Unit-2

Data Recovery

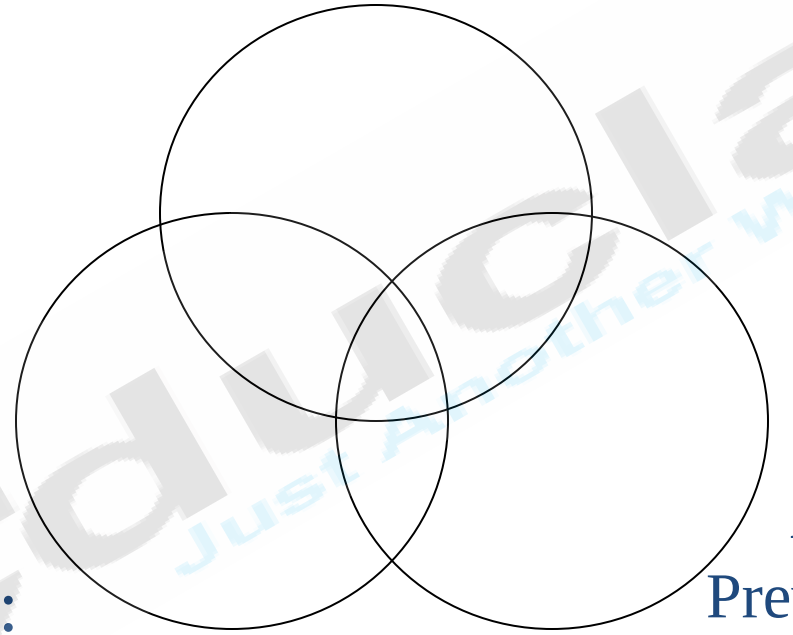
Contents

- Encryption and Decryption
- Recovery deleted files
- Identifying false images
- Steganography methods for media data including text, image and audio data

Security Objectives

Confidentiality (Secrecy):

Prevent/Detect/Deter improper disclosure of information



Integrity:

Prevent/Detect/Deter improper modification of information

Availability:

Prevent/Detect/Deter improper denial of access to services provided by the system

Security Services

- Confidentiality: protection of any information from being exposed to unintended entities.
  - Information content
  - Parties involved
  - Where they are, how they communicate, how often, etc.
- Authentication: assurance that an entity of concern or the origin of a communication is authentic - it's what it claims to be or from
- Integrity: assurance that the information has not been tampered with

Encryption/Decryption

- Plaintext: a message in its original form
- Ciphertext: a message in the transformed, unrecognized form
- Encryption: the process for producing ciphertext from plaintext
- Decryption: the reverse of encryption
- Key: a secret value used to control encryption/decryption

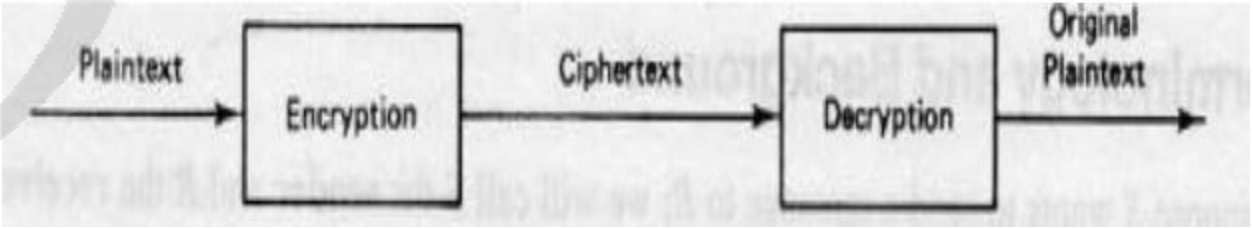
- plaintext to ciphertext: encryption

$$C = E(P)$$

- ciphertext to plaintext: decryption:

$$P = D(C)$$

requirement: $P = D(E(P))$

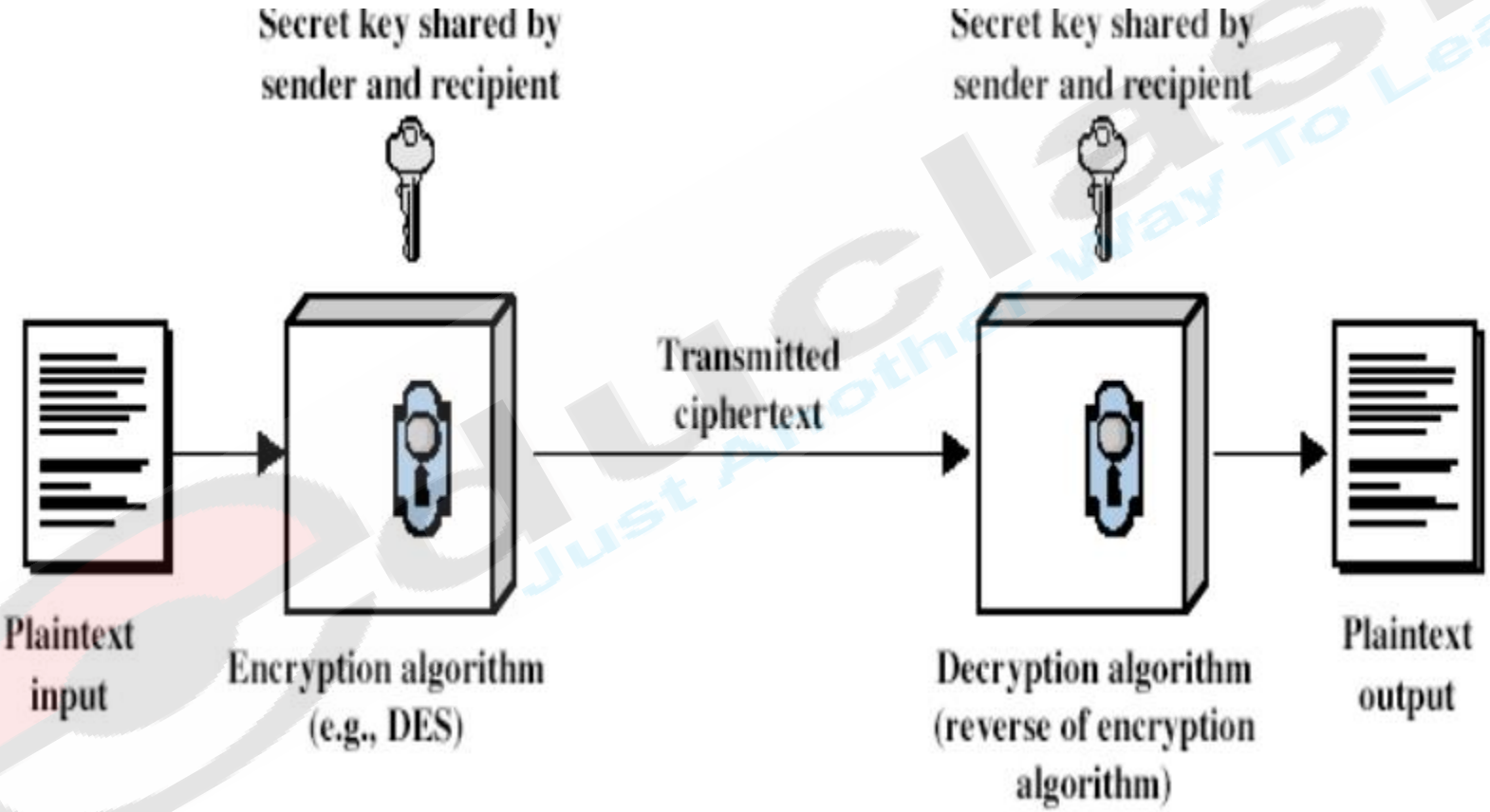


Classical Encryption Techniques

- Symmetric key encryption
- Asymmetric key encryption

Symmetric key encryption

- Sender and recipient share a common key
- All traditional schemes are symmetric / single key / private-key encryption algorithms, with a single key, used for both encryption and decryption, since both sender and receiver are equivalent, either can encrypt or decrypt messages using that common key.



Use the additive cipher with key = 15 to encrypt the message “hello”.

Plaintext: h → 07	Encryption: (07 + 15) mod 26	Ciphertext: 22 → W
Plaintext: e → 04	Encryption: (04 + 15) mod 26	Ciphertext: 19 → T
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: o → 14	Encryption: (14 + 15) mod 26	Ciphertext: 03 → D

Ciphertext: W → 22	Decryption: (22 – 15) mod 26	Plaintext: 07 → h
Ciphertext: T → 19	Decryption: (19 – 15) mod 26	Plaintext: 04 → e
Ciphertext: A → 00	Decryption: (00 – 15) mod 26	Plaintext: 11 → l
Ciphertext: A → 00	Decryption: (00 – 15) mod 26	Plaintext: 11 → l
Ciphertext: D → 03	Decryption: (03 – 15) mod 26	Plaintext: 14 → o

Recovering Deleted files on window systems

- The files that are begin deleted are the ones that marks or breaks your investigation
- Deleted files are actually not deleted but marked for deletion
- For eg.Fat system when file or directory is deleted,first letters of its name is ser to sigma character or in hex.
- Deleted files located on harddisk will remain intact(unbroken) until a new file or data
- Tools are available to “intact” deleted files and recover them for review

1.Using window-based tools to recover files on FAT systems:

- To recover files on FAT we use tools-Encase and FTK
- Both tools have built-in capability to automatically recover any files

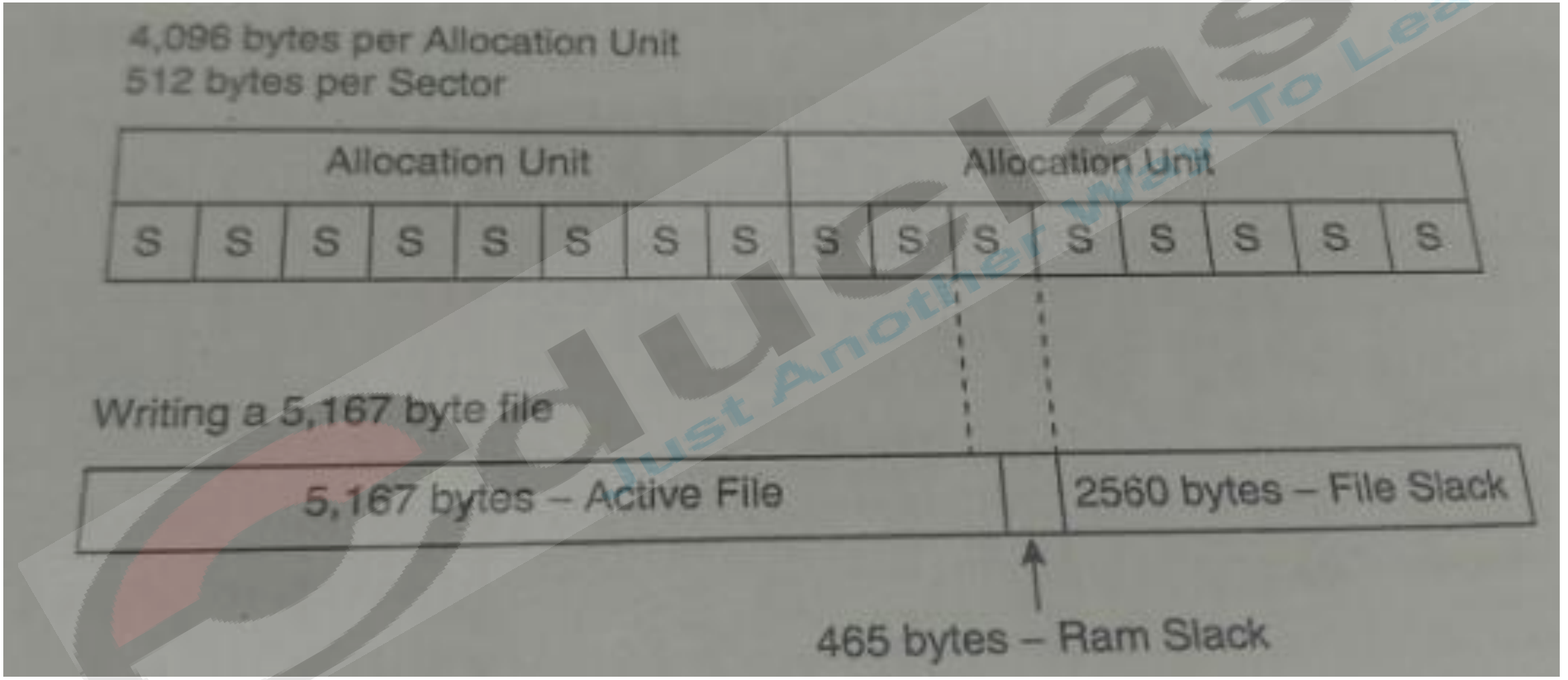
2.Using Linux tools to recover files on FAT file systems:

- Following capabilities provided by an operating system to value to a computer forensic examiner:
  - Supports wide variety of files including FAT12,FAT16,FAT32,NTFS,HPFS,EXT2,EXT3 and UFS
  - Recovers file slack and not allocate space
  - Provides an efficient, effective and accurate undeleted utility
  - Handles compressed drives(Drivespace, Dblspace and drivespace3)
  - Delivers widespread checking and cataloging of all forensic activities
  - Delivers for data authentication and reliability

Recovering Unallocated Space, Free Space and Slack Space

- Forensic duplication of media and recovery of entire possible file is done still data left for evidence media that we review
- Remaining data is stored in slack space, unallocated space and free space
- All data stored on harddisk are arranged by operating systems into segments called allocation unit or clusters
- For eg.os uses 32k clusters reads and writes that from hard drive at a time
- When os utilize 32 k clusters to hard drive is being asked to save 20k word documen,12k of unused space called file slack

Illustration of Slack space



Slack and Its Types

- Two types os slack space:RAM slack and File slack

1.File slack:

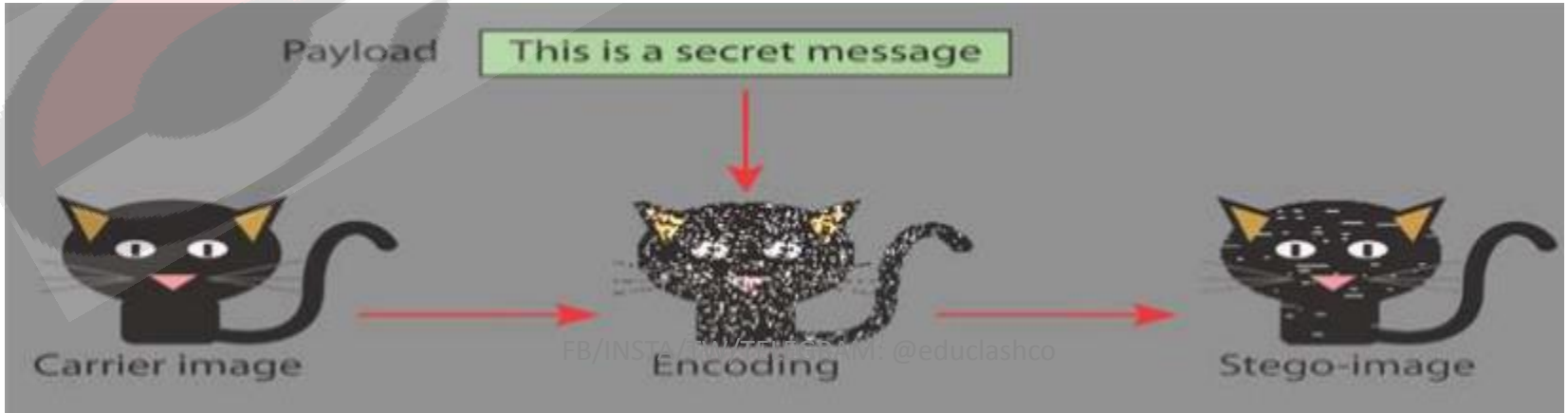
- Cluster is the place to store files. file size uses fixed size container or block of sectors.
- OS arrange all data stored on a harddisk into segments called allocation units or clusters.
- Ex 5000 byte file takes upto 9 sectors,OS allocate 2 clusters,does not fit in 1 sector. Two sector is 8 kB.
  - 2500 byte file will fit into 5 sectors,OS allocate 1 clusters, one sector is 4 kB.

2.RAM slack:

- It is basically data between end of a logical file and sector
- It takes upto 512 bytes on harddrive,if file takes upto 400 bytes in last logical sector, remaining 112 bytes will be RAM slack
- RAM slack contains a small portion of random data whose source is whatever contents of RAM that is chosen to fill that space
- For ex,512 bytes of sector and 8 sectors per cluster, size of cluster is 4096 bytes

What is Steganography?

- Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity.
- The word steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered or protected", and graphein meaning "writing“.
- “Steganography means hiding one piece of data within another”.



Steganography V/s Cryptography

- Steganography
- Unknown message passing
- Little known technology
- Technology still being develop for certain formats
- Steganography does not alter the structure of the secret message

Cryptography

- Known message passing
- Common technology
- Most of algorithm known by all
- Cryptography alter the structure of the secret message

Steganography	Cryptography
Unknown message passing	Known message passing
Steganography prevents discovery of the very existence of communication	Encryption prevents an unauthorized party from discovering the contents of a communication
Little known technology	Common technology
Technology still being develop for certain formats	Most of algorithm known by all
Once detected message is known	Strong current algorithm are resistant to attacks ,larger expensive computing power is required for cracking
Steganography does not alter the structure of the secret message	Cryptography alter the structure of the secret message

Advantages of steganography

- The secret message does not attract attention to itself as an object of scrutiny.
- steganography is concerned with concealing a secret message is being sent, as well as concealing the contents of the message.
- Difficult to detect. Only receiver can detect.
- Provides better security for data sharing

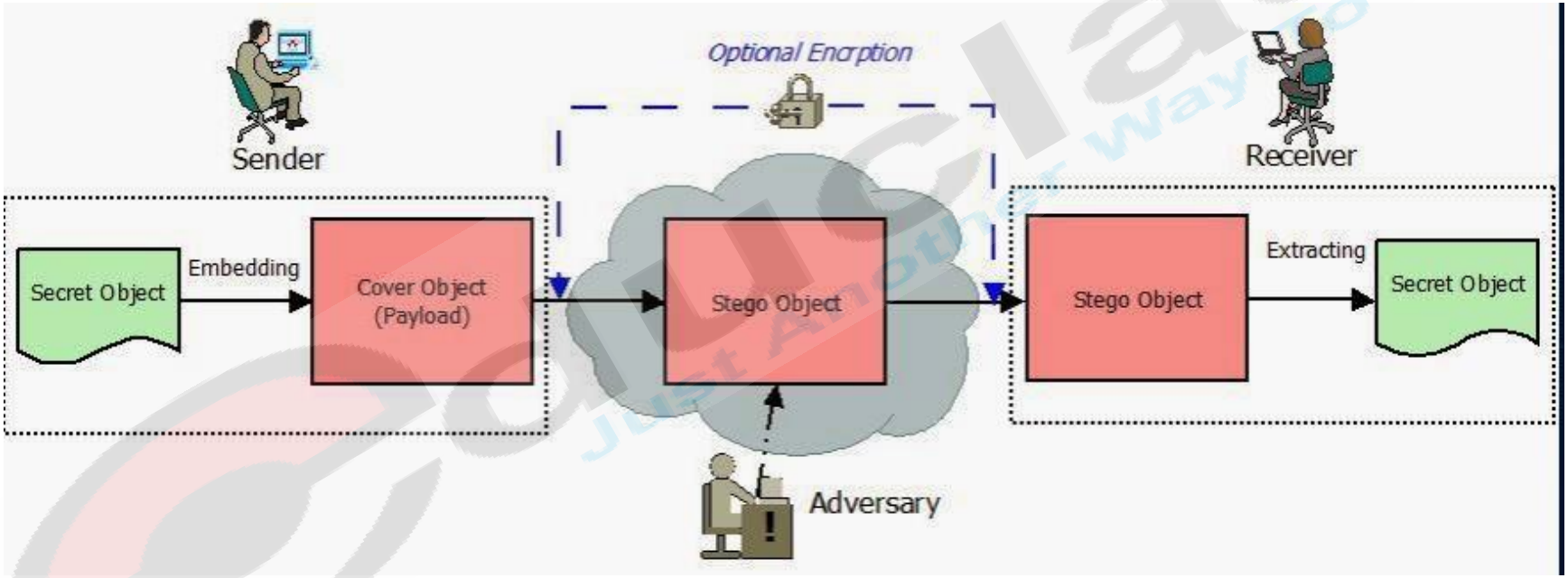
Limitations

- The confidentiality of information is maintained by the algorithms, and if algorithms are known then this technique is of no use.
- Password leakage may occur and it leads to the unauthorized access of data.

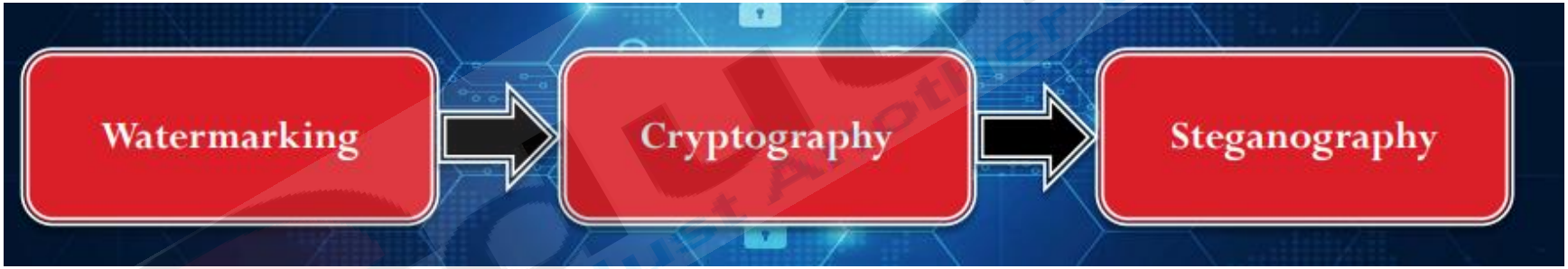
Application

- several information sources like our private banking information, some military secrets, can be stored in a cover source.
- Steganography is used by some modern printers and color laser printers.
- Steganography can be used for digital watermarking.

Basic Steganography Model

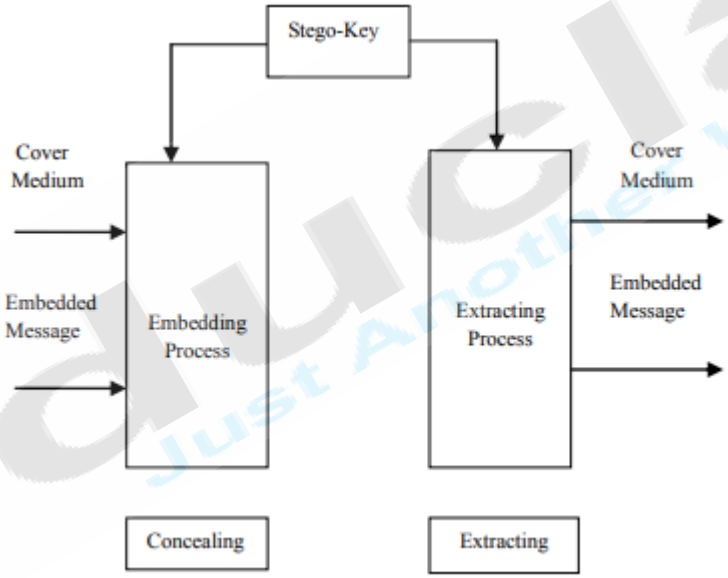


Evolution



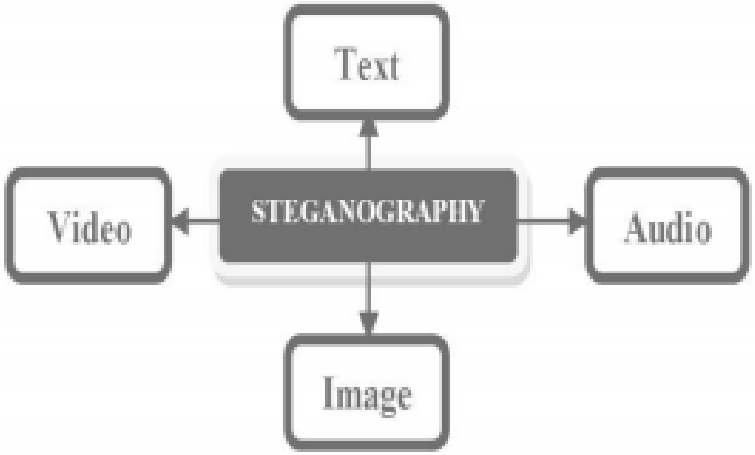
Steganography Terms

- Carrier or Cover File - A 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.
- Embedded or Payload - The information which is to be hidden or concealed.
- Steganalysis - The process of detecting hidden information inside a file.



Types of Steganography

- Types Of Steganography
  - Text Steganography
  - Image Steganography
  - Audio Steganography
  - Video Steganography



- **Steganography in Images:** Image steganography is very effective, efficient and can serve a variety of purposes included authentication, concealing of messages etc. The hidden messages will change the last bit of byte in an image in Least significant bit method So by doing this, there will be relatively no change within the carrier image.
- **Steganography in Audio:** In audio Steganography system, secret messages are embedded into digitized audio signal which results into altering binary sequence of corresponding audio files.
- **Steganography in Text**: Encoding secret messages in text can be a very challenging task. This is because text files contain redundant data to replace with a secret message. Another cons is the ease of which text based Steganography can be altered by an unwanted parties by just changing the text itself or reformatting the text to some other form (from .TXT to .PDF, etc.).

Text Steganography

- Text steganography can be applied in the digital makeup format such as PDF, digital watermark or information hiding
- It is more difficult to realize the information hiding based on text. The simplest method of information hiding is to select the cover first, adopt given rules to add the phraseological or spelling mistakes, or replace with synonymy words.
- Ex: TextHide hides the information in the manner of text overwriting and words' selection.

Text Steganography Model

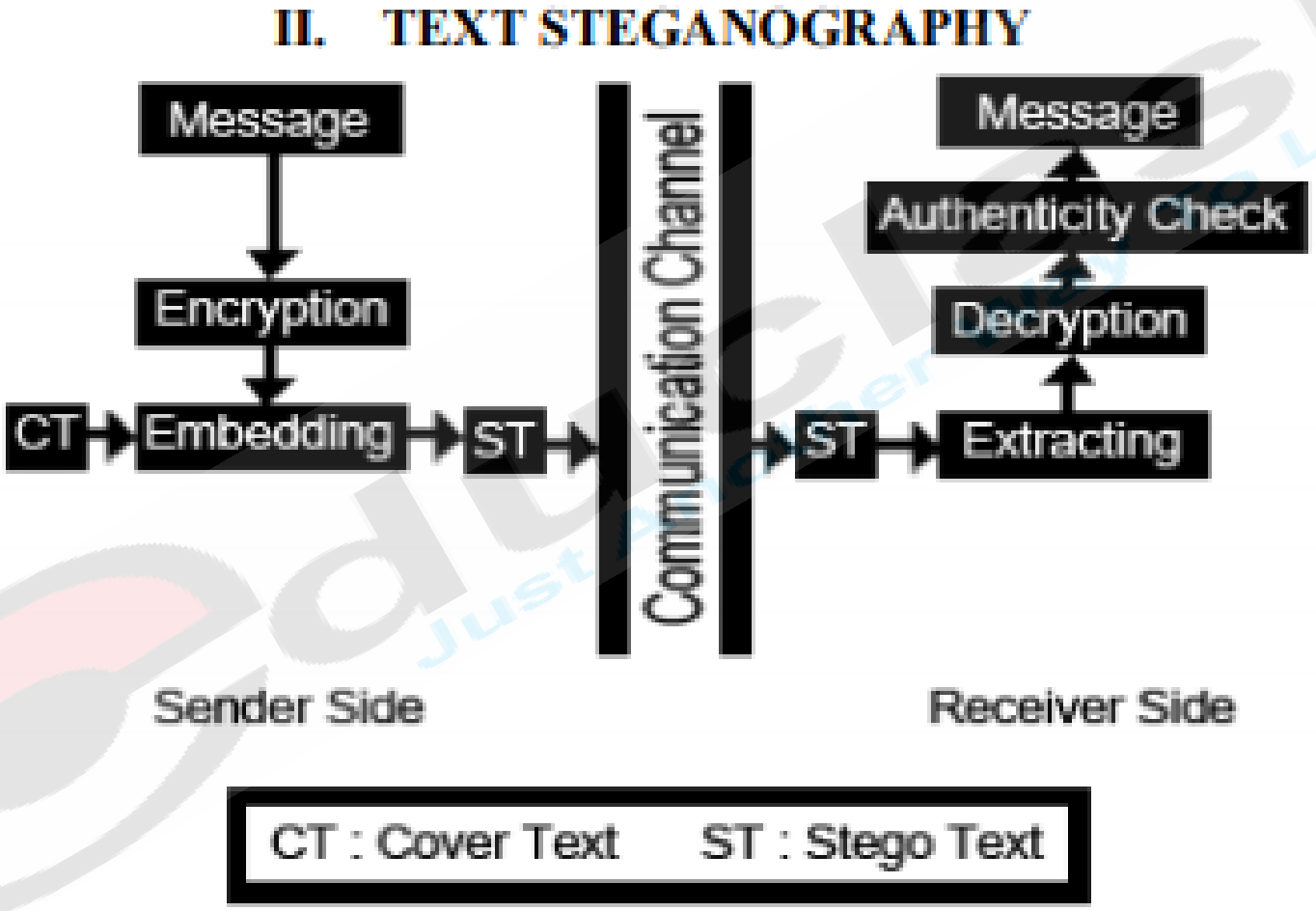
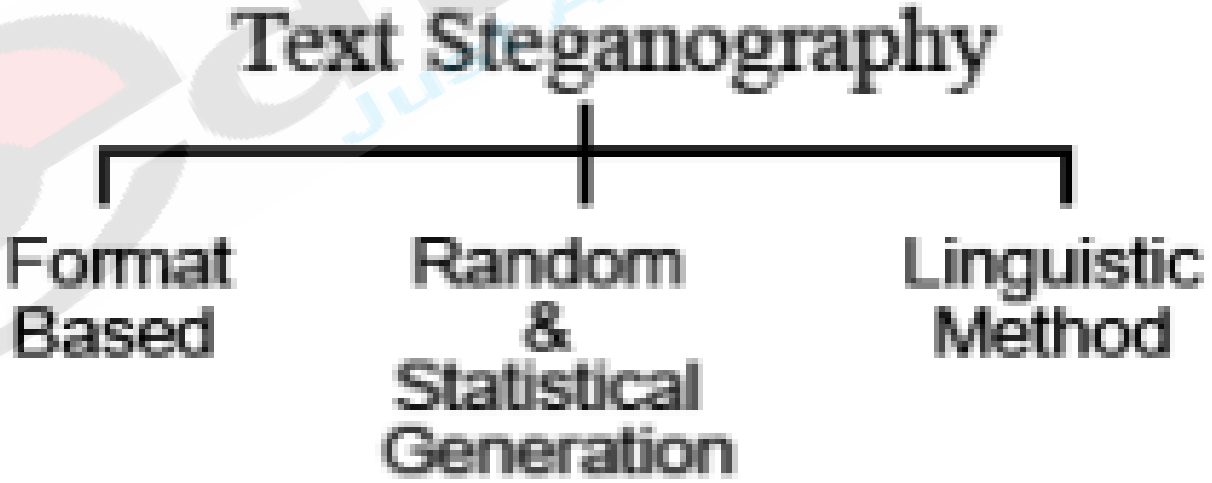


Fig: Text Steganography Model

- The text steganography is a method of using written natural language to conceal a secret message
- A message is embedded in a text (cover text) through an embedding algorithm.
- The resulting stego text is transmitted over a channel to the receiver where it is processed by the extraction algorithm with the help of a secret key.
- During transmission the stego text, it can be monitored by unauthenticated viewers who will only notice the transmission of an innocuous-text without discovering the existence of the hidden message in it.
- Text steganography can be broadly classified into three types- format-based, random and statistical generations and Linguistic method



(1)**Format-based methods :** This method uses the physical formatting of text as a space in which to hide information.

- Insertion of spaces or non-displayed characters, careful errors tinny throughout the text and resizing of fonts are some of the many format-based methods used in text steganography.
- Some of these methods, such as deliberate misspellings and space insertion, might fool human readers who ignore occasional misspellings, but can often be easily detected by a computer.

(2) Random and statistical generation method : Random and statistical generation methods are used to generate cover-text automatically according to the statistical properties of language. These methods use example grammars to produce cover-text in a certain natural language. A probabilistic context-free grammar (PCFG) is a commonly used language model where each transformation rule of a context- free grammar has a probability associated with it.

(3) Linguistic methods : Linguistic steganography specifically considers the linguistic properties of generated and modified text, and in many cases, uses linguistic structure as the space in which messages are hidden .

Format-based methods

- A format-based text steganography method is open space method .
- In this method extra white spaces are added into the text to hide information. A single space is interpreted as‖0‖ and two consecutive spaces are interpreted as‖1‖.
- Another two format-based methods are word shifting and line shifting.

(1)Word shifting method:

- In this method, by shifting words horizontally and by changing distance between words, information is hidden in the text.
- This method is acceptable for texts where the distance between words is varying.
- This method can be identified less, because change of distance between words to fill a line is quite common.
- But if somebody was aware of the algorithm of distances, he can compare the present text with the algorithm and extract the hidden information by using the difference. The text image can be also closely studied to identify the changed distances. Although this method is very time consuming, there is a high probability of finding information hidden in the text. Retyping of the text or using OCR programs destroys the hidden information

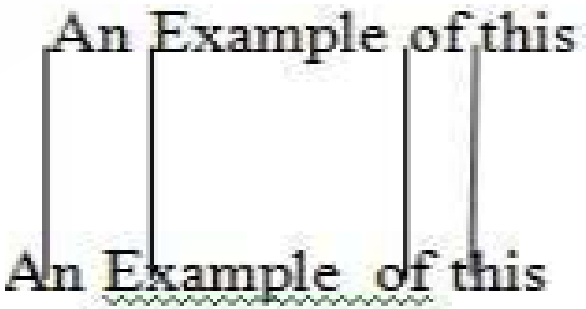


Fig. Word Shifting

(2) Line shifting:

- In this method, the lines of the text are vertically shifted to some degree (for example, each line is shifted 1/300 inch up or down) and information are hidden by creating a unique shape of the text. This method is suitable for printed texts.
- However, in this method, the distances can be observed by using special instruments of distance assessment and necessary changes can be introduced to destroy the hidden information. Also if the text is retyped or if character recognition programs (OCR) are used, the hidden information would get destroyed. This method hides information by shifting the text lines to some degree to represent binary bits of secret information

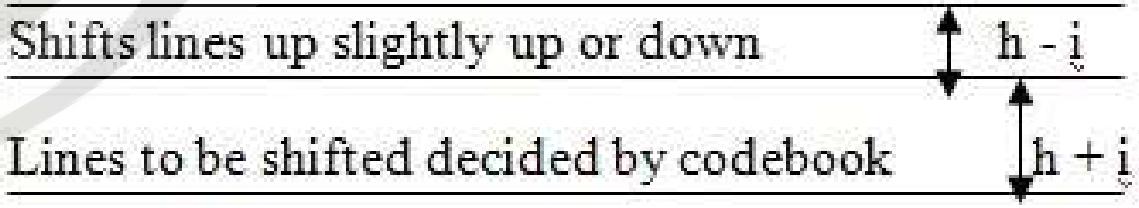


Fig: Line Shifting

(3)Feature coding:

- In feature coding method, some of the features of the text are altered.
- For example, the end part of some characters such as h, d, b or so on, are elongated or shortened a little thereby hiding information in the text.
- In this method, a large volume of information can be hidden in the text without making the reader aware of the existence of such information in the text.
- By placing characters in a fixed shape, the information is lost. Retying the text or using OCR program destroys the hidden information

Random and statistical generation:

- Random and statistical generation is generating cover text according to the statistical properties. This method is based on character sequences and words sequences

- **Character sequences:** The hiding of information within character sequences is character based information that is available and transmitted over networks. One approach to text steganography might hide information in what appears to be a random sequence of characters. Of course, to both the person sending and receiving the message, this sequence is far from random, but it must appear to be random to anyone who intercepts the message.
- **Word sequences:** To solve the problem of detection of non-lexical sequences, actual dictionary items can be used to encode one or more bits of information per word. This might involve a code-book of mappings between lexical items and bit sequences, or the words themselves (length, letters, etc.) might encode the hidden information.

Statistical generation of sequences

- Text mimicking: In addition to using the statistical frequency of letters or words in order to generate cover text, Wayner proposed a clever method of generating text which can be fairly convincing lexically and syntactically (and often semantically).
- One string is picked at random to start the steganographic text, and the next letter in the text is chosen by looking at a window of the last n – 1 characters in the steganographic text and finding all of the strings in the table which start with those characters.
- The next letter is chosen from the last letter of these strings by using the data structures from the Huffman compression algorithm in reverse;
- the statistical frequency of all of the possible next letters that end the strings that start with the desired n – 1 characters is used to generate a tree which uses the frequency of each of the selected strings to organize the last letters into an encoding tree

Text Steganography methods	Advantage	Dis-Advantage
Line shifting	This method is suitable only for printed text.	When OCR (character recognition program) applied the hidden information gets destroyed.
Word shifting	Word shifting method identify less because of change of distance between words to fill line is quite common.	The algorithm that related to word shifted distance, easily can get hidden data.
Syntactic Method	The amount of information to hidden the method is trivial.	Smart reader can find hidden data easily.
Semantic-based hiding	This method is better than above methods, syntactic, line shifting and word shifting because that cannot detect by retyping or using OCR programs.	Smart reader which has huge knowledge of words their synonyms or antonyms can discover it.
Abbreviation based hiding	This method is because it's a kind of any abbreviation present and we built also.	It is limited only for small data means out of large data. Only small part of data can be hidden.
Hiding Data using white spaces	One way of hiding data in text is to use white space. Due to the fact that in practically all text editors, extra white space at the end of lines is skipped over, it won't be noticed by the casual viewer.	In a large piece of text, this can result in enough room to hide a few lines of text or some secret codes.
Hiding Data in Paragraphs	The approach works by hiding a message using start and end letter of the words of a cover file. A word having same start and end letter is skipped. Since no change is made to the cover, the cover file and its corresponding stego file are exactly the same.	The volume of data hiding in the paragraph would be very less. The capacity of hiding the large volume of data leads to the challenge

Linguistic methods

- Linguistic method is a combination of syntax and semantics methods. Syntactic steganalysis is to ensure that structures are syntactically correct. In Semantic Method you can assign the value to synonyms and data can be encoded into actual words of text.

(1) Syntactic method: By placing some punctuation marks such as full stop (.) and comma (,) in proper places, one can hide information in a text file. This method requires identifying proper places for putting punctuation marks. The amount of information to hide in this method is trivial.

(2) Semantic method: This method uses the synonym of certain words thereby hiding information in the text. The synonym substitution may represent a single or multiple bit combination for the secret information. However, this method may alter the meaning of the text

Example of Text stenography

Minor changes to shapes of characters

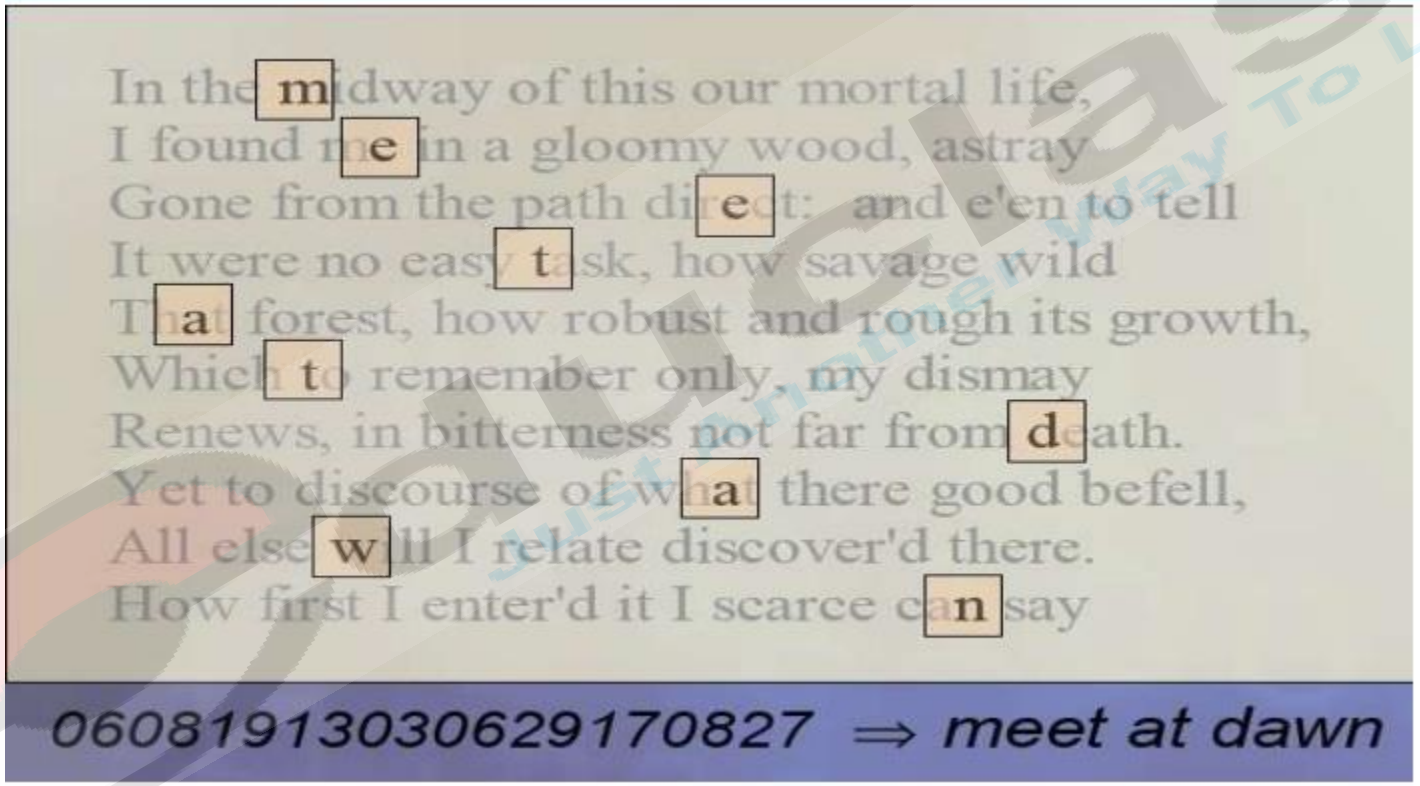
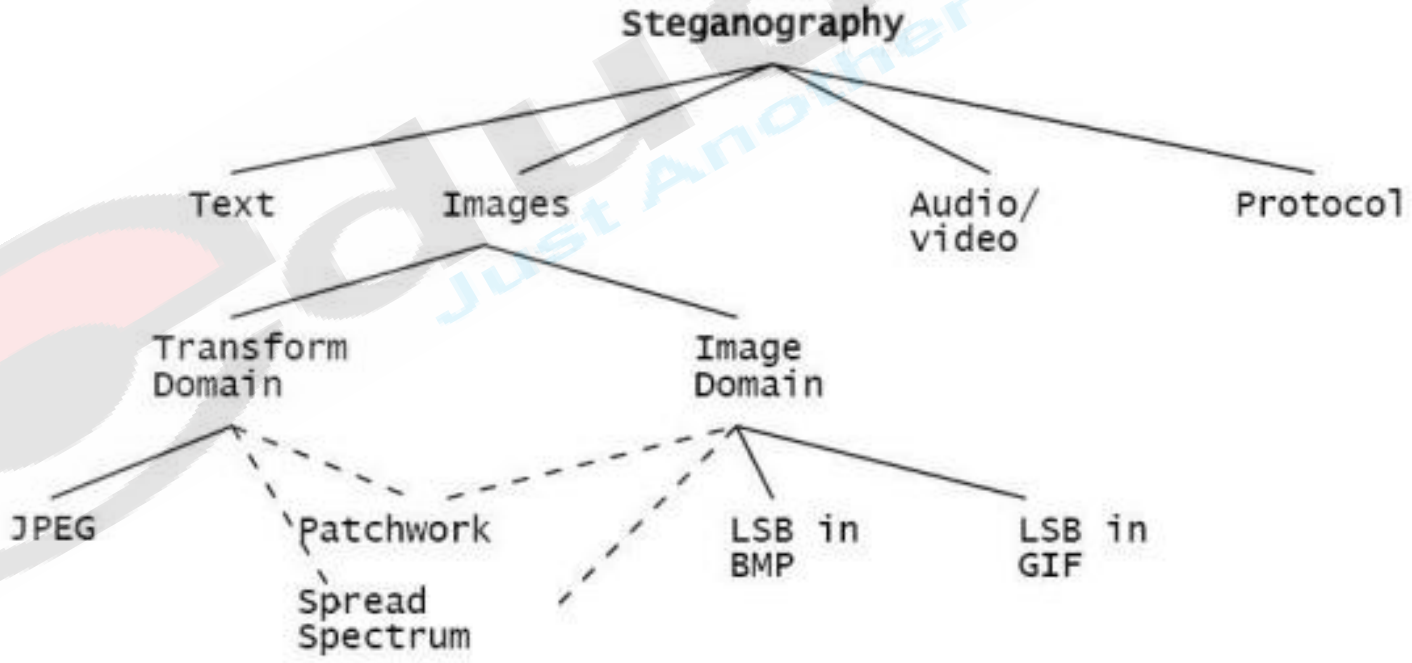
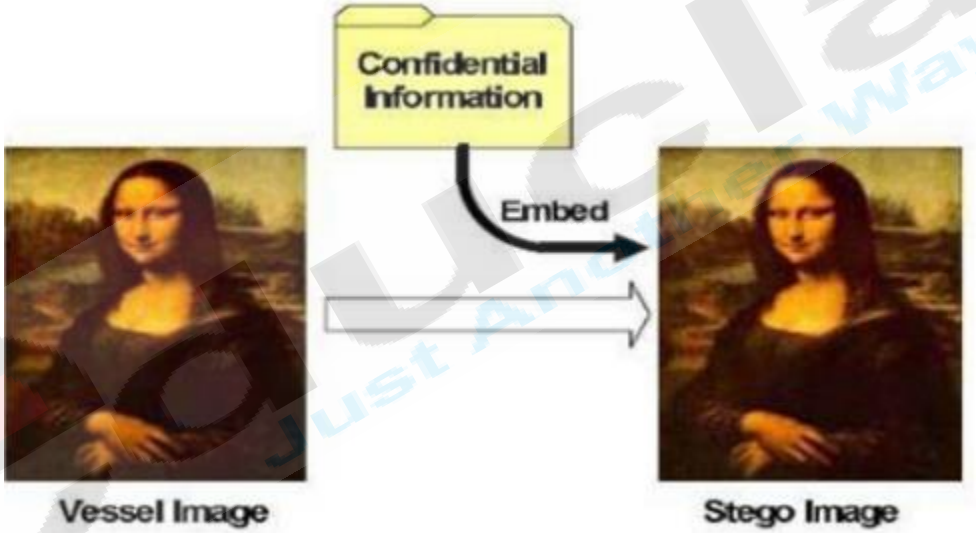


Image Steganography

- Using image files as hosts for steganographic messages takes advantage of the limited capabilities of the human visual system
- Some of the more common method for embedding messages in image files can be categorized into two main groups, image domain methods and transform domain methods





- Image Steganography requires following elements to carry out the work:
  - Cover medium: It is an image that holds secret message.
  - The Secret message: it is message to be transmitted. It can be plain or encrypted text, images or any other data.
  - The Stego-key: it is key used to hide the message (May or may not be used).

TECHNIQUES FOR USING IMAGE STEGANOGRAPHY

- By using LSB(Least Significant Bit algorithm)
- Masking and Filtering
- Algorithms and Transformation

The LSB algorithm

- The most common and popular method of modern day steganography is to make use of LSB of picture's pixel information.
- This technique works best when the file is longer than the message file and if image is grayscale.
- When applying LSB techniques to each byte of a 24 bit image,three bits can be encoded into each pixel.

The LSB algorithm

- The most common and popular method of modern day steganography is to make use of LSB of picture's pixel information.
- This technique works best when the file is longer than the message file and if image is grayscale.
- When applying LSB techniques to each byte of a 24 bit image,three bits can be encoded into each pixel.

- If the LSB of the pixel value of cover image C(i,j) is equal to the message bit SM of secret massage to be embedded, C(i,j) remain unchanged; if not, set the LSB of C(i, j) to SM.
- message embedding Procedure is given below:
- 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
- Where LSB(C(i, j)) stands for the LSB of cover image C(i,j) and "SM" is the next message bit to be embedded. S(i,j) is the stego image.

Example:

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

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.

Message: 01000001

Pixel 1: 11111000 11001001 00000010

Pixel 2: 11111000 11001000 00000010

Pixel 3: 11111000 11001001 00000011

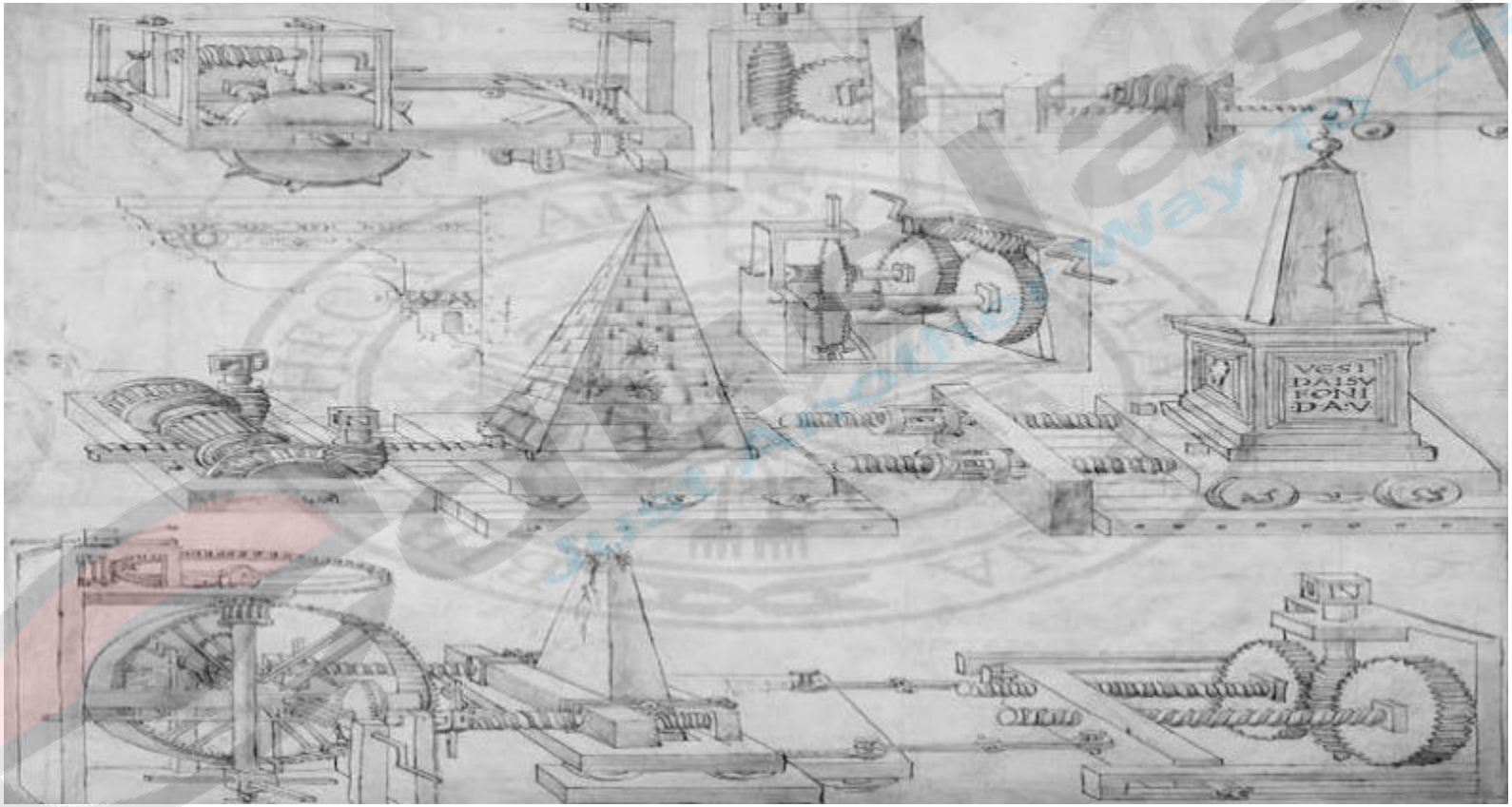
New image: 

MASKING & FILTERING

- Masks secret data over the original data by changing the luminance of particular areas.
- During masking, it embed the message within significant bits of the cover image.
- Not susceptible to lossy techniques because image manipulation does not affect the secret message.

MASKING & FILTERING - Uses

- Digital Watermarking – provides identification pertaining to the owner; i.e. license or copyright information.
- Fingerprinting – provides identification of the user; used to identify and track illegal use of content



Algorithm Transformation

- In the transformation methods, two things are considered:

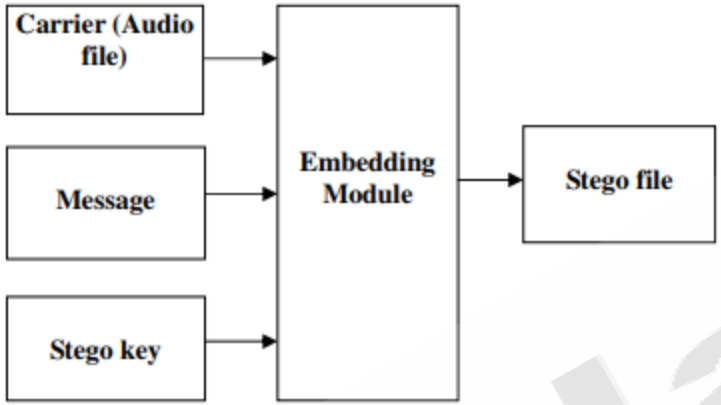
  (i) To accommodate the data of the payload, there is slight modification in the coefficients and

  (ii) The unused coefficients of the payload data are replaced.

Technique	Description	Features	Limitations
LSB Substitution	Data hides at the least significant bits of the pixel.	Less chances of degradation of the original image with more hiding capacity.	The data may be lost while doing image manipulation (compression), less robust, simple attacks could destroy the hidden data.
Masking and Filtering	It masks secret message over the cover image by changing the luminance i.e. embedding the message within significant bits.	It is more robust as compared to LSB substitution. It is used for lossy JPEG images as it is resistant to image compression, processing, cropping etc.	It can be detected by simple statistical analysis and tools.
Algorithm Transformation	Data is embedded in cover image by changing the coefficients of transform of the image.	Compression is used to reduce bandwidth, hence it is achieved by using quantization techniques and run length coding of the transformed coefficients. It increases the level of capacity and controls the compression ratio.	Some of the transformation techniques like FFT (Fast Fourier Transform) generates round off errors which is unsuitable for hiding process. Hence, large amount of data cannot hide as it causes degradation in the cover image.

Audio steganography

- The basic model of Audio steganography consists of Carrier (Audio file), Message and Password.
- Carrier is also known as a cover-file, which conceals the secret information.
- Message is the data that the sender wishes to remain it confidential. Message can be plain text, image, audio or any type of file.
- Password is known as a stego-key, which ensures that only the recipient who knows the corresponding decoding key will be able to extract the message from a cover-file.
- The cover-file with the secret information is known as a stego-file.



The information hiding process consists of following two steps.

i. **Identification of redundant bits in a cover-file. Redundant bits are those bits that can he modified without corrupting the quality or destroying the integrity of the cover-file. Message Stego key Embedding Module Stego file Carrier (Audio file)**

ii. **To embed the secret information in the cover file, the redundant bits in the cover file is replaced by the bits of the secret information**

METHODS OF AUDIO STEGANOGRAPHY

- Some commonly used methods of audio steganography are listed and discussed below in brief.
  1. Least Significant Bit (LSB) Coding
  2. Parity Coding
  3. Phase Encoding
  4. Spread Spectrum
  5. Echo Data Hiding

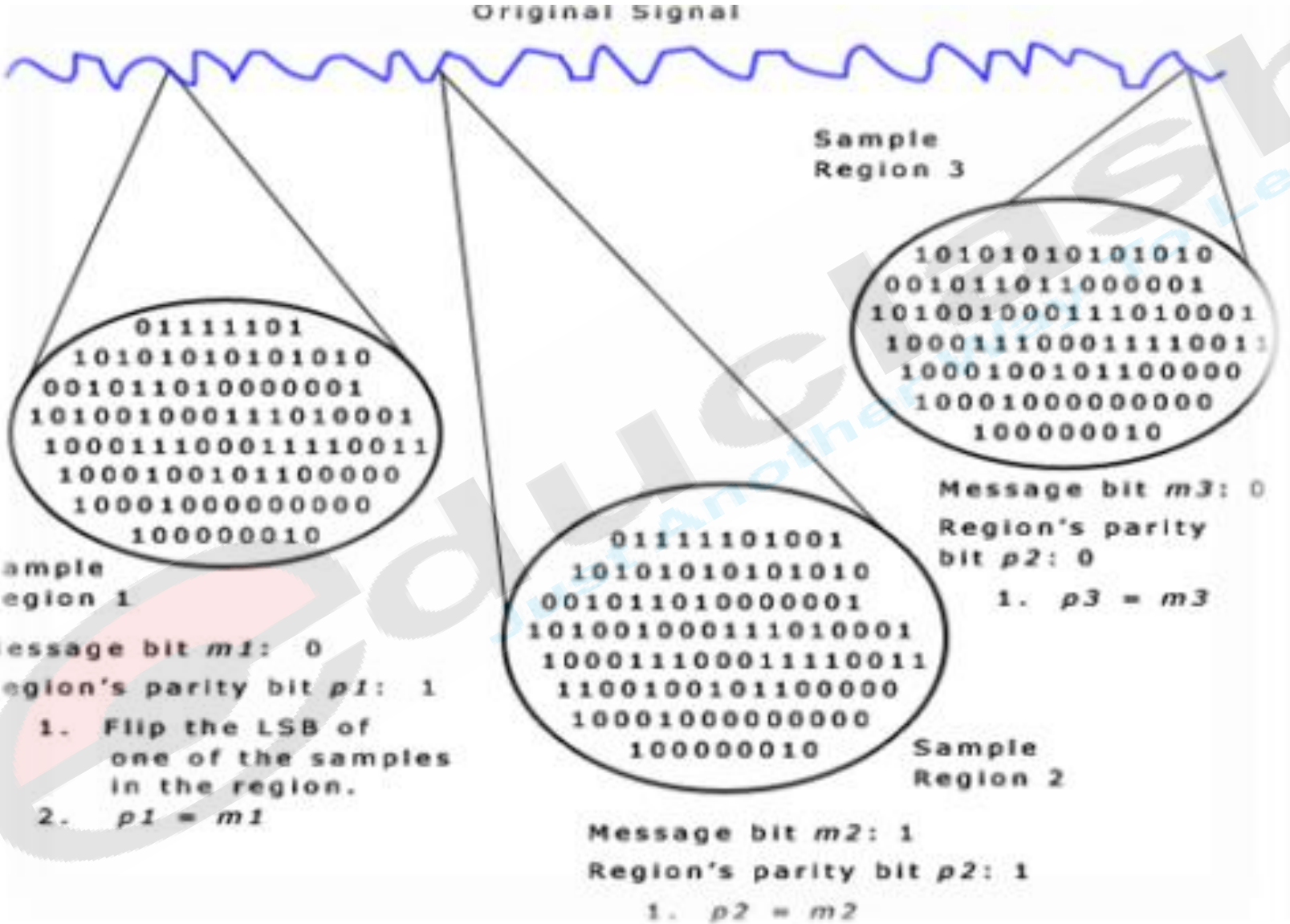
Least Significant Bit (LSB) Coding

- It is one of the earliest techniques studied in the information hiding of digital audio (as well as other media types) is LSB coding.
- In this technique LSB of binary sequence of each sample of digitized audio file is replaced with binary equivalent of secret message .
- The capacity is only one bit per sample of the cover audio which could be less for many applications.

Parity Coding

- In this method, Instead of breaking a signal down into individual samples, the parity coding method breaks a signal down into separate regions of samples and encodes each bit from the secret message in a sample region's parity bit.
- If the parity bit of a selected region does not match the secret bit to be encoded, the process flips the LSB of one of the samples in the region.
- Advantage: The sender has more of a choice in encoding the secret bit, and the signal can be changed in a more unobtrusive manner.
- Disadvantage: This method like LSB coding is not robust in nature. The capacity remains the same as that of LSB method.

- Parity coding is one of the robust audio Steganographic techniques.
- Instead of breaking a signal into individual samples, this method breaks an original signal into separate samples and embeds each bit of the secret message from a 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 the region.
- Thus, the sender has more of a choice in encoding the secret bit.



Phase Coding

- The block of phase spectrum as a place for embedding the message that gets from dividing the original signal of audio stream or carrier file, that is part of basic ide from phase encoding.
- Procedure of Phase Coding is:

  i. The original sound signal (C) segmented into the header of the signal. The rest is broken up into smaller segment whose have lengths equal to the size of the message that will be encoded into a cover media.

  ii. Applying each of segments to create a matrix of the phase is from Discrete Fourier Transform (DFT).

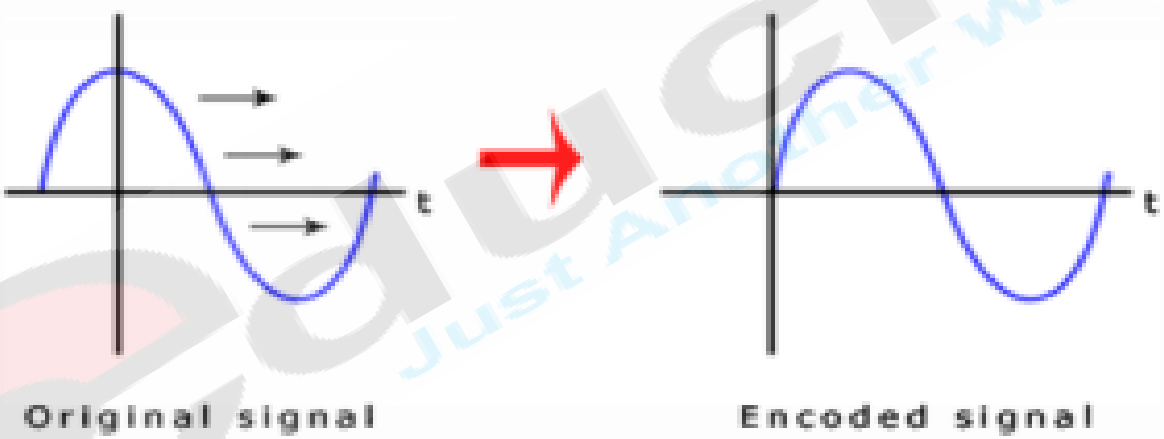
iii. The formula that can calculate the value of new phase with message bit condition as follows :

$$New\ Phase = \begin{cases} Old\ Phase + \frac{\pi}{2}\ if\ message\ bit = 0 \\ Old\ Phase - \frac{\pi}{2}\ if\ message\ bit = 1 \end{cases}$$

- Old phase is get from the original sound signal and message bit is the length of message that will encode into a cover media.

  iv. Using first segment and the original phase of matrix can create a new phase of matrix.

  v. Using the new phase of the matrix, the sound signals are reconstructed by applying an inverted DFT and then combine a segment of a sound in the original order.

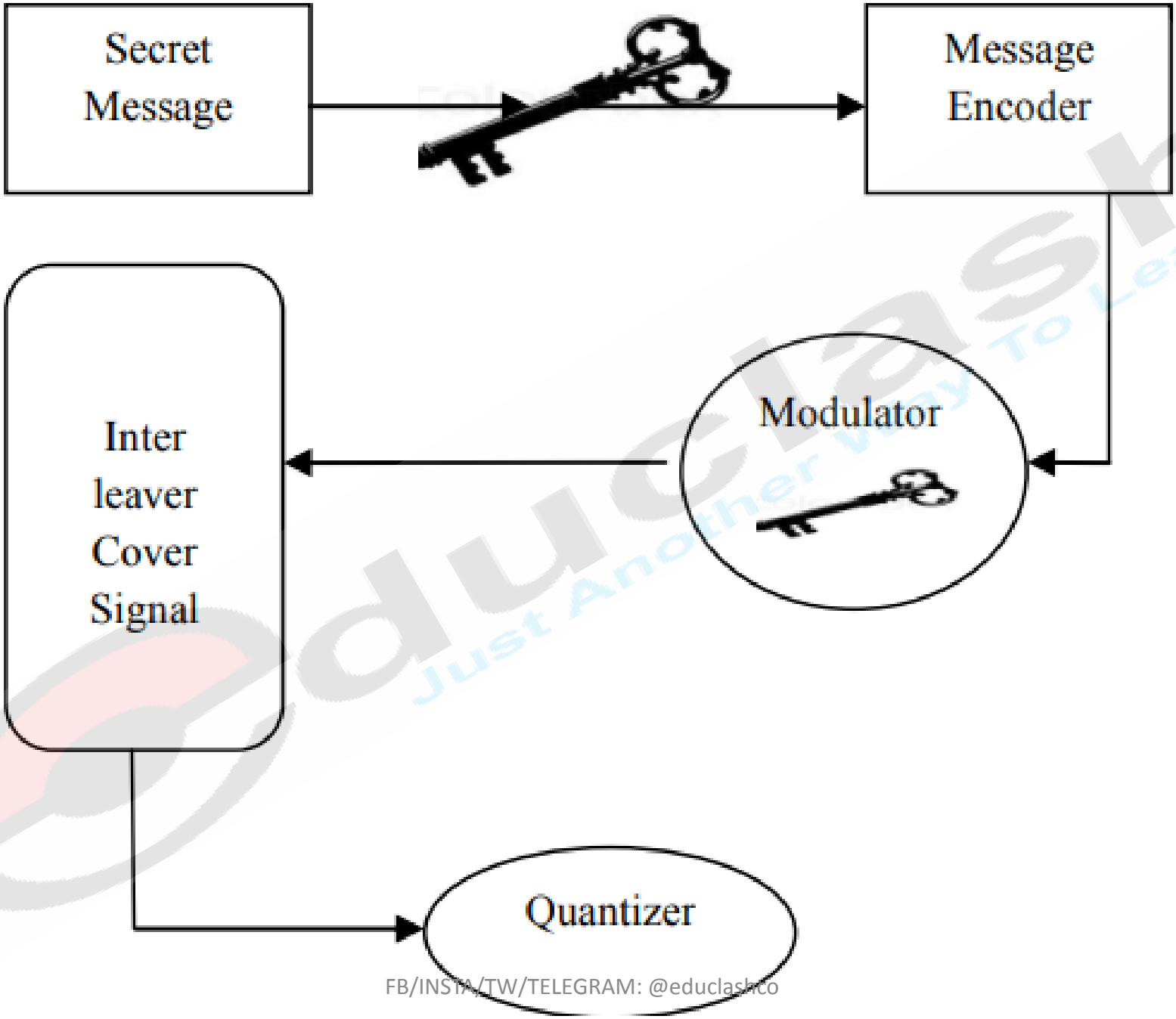


Spread Spectrum

- : In audio steganography, the basic spread spectrum (SS) method attempts to spread secret information across the frequency spectrum of the audio signal using a code which is independent of the actual signal.
- Two versions of Spread Spectrum can be used in audio Steganography:
- **Direct-sequence:** Direct-sequence SS attempts to spread out the secret message by a constant called the chip rate and then modulated with a pseudorandom signal and interleaved with the cover-signal.
- **Frequency-hopping schemes :** In frequency-hopping SS, the frequency spectrum of audio files is changed so that it hops rapidly between frequencies

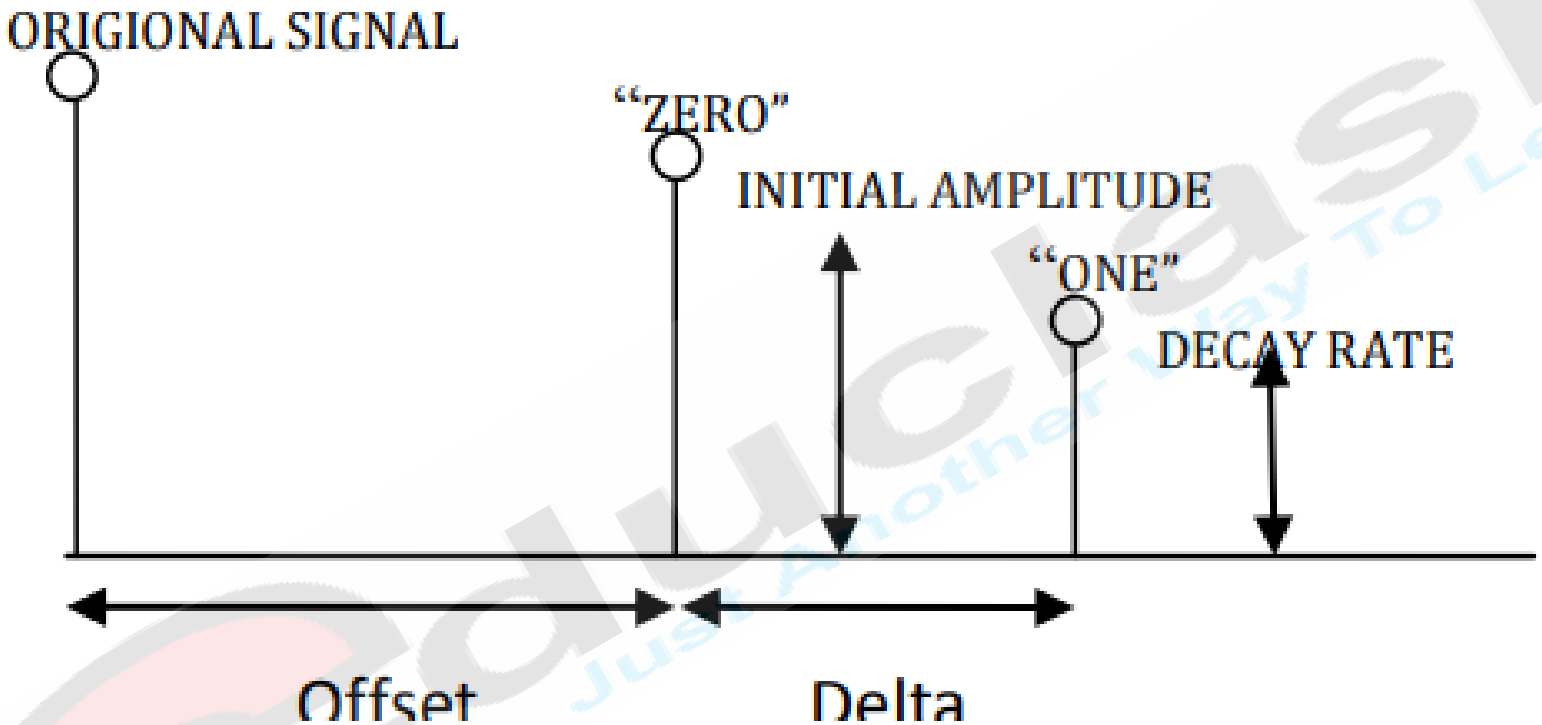
Steps of spread spectrum

a. The secret message is encrypted using a symmetric key k1.
b. Then encode encrypted message using a low rate error correcting code that increase overall robustness of the system.
c. The encoded message is then modulated with a pseudorandom signal that was generated using a second symmetric key.
d. The resulting random signal that contains the message is interleaved with cover signal.
e. The final signal is quantized to create a new digital audio file that contains the message.
f. This process is reversed for message extraction.



Echo Data Hiding

- The information is inserted by adding an echo sound to the cover file.
- Embedding data is expressed in terms of decay rate, initial amplitude and delay .
  a) The initial amplitude is used to determine the original data sound.
  b) Decay rate is useful for determination of echo function to be made.
  c) The Offset function is used to determine the distance between the original speech signals with the echo that has been made



One offset value represents a binary one, and a second offset value represents a binary zero.

Comparison Of Audio Steganography Teqniques

Methods	Embedding Techniques	Strengths	Weakness	Hiding Rate
Least Significant Bit	LSB of each sample in the audio is replaced by one bit of hidden information	Simple and easy way of hiding Information with high bit rate	Easy to extract and to destroy	16 Kbps
Echo Hiding	Embeds data by introducing echo in the cover signal	Resilient to lossy data compression algorithms	Low security and capacity	40-50 Bps
Phase Coding	Modulate the phase of the cover signal	Robust against signal processing manipulation and data retrieval needs the original signal	Low capacity	333 Bps
Parity Coding	Break the signal into separate samples and embeds each bit from secret message in sample region parity bit	Sender has more of a choice in encoding the secret bit.	Not Robust	320bps
Spread Spectrum	Spread the data over all signal frequencies	Provide better robustness	Vulnerable to time scale modification	20 Bps

Example

- Since everyone can read, encoding text in neutral sentences is doubtfully effective
- Since Everyone Can Read, Encoding Text In Neutral Sentences Is Doubtfully Effective
- ‘Secret inside’

Advantages

- The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages—no matter how unbreakable—will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.
- This method featured security, capacity, and robustness, the three needed aspects of steganography that makes it useful in hidden exchange of information through text documents and establishing secret communication.
- Important files carrying confidential information can be in the server in and encrypted form No intruder can get any useful information from the original file during transmit.
- With the use of Steganography Corporation government and law enforcement agencies can communicate secretly.

Limitation

- Huge number of data, huge file size, so someone can suspect about it. a. If this techniques is gone in the wrong hands like hackers, terrorist, criminals then this can be very much dangerous.