

# STEGANOGRAPHY

Vundavalli Aswini-B150519EC

National Institute Of Technology Calicut

February 26, 2019

# NETWORK SECURITY

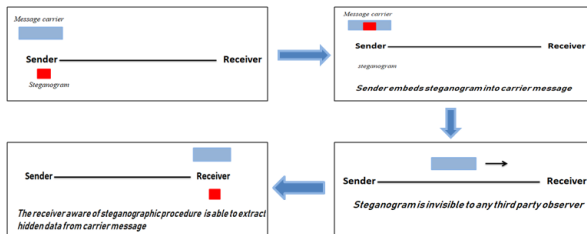
- Security-Utmost important in today's world
- Two techniques for providing confidentiality
  - Cryptography
  - Steganography

- Hides the meaning of the message
- Alters the secret message structure
- Transmission of secret data is known

# What is Steganography?

- Greek words:  
STEGANOS- "Covered" GRAPHIE- "Writing"
- Steganography means Covered writing
- **Definition:** It is an art and science of hiding information by embedding it in some other data.
- **Goal:** To hide a secret message inside other objects in such a way that presence of secret message is not visible.

# General view of Steganography



- **Tattoos on shaved heads**-First used by a Greek ruler HISTAEUS,shaved a slaves head and tattooed message on it.
- **Wax tablets**- The secret message was carved on the wood of wax tablet, and then covered with a fresh layer of wax.
- **Invisible Inks**-In World War II,invisible inks are used to write messages in between the lines of normal text message.
- **Null ciphers**- Null ciphers are normal messages with secret messages embedded in the current text.

*Fishing freshwater bends and saltwater coasts rewards anyone feeling stressed. Resourceful anglers usually find masterful leapers fun and admit swordsh rank overwhelming any day*

**Secret message**- *send lawyers, guns, and money*

- **Micro Dots**-During World War II the Germans developed microdot technology, Message is neither hidden nor encrypted. It was just so small as to not draw attention to itself
- **Morse Codes**-either of two codes consisting of variously spaced dots and dashes or long and short sounds used for transmitting messages by audible or visual signals  
**TORTURE:** “- — .- - ..- ..- .”
- In the times of using printing press, secret messages are hidden by using different typefaces, such as italic or normal

# Modern Steganographic System

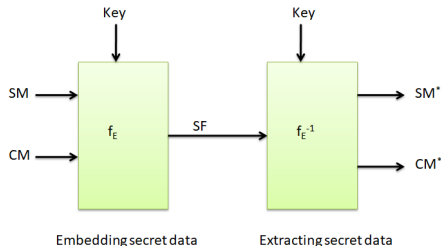


Figure: General Steganographic system

- SM: The secret message to be hidden.
- CM: The data used to conceal the secret message.
- Stego file (SF): Cover message with secret embedded in it.
- Steganalysis: It is the process of identifying steganography by inspecting various parameters of a Stego media



# Classification of Steganography

Based on the cover media used to hide secret

- Text Steganography
- Image Steganography
- Audio Steganography
- Video Steganography
- Network Steganography

# TEXT STEGANOGRAPHY

- Text is used as a cover media to hide the secret data.
- Text steganography can be classified into 3 basic categories: Format based, Random generation, Linguistic methods.

**Format based method:** modifies the existing text in order to hide the secret message.

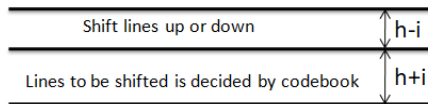
**Random generation:** Hides the information in a random looking sequence of characters.

**Linguistic method:** Combination of Syntax and Semantics methods.

# TEXT STEGANOGRAPHY

## LINE SHIFT CODING

- Vertically shift lines in a document by a small fraction
- Upward shift indicates presence of binary bit- “0”
- Downward shift indicates presence of binary bit- “1”



**Drawbacks:** When OCR is applied, the hidden information is destroyed.

# TEXT STEGANOGRAPHY

## WORD SHIFT CODING

- Horizontally shift words in a document
- Rightward shift indicates presence of binary bit- “1”
- Leftward shift indicates presence of binary bit- “0”

The quick brown fox jumps over the lazy dog.  
The quick brown fox jumps over the lazy dog.

In this example the first line uses normal spacing while the second had each word shifted left or right inorder to encode the sequence 01000001  
i.e. ASCII code for character 'A'

**Drawbacks:** managed to trick most of the human eyes but it cannot trick once computer systems have been used.

# TEXT STEGANOGRAPHY

## FEATURE CODING

- Features of the text are altered.
- For example, point in letters i and j can be displaced, length of strike in letters f and t can be changed, or by extending or shortening height of letters b, d, h, etc.

**Drawbacks:** If an OCR program is used or if retyping is done, the hidden content would get destroyed.

# TEXT STEGANOGRAPHY

## WHITE SPACE MANIPULATION

- This technique uses white spaces for hiding a secret message
- In **Inter Sentence Spacing**, we place single space to hide bit 0 and two spaces to hide bit 1 at the end of each terminating character .
- In **Inter Word Spacing** technique, one space after a word represents bit 0 and two spaces after a word represents bit 1.

**Drawbacks:** If an OCR program is used or if retyping is done, the hidden content would get destroyed.

# TEXT STEGANOGRAPHY

## SYNTACTIC METHOD

- Hides the message, by placing some punctuation marks such as full stop (.) and comma (,) in proper places.
- These marks serve as a basis of hiding 0 or 1.
- This method requires identifying proper places for putting punctuation marks.

### Drawback

An intruder having good knowledge in English can intercept because he or she knows that what the exact may position of such marks in a text document and has low hidden ratio

# TEXT STEGANOGRAPHY

## SEMANTIC METHOD

- Hides the information by using synonyms of certain words.
- For example, the word “big” could be considered primary and “large” secondary.
- while decoding, primary words will be read as ones, secondary words as zeros.



# TEXT STEGANOGRAPHY

## TEXT ABBREVIATION OR ACRONYM

- hides the information by using abbreviations like as soon as possible is replaced by ASAP
- A full word can hide a “1” and the abbreviated word can hide a “0” or viceversa.

# IMAGE STEGANOGRAPHY

- Images are used as a cover media to hide the secret data
- Images are made up of lot of little dots called pixels
- Each pixel is represented by 3 bytes, one for red, one for green, one for blue

The representation of orange color is shown below

R	G	B
11111000	11001001	00000011
248	201	3

# IMAGE STEGANOGRAPHY

## LSB SUBSTITUTION

- The difference between two colors that differ by one bit(LSB bits) in either red,green or blue value is hard to detect
- So, even if the least significant bit of a byte is changed,it wont change the color it appears to be.
- one byte of secret data can be hidden for every 8 bytes of cover.
- 50% chance that the bit you're replacing is same as its replacement
- Necessary to use lossless compression format.

Algorithm:

$S(i,j)=C(i,j)-1$  if  $LSB(C(i,j))=1$  and  $SM=0$


$S(i,j)=C(i,j)+1$  if  $LSB(C(i,j))=0$  and  $SM=1$

$S(i,j)=C(i,j)$  if  $LSB(C(i,j))=SM$

# IMAGE STEGANOGRAPHY

## LSB SUBSTITUTION

**Message: A**    **01000001**

**Image with 3 pixels:**    

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

**Now we hide our message in the image:**

**Pixel 1:**    **11111000**    **11001001**    **00000010**  
**Pixel 2:**    **11111000**    **11001000**    **00000010**  
**Pixel 3:**    **11111000**    **11001001**    **00000011**

**New image:**    

# IMAGE STEGANOGRAPHY

## LSB SUBSTITUTION

Original Image



11111111	00000000
00000000	00000000
00000000	00000000
11111111	00000000
11111111	00000000
00000000	11111111

Least Significant Bit  
Steganography

Stego Image



11111101	00000011
00000010	00000001
00000000	00000010
11111100	00000011
11111101	00000001
00000001	11111100



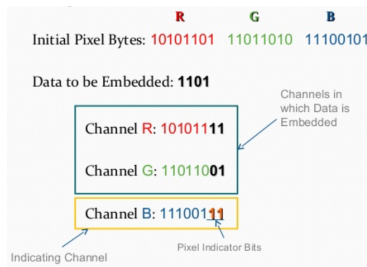
<b>c</b>	<b>a</b>	<b>t</b>
01 10 00 11	01 10 00 01	01 11 01 00

# IMAGE STEGANOGRAPHY

## PIXEL INDICATOR

This method uses 2 least significant bits of one byte to indicate the presence of data in the other 2 bytes

Indicator	Channel 1	Channel 2
00	No hidden data	No hidden data
01	No hidden data	2 bits of hidden data
10	2 bits of hidden data	No hidden data
11	2 bits of hidden data	2 bits of hidden data



# IMAGE STEGANOGRAPHY

## DISTORTION TECHNIQUES

- stego object is created by applying a sequence of modifications to the cover image
- sequence of modifications is used to match the secret message required to transmit

Decoder should know the cover image

message bit= "1"; if Stegoimage is different from cover image at the given message pixel

message bit= "0"; else

# AUDIO STEGANOGRAPHY

## LSB CODING

- Sampling followed by quantization converts analog audio signal to digital binary sequence.
- LSB of binary sequence of each sample of digitized audio file is replaced with binary equivalent of secret message.



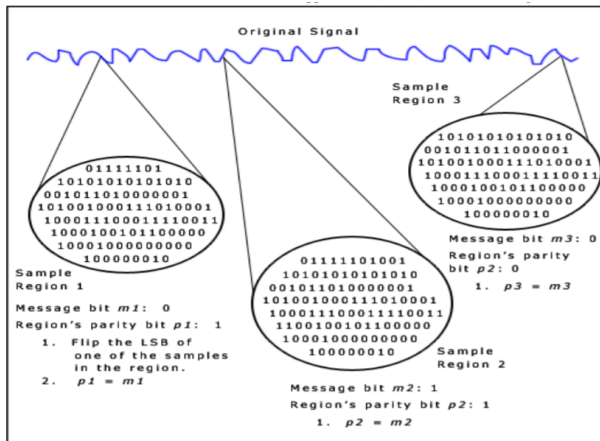
# AUDIO STEGANOGRAPHY

## PARITY CODING

- Instead of breaking a signal into individual samples, this method breaks a signal into separate regions of samples
- Encode each bit from the secret message in a sample regions parity bit
- If the parity bit of a selected region does not match the secret bit to be encoded, the process inverts the LSB of one of the samples in that region.

# AUDIO STEGANOGRAPHY

## PARITY CODING



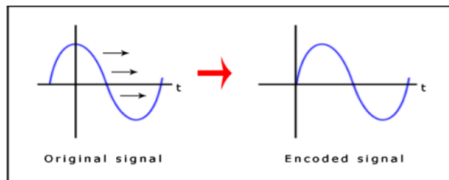
# AUDIO STEGANOGRAPHY

## PHASE CODING

- Cover Audio signal is broken into series of N short segments
- Replace the phase of an initial audio segment with a reference phase that represents the secret information.

$$\text{Phasenew} = \begin{cases} \frac{\pi}{2} & \text{if message bit}=0 \\ -\frac{\pi}{2} & \text{if message bit}=1 \end{cases}$$

- The remaining segments phase is adjusted in order to preserve the relative phase between segments.



# VIDEO STEGANOGRAPHY

## LSB CODING

- Same as the LSB method discussed in image and audio steganographic techniques
- The cover video's pixel values are extracted which are in bytes, then its LSB are substituted by the bits of the secret message.

# VIDEO STEGANOGRAPHY

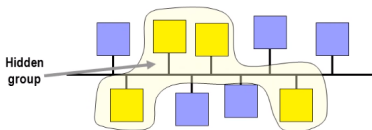
## NON-UNIFORM RECTANGULAR PARTITION

- data hiding is done by hiding an uncompressed secret video file in the host video stream.
- both the secret as well as the cover file should be of almost the same size.
- Each of the frames of both the secret as well as cover videos is applied with image steganography
- secret video file will be hidden in the leftmost four least significant bits of the frames of the host video

# NETWORK STEGANOGRAPHY

HICCUPS (HIdden Communication system for CorrUPted networkS)

- HICCUPS is a steganographic system for hidden group with common knowledge
- A station sends a corrupted frame (incorrect checksum)
- Hidden stations changes there mode as per the corrupted frame
- Replaces the payload of intentionally corrupted packets with steganogram



# NETWORK STEGANOGRAPHY

## LACK (Lost Audio paCKets )

- Used in IP Telephony
- Voice packets are generated at the transmitter end and out of those generated voice packets one is delayed intentionally
- The payload of the delayed packet is replaced with the steganogram.
- As soon as the delay timer expires the packet is sent to the receiver.

# NETWORK STEGANOGRAPHY

## LACK (Lost Audio paCKets )

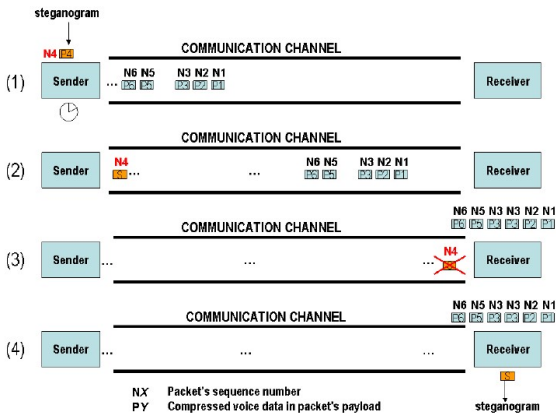


Figure: LACK Scenario



# NETWORK STEGANOGRAPHY

## RSTEG (Retransmission STEGanography )

- Receiver intentionally acknowledge that few received packets are not received invoking the need of retransmission
- Retransmitted packet is now replaced with the steganogram and transmits this packet

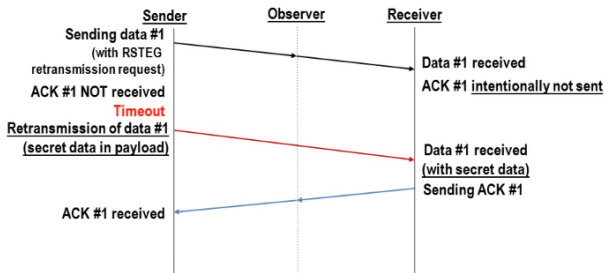


Figure: Transmission ow in RSTEG

# PERFORMANCE MEASUREMENT METRICS

- **Capacity**- It is defined as the maximum amount of data that can be hidden in a cover, compared to the size of the cover.
- **Robustness**-The term robustness means the difficulty of removing hidden information from a stego object.
- **Security**-The security of a steganographic system is judged by the impossibility of detecting rather than by the difficulty of reading the message content

**Hacking** is an unauthorized access of data which can be collected at the time of data transmission.

So, whatever be the technique will be developed in future, degree of security related with that has to be kept in mind. It is hoped that Dual Steganography, Steganography along with Cryptography may be some of the future solution for this above mentioned problem.

# CONCLUSIONS

- Different methods of Steganography are discussed. Each method has a unique procedure of embedding secret data. It is not possible to say that a specified method is the best. One can just compare different methods from different aspects, which results in determining a suitable method for a specific usage.
- Steganographic algorithms developed for one cover media may not be effective for another media.
- Cryptography and Steganographic techniques can be combined for improving secrecy.

# REFERENCES



Govinda Borse,Vijay Anand,Kailash Patel , “Steganography:Exploring an ancient art of Hiding Information from Past to Future” ,*International Journal of Engineering and Innovative Technology(IJEIT)*,ISSN:2277-3754Volume 3,Issue 4,October 2013



Sunita Chaudary, Meenu Dave, Amit Sanghi, “Reveiw of Linguistic Text Steganographic Methods ” , *International Journal of Recent and Innovation Trends in Computing and Communication* ,ISSN:2321-8169,Volume:4 Issue:7,July 2016



Monika Agarwal, “TEXT STEGANOGRAPHIC APPROACHES:A COMPARISON ” , *International Journal of Network Security Its Applications(IJNSA)* ,Vol.5,No.1,January 2013



Sheetal Deshpande,Shubham Mallayanavarmath, “COMPLETE STUDY ON STEGANOGRAPHY ” , *International Journal for Research in Applied Science Engineering Technology(IJRASET)* ,e-ISSN:2321-9653,Volume 5,Issue VI,June 2017

# REFERENCES



Palwinder Singh, "A COMPARATIVE STUDY OF AUDIO STEGANOGRAPHY TECHNIQUES ", *International Research Journal of Engineering and Technology(IRJET)*, e-ISSN:2395-0056,p-ISSN:2395-0072,Vol.03,Issue:4,April 2016



Syeda Musfia Nasreen, Gaurav Jalewal, Saurabh Sutradhar, "A study on Video Steganographic Techniques ", *International Journal of Computational Engineering Research (IJCER)*,ISSN(e):2250-3005,Volume 05,Issue 10,October-2015



Namrata Singh,Jayati Bhardwaj,Gunjan Raghav, "Network Steganography and its Techniques", *International Journal of Computer Applications(0975-8887)*,Volume 174-No.2,September 2017



Aryfandy Febryan,Tito Waluyo Purboyo,Randy Erfa Saputra, "Steganography Methods on Text,Audio,Image and Video:A Survey ", *International Journal of Applied Engineering Research*,ISSN 0973-4562,Volume 12,Number 21,2017