STEGANOGRAPHY

PRESENTED BY
SHRUTI PATHAK
Roll No.- 002210503021
MCA- 2nd Year 2nd Semester
Session- 2022 - 2024
JADAVPUR UNIVERSITY

OVERVIEW

- What is Steganography?
- History
- Steganography Vs. Cryptography
- Basic steganography model
- Types of steganography
- Steganalysis
- Uses of Steganography
- Advantages
- Limitation
- Future Scope
- Conclusion
- References

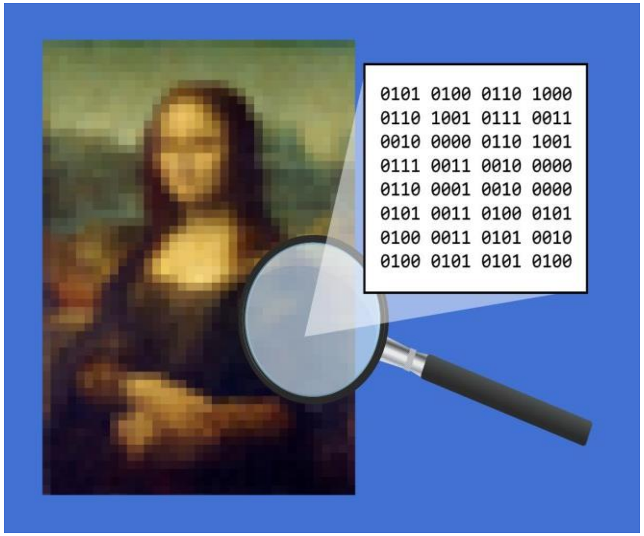
What is Steganography?

- **Steganography** is the art and science of writing hidden messages in such a way that no one apart from the intended reciepient knows about the existence of the message.

- Derived from Greek words:

“steganos” - covered **“graphia”** - writing

- **Goal of steganography:-** To hide one piece data into another.



EXAMPLE

Since everyone can read, encoding text in neutral sentences is doubtfully effective

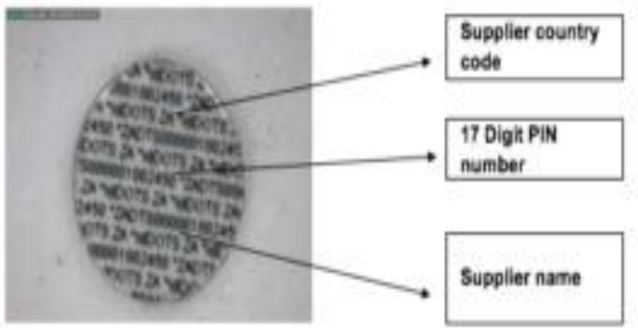
Taking the first alphabet in each word the following message emerges:

Since Everyone Can Read, Encoding Text In Neutral Sentences Is Doubtfully Effective

“SECRET INSIDE”

History

- The first recorded use of steganography can be traced back to **440 BC** ,when **Herodotus** mentions examples of steganography in his Histories.
- Ancient Chinese wrote messages on fine silk, which was then crunched into a tiny ball and covered in wax.
- **Invisible inks** were important steganographic tools during Second World War.
- During World War II **Microdots** were used widely.



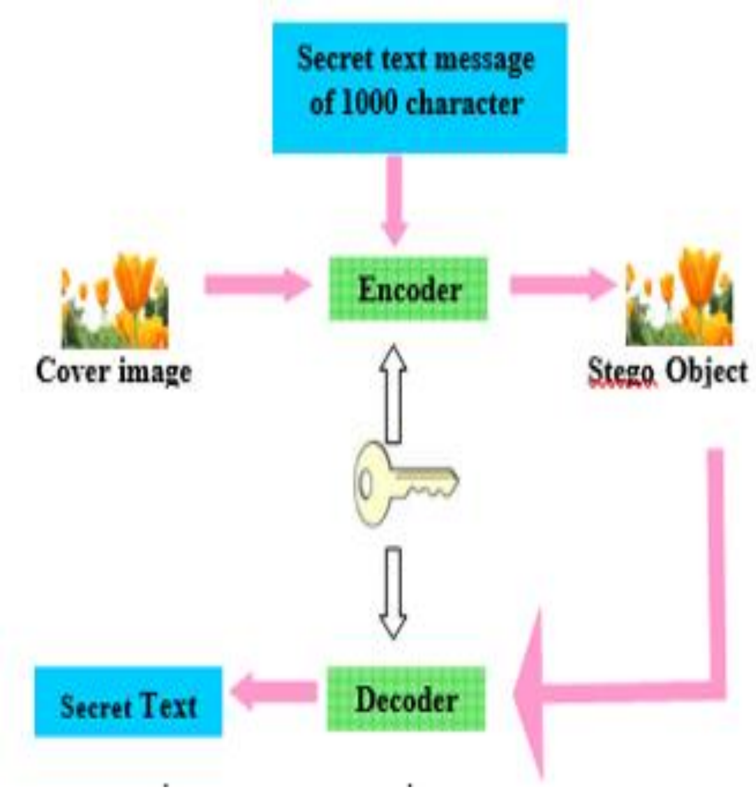
Steganography vs. Cryptography

Basis	Steganography	Cryptography
Definition	Steganography means **covered writing.**	Cryptography means **secret writing.**
Visibility	In steganography, the fact that a secret communication is taking place is hidden.	While in cryptography only a secret message is hidden.
Data Alteration	In steganography, the structure of data is not usually altered.	While in cryptography, the structure of data is altered.
Goal	The goal of steganography is to make the information invisible to anyone who doesn’t know where to look or what to look for	The main goal of cryptography is to keep the contents of the message secret from unauthorized access.

Basic steganographic model

- Steganography is the art of embedding a hidden message into a cover object without obviously changing the cover object's characteristics.

- The embedding procedure is typically related with a key, usually called a stego-key.



Types of Steganography

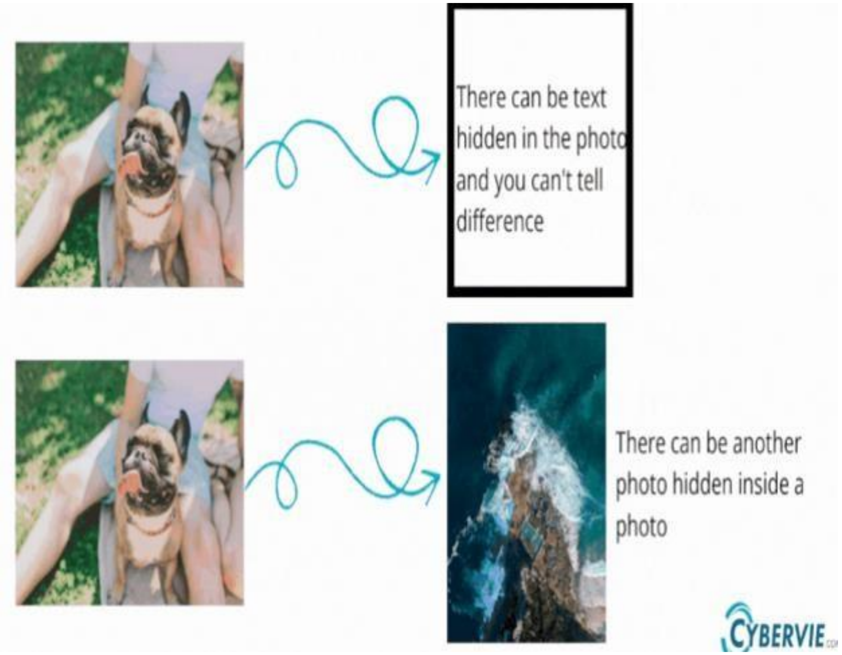
Most common types of Steganography are:-

- TEXT STEGANOGRAPHY

- IMAGE STEGANOGRAPHY

- AUDIO STEGANOGRAPHY

- VEDIO STEGANOGRAPHY



There can be text hidden in the photo and you can't tell difference

There can be another photo hidden inside a photo

Text steganography

It is a mechanism of hiding secret text inside another text.

Example:

A message containing cipher is German Spy in World War II:

“Apparently neutral's protest is thoroughly discounted And ignored. Isman hard hit. Blockade issue affects Pretext for embargo on by products, ejecting suets and Vegetable oils. ”

Taking the second letter in each word the following message emerges:

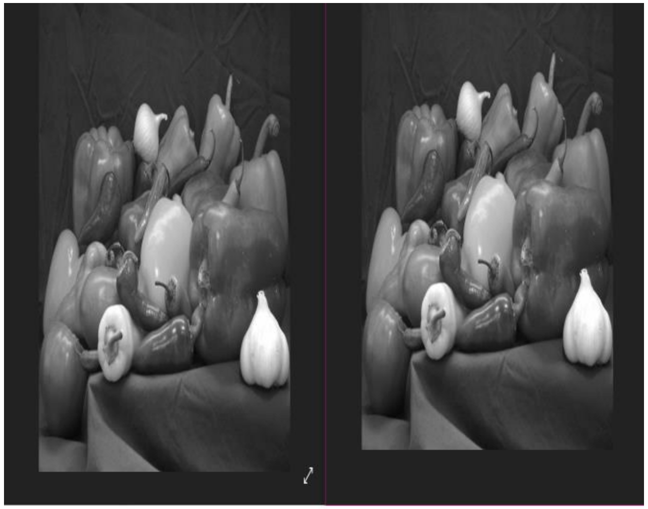
Pershing sails from NY June 1.

Image Steganography

- This technique involves changing the pixel values in an image to embed a secret message.
- The image compression techniques are extensively used in Steganography. Two type of compression techniques are:
  - Lossy compression – High compression rate but no integrity of originals.
  - Lossless compression – Low compression rate but with integrity of original data.
- **Lossless compression** is generally used in steganography.
- The most common image steganography technique is **LSB** (Least Significant Bit) method.

Least Significant Bit (LSB) method.

- This method functions well in cases where the image is grayscale and the file is longer than the message file.
- The LSB of some or all of the bytes inside a image is changed to a bit of secret message.
- When using a 24-bit image, a bit of each of the red, green, blue colour components can be used, since they are each represented by a byte. Put otherwise, every pixel has the capacity to store three bits.
- The image obtained after embedding is almost similar to original image because the change in the LSB of image pixel does not bring too much differences in the image.



ORIGINAL IMAGE

STEGO IMAGE

Example of LSB Method

- We can use images to hide things if we replace the last bit of every color's byte with a bit from the message

- A grid of 3 pixels of a 24- bit image can be as follows:

Pixel 1:	11111000	11001001	00000011
Pixel 2:	11111000	11001001	00000011
Pixel 3:	11111000	11001001	00000011

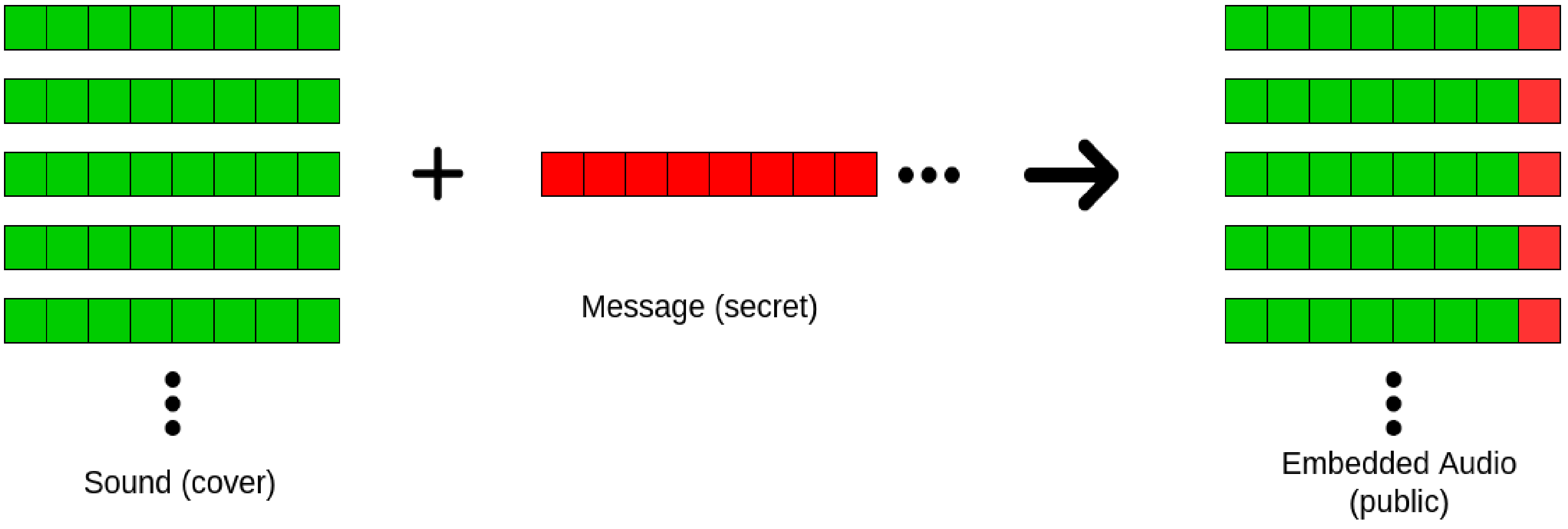
- Now we hide a number let it be 200, its binary representation is **11001000**

Resulting pixel of values will become :

Pixel 1:	1111100**1**	1100100**1**	0000001**0**
Pixel 2:	1111100**0**	1100100**1**	0000001**0**
Pixel 3:	1111100**0**	1100100**0**	00000011

Audio steganography

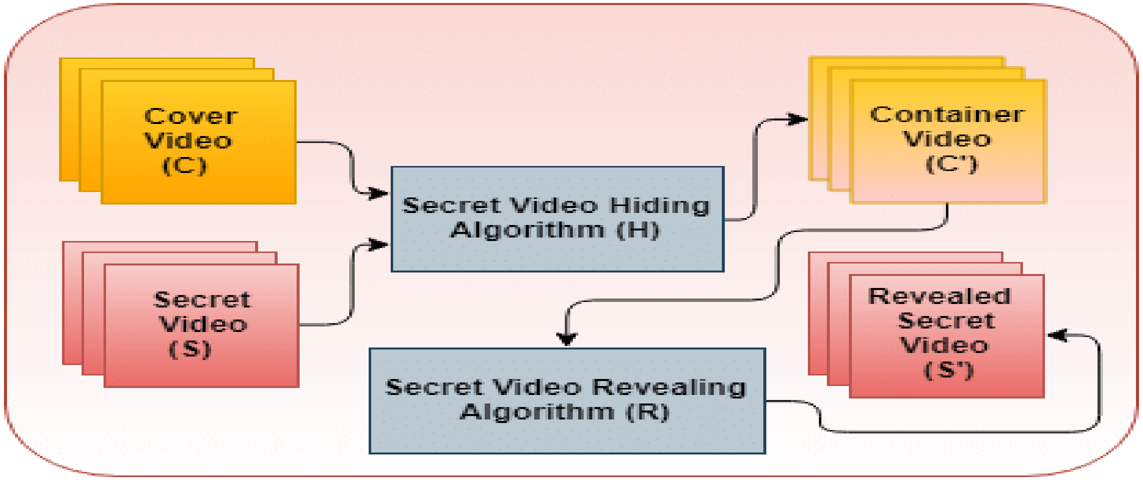
- In audio steganography, a secret message is encoded into a digital audio signal by slightly changing the corresponding audio file's binary sequence.



Vedio steganography

- Video Steganography is the process of hiding some secret information inside a video. The secret information can be any media like text, images, audio or another vedio.

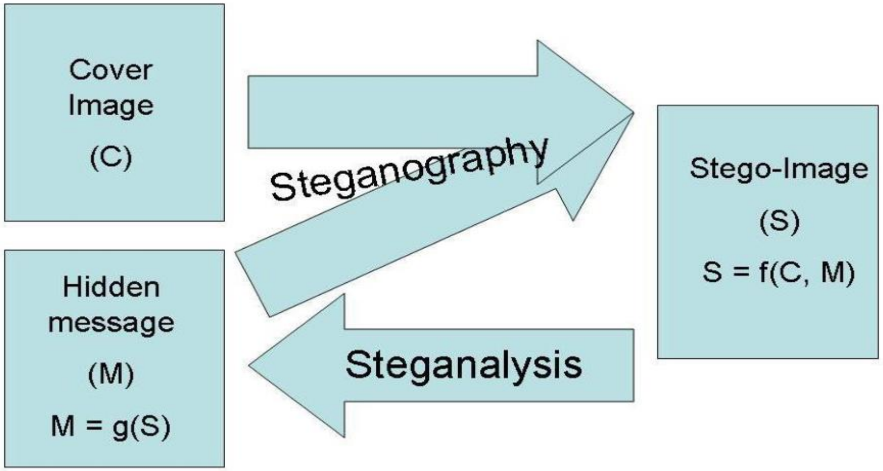
Video Steganography



Cover Video (C)
Secret Video (S)
Secret Video Hiding Algorithm (H)
Container Video (C')
Secret Video Revealing Algorithm (R)
Revealed Secret Video (S')

Steganalysis

- Steganalysis is the study of detecting messages hidden using steganography.
- The basic purpose of steganalysis is as a penetration tool to test the efficiency (Robustness, Capacity & Imperceptibility) of a particular Steganographic method.



Uses of Steganography

- Confidential communication and secret data storing.
- Protection from data alteraton.
- Usage in modern printers.
- Can be used to carry out hidden exchanges by Governments, military community etc.
- Transportation of sensitive data is another key use of steganography. A potential problem with cryptography is that eavesdroppers know they have an encrypted message when they see one.

Advantages

- Difficult to detect - only the receiver can detect.
- No one suspects existence of any kind of secret message being passed.
- Can be used for safeguarding data, such as in the field of media where copywrite ensures authenticity.
- Can be used by intelligence agencies for sending their secret data.

Limitations

- Steganography is limited, just as encryption. For example, if Jack wishes to give Lily an image that contains a hidden message, he must first secretly agree with Lily on a steganography method; otherwise, the image will be useless because the recipient won't know that it contains a secret message.
- This method can be extremely dangerous for everyone if it falls into the wrong hands, such as those of hackers.

Future scope

In the near future, the possible use of steganography technique is as following:

- Hiding data on the network in case of a breach.
- Peer-to-peer private communications.
- Manufacturers of digital cameras could include steganographic functionality in the firmware of their devices to annotate images with the photographer's copyright details.

Conclusion

- Hiding a message with steganography methods reduces the chance of a message being detected.
- Like any technology, steganography is neither intrinsically beneficial or detrimental; rather, how it is applied will determine whether it serves our society well or poorly, and whether it is utilized in an authorized or illegitimate manner.
- Steganography by itself isn't very secure, but when paired with cryptography, it can provide a considerably more powerful encryption technique.

References

- https://en.wikipedia.org/wiki/Steganography
- Cryptography and network security by William Stallings 2nd edition.
- International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010
- Steganography and Steganalysis: An Overview | SANS Institute - https://www.sans.org/white-papers/553/