography. The two ways of LSB steganography are LSB replacement and LSB matching. The first is the LSB replacement, which is the most basic of the LSB. The end parts of a cover image are replaced with each bit of the message that has to be hidden using LSB replacement steganography.

Types in steganography:

- >>Text steganography
  >>Image steganography
  >>Video steganography
  >>Audio steganography
  >>Network steganography

Basic principle of steganography :

Steganography is the practice of concealing a file, message, image, or video within another file, carrier image, or video. It can be used to hide messages in text, images, and audio files. Common techniques for images involve least significant bit insertion and masking/filtering.

Benefits of steganography :

By hiding information in another file or message, steganography can provide an additional layer of security, protecting data from unauthorized access.

Features :

Image steganography has a high capacity to carry secret information as it can hide a large amount of data within an image.
::Concealment: Steganography is used to conceal the existence of a message.
::Covert communication: Steganography is often used for covert
::Security: Steganography provides an additional layer of security by making it.
::Plausible deniability: Steganography can be used to provide plausible
→Text steganography involves hiding information inside text files.
→ This includes changing the format of existing text, changing words within a text, using context-free grammars to generate readable texts, or generating random character sequences.

Advantages :

Advantages of Steganography	Disadvantages of Steganography
1. Covert communication	1. Potential for misuse (e.g., hiding illegal content)
2. Enhanced security (when used with encryption)	2. Detection challenges (advanced tools can uncover hidden information)
3. Resistance to detection	3. Issues with lossy compression (may affect hidden data)
4. Versatility across digital media	4. Capacity limitations (amount of data that can be hidden is limited)
5. Analog security options	5. Complexity of implementation and decoding
6. Complementary to encryption	

Explanation of the Table:

- Advantages:

- Covert communication: Enables hiding messages within innocent-looking carrier files, maintaining secrecy.
- Enhanced security: Adds an extra layer of security when combined with encryption, making it harder for unauthorized access.
- Resistance to detection: Difficult to detect without prior knowledge or suspicion, enhancing stealth.
- Versatility: Can be applied to various digital formats, accommodating different types of data.
- Analog security options: Historical and modern techniques exist for hiding information physically.
- Complementary to encryption: Provides additional protection by hiding the fact that data is encrypted.

Disadvantages:

- Potential for misuse: Could be used for illicit purposes like hiding illegal content.
- Detection challenges: Advanced detection methods and suspicion can reveal hidden data.
- Lossy compression issues: Compression algorithms may degrade hidden data quality.
- Capacity limitations: Limits on how much data can be effectively hidden within a carrier file.
- Complexity: Implementing and decoding steganographic methods can be challenging and prone to errors.

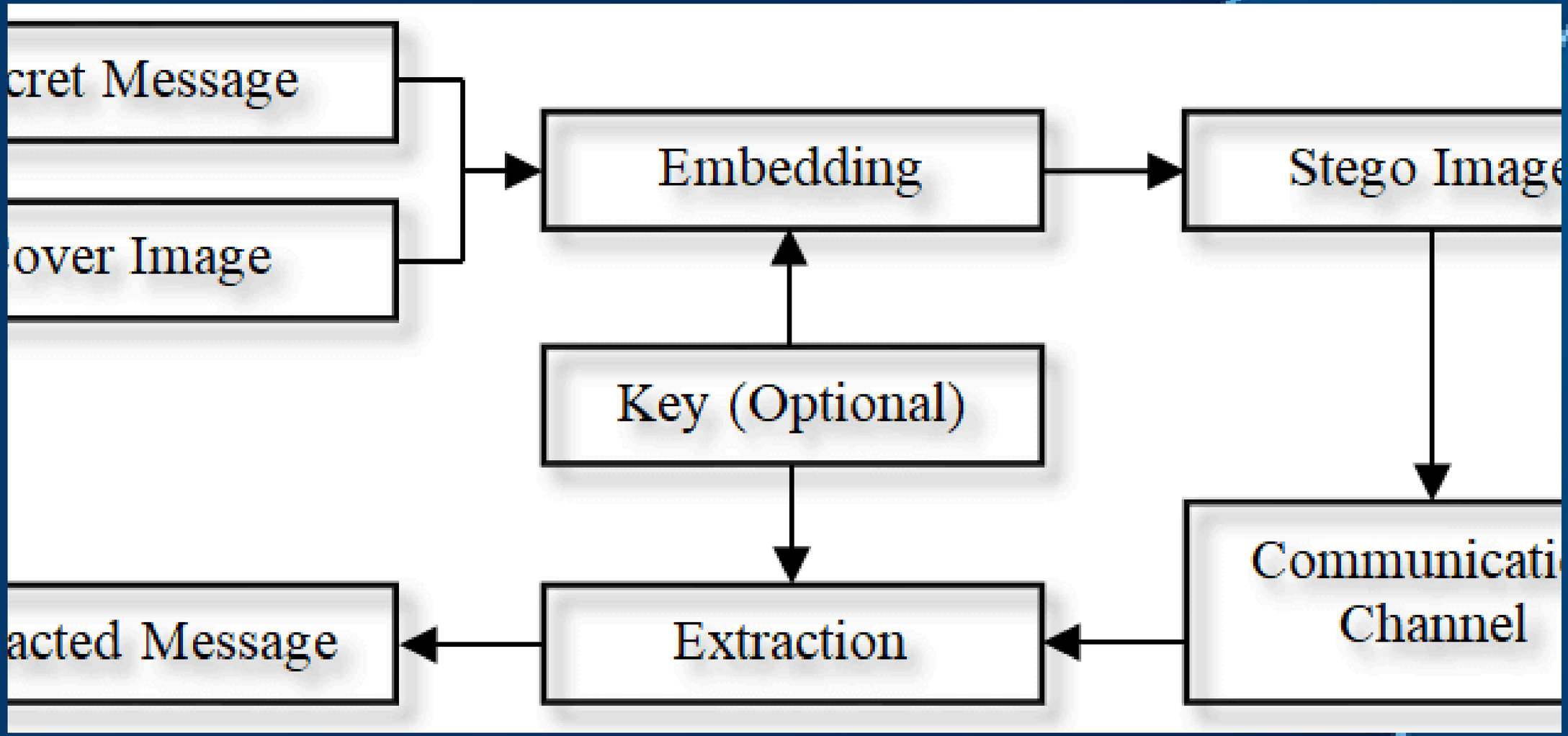
Purpose :

→ Steganography works by concealing information in a way that avoids suspicion.
→ Steganography is the practice of concealing information within another message or physical object to avoid detection.
→ Steganography is the technique of hiding data within an ordinary , nonsecret file or message to avoid detection; the hidden data is then extracted at its destination.
→ Steganography use can be combined with encryption as an extra step for hiding or protecting data.
→ It involves hiding data behind digital images.
→ There are various techniques for image steganography which include the Least Significant Bit technique, Masking and
Filtering, and Coding and Cosine Transformation.
→ Basically, no human on earth can tell the visual difference.Steganography hiding the image :
→ if we change the rightmost bits it will have a small visual impact on the final image.

→ This is the steganography key to hide an image inside
another.

- → Change the least significant bits from an image and include
- the most significant bits from
the other image.

text hidding in an image using steganography



github link:

- https://github.com/Sowmya1431/Stegnography-project

THANK YOU