# AN OVERVIEW OF STEGANOGRAPHY: DATA HIDING TECHNIQUE

**Priya Pareek[1], N. Monica[2]**

*[1]Student, Department of Computer Science and Engineering, GMRIT, Rajam, India*
*[2]Student, Department of Computer Science and Engineering, GMRIT, Rajam, India*

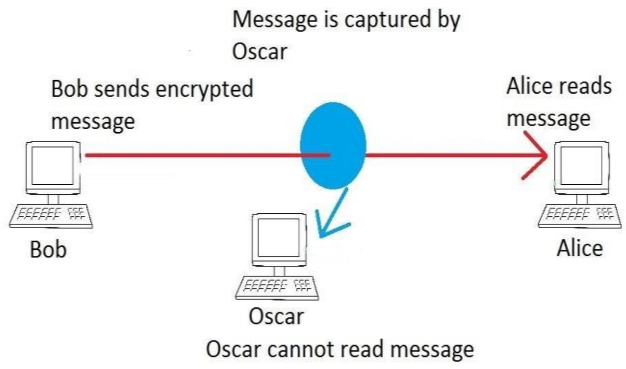
---

**Abstract -** *Steganography is a methodology which is used to hide the secret data in the form of embedded messages, simply it is covered by the other messages. The word Steganography is derived from two ancient Greek word names "Stegano"(which means hiding or covering) and "graph"(meaning to write). Steganography is very different from cryptography. Cryptography is a technique which is used to create or generate the code which keeps information very secure. In simple comparisons, cryptography is the one that cannot be decrypted without the proper knowledge of encrypted data key whereas, steganography is the one which can be easily used to encrypt or decrypt the data.*

***Key Words*: Steganography, Data hiding, Cryptography, Types of Steganography.**

## 1. INTRODUCTION

Steganography is a hiding technique which is used to hide important information. It accepts or includes the confidential report method in an unexpected manner. These methods include types of information like digital signatures, microdots, convert channels, invisible inks, spread spectrum communication, etc., In the below figure, initially, Bob wants to send the message to Alice so, Bob encrypts the message so that user can get the particular message perfectly. But, meanwhile sending the data some of the hackers(here in the below diagram Oscar) is waiting to receive the messages or data so, Bob encrypts the message and sent it to Alice. By sending the encrypted data no one is able to receive or retrieve the data before received by the receiver. This type of methodology is known as Steganography.


Message is captured by Oscar
Bob sends encrypted message
Alice reads message
Bob
Alice
Oscar
Oscar cannot read message

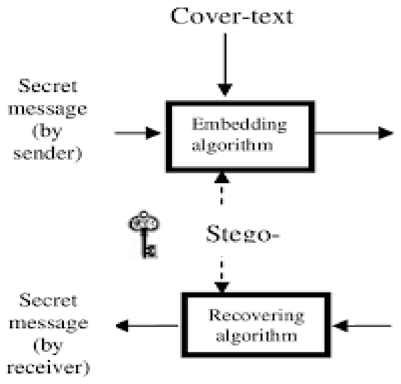
## 2. HISTORY:

Steganography was first developed in Ancient Greece around 440 BC. It describes the practice of writing messages and then inscribing that message in the underlying wood. The message was carved on the wood of wax tablet and it was covered with fresh wax, giving the appearance as the unused tablet. These tablets are transported without suspecting. An ancient Greek describes writing messages with the practice of melting wax of the wax tablet and then inscribing a message in the underlying wood. The message was covered with wax by reapplying. Later, Germans developed Microdot technology with the help of FBI Director J. Edgar Edgar Hoover. Microdots are photographs the size of a printed period and typewritten pages. The message was not hidden or encrypted. It has no attention. People have no idea and attention towards as it is very small. Microdots transmit the data in the form of drawings, photographs, or messages. Another form of invisible writing is through invisible inks. Messages are written with the help of invisible inks like fruit juices, milk, vinegar, and urine. All of these are visible when heated.

## 3. TYPES OF STEGANOGRAPHY:

### 3.1. Text Steganography:

It is one type of steganography which hides the message behind the other cover text file. It involves anything from changing the formatting of an existing text to random characters. This message can be hidden by some of the techniques by word shifting, line shifting. These techniques can be divided into categories:



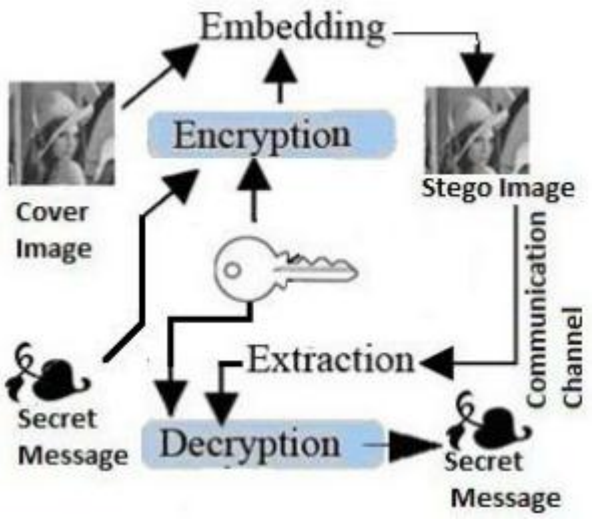
a) Format based techniques: The formatted text is changed to hide the original information. The information is written in a secret code. For example; one extra space is considered as 0 and two extra spaces are considered as 1. Word shifting is about adding the extra spaces between the words in which it can hide the data. Text resizing and change in a font style like bold, italic is used to hide the text hidden format. Line shifting is done only when it contains a huge amount of text in a file.

b) Statistical Techniques: The word sequences or character sequences can be used for the statistical generation of cover text. Generally, the character sequences appear to be random, but it hides the information. In word sequences, the bits of information is hidden by dictionary words.

c) Linguistics Techniques: In these methods, the syntax, and semantics are placed in order to hide the information. In syntactic methods, the punctuation marks like full stops or commas are used to hide the data. In semantic methods, the synonyms can be used to hide the secret code between words.

### 3.2. Image Steganography:

If the hidden data is an image file then it is called image steganography. The simplest method is to append the message to the end of the image. So the image is viewed by some image viewer application and the text at the EOF(end of file) is generally ignored. But, if the image is viewed in the text editor, the message can be read. The image steganography can be classified as spatial domain steganography and transform domain steganography.



a)Spatial domain steganography: The most common and simplest method used in image steganography is the least significant bit(LSB). It is used for embedding information in a cover image. The bits present in the image can be replaced by the hidden message. These changes cannot be identified by the human eye. The least significant bit can be changed. When using a 24-bit color image a bit of each of the red, green and blue color components can be used, so a total of 3 bits can be stored in each pixel. To insert a character only three bits are needed. Here, only half of the bits are used to hide the message effectively.

b)Transform domain steganography: It is used for hiding a large amount of data with high security. It hides the information in the frequency domain by altering magnitudes of Discrete Cosine Transform (DCT). The 2-D DCT transforms the image blocks from spatial domain to frequency domain. In this JPEG image steganography technique. One of the key characteristics of Steganography is the fact that information is hidden in the redundant bits of an object and since redundant bits are left out when using JPEG it was feared that the hidden message would be damaged. The JPEG compression algorithm has lossy and lossless stages. The lossy stage is used to hide the messages. It is not feasible to embed information which uses lossy compression, it would destroy the information in the process.

### 3.3. Audio Steganography:

The secret message is embedded into digitized audio. There are several methods are available in audio steganography.

a) Echo Hiding: This method embeds data or text into audio signals by adding a small echo to the host signal. The Nature of the echo is a resonance added to the host audio. If only one echo is produced from the original signal, then only one bit of information could be encoded.

b) Phase Coding: In this phase components of sound are not as perceptible to the human ear. It can be done by substituting the phase of an initial audio segment with a reference phase that represents the data. It encodes the message bits as phase shifts in the phase spectrum of a digital signal.

c) Parity Coding: This method breaks a signal down into different regions of samples and encodes each bit from the secret message in a sample region's parity bit. If the parity bit of the selected region does not match the secret bit to be encoded.

d) Spread Spectrum: It spreads the message bits over the entire sound file. It is used to encode a category of information by spreading the encoded data across the frequency spectrum.

e)Tone insertion: In this inaudibility of lower power tones in the presence of significantly higher ones. Tone insertion method can resist attacks such as low-pass filtering and bit truncation addition to low embedding capacity

### 3.4. Video Steganography:

The main aim of video steganography is to hide the data from others and main secrecy of which is going to be transmitted. The messages do not know the third person. The message is unknown to others except for sender and receiver. It is of hiding the information within other video information such that there is no change in the cover information. Generally, humans have some weaknesses in the Human Vision System(VHS). Due to these weaknesses, a human cannot observe very minor changes in the vision. So, the data can be hidden from other people with the help of videos. A video contains various frames which can be played back the video at fixed frame rates. The video size can also be compressed by some techniques.

## 4. CONCLUSION:

Steganography is a technique which is used to hide the information but there is no guarantee of hiding the complete information without proper security. The data can be stored in different formats like image, video, audio, etc., as discussed earlier in this paper. In recent years, hiding the data with confidentiality is more important so many of the people are showing interest towards the Steganography.

## 5. REFERENCES:

1. Arvind Kumar and Km. Pooja. Article: Steganography- A Data Hiding Technique. *International Journal of Computer Applications* 9(7):19–23, November 2010. Published By Foundation of Computer Science.

2. Harjit Singh, "Analysis of Different Types of Steganography". International Journal of Scientific Research in Science, Engineering, and Technology.IJSRSET | Volume 2 | Issue 3. 2016

3. http://ijsrset.com/IJSRSET1623161

4. Maninder Singh Rana, Bhupender Singh Sangwan, Jitendra Singh Jangir, "Art of Hiding: An Introduction to Steganography", International Journal Of Engineering And Computer Science Volume-1 Issue 1 Oct 2012 Page No. 11-22

5. http://www.webtorials.com/main/eduweb/security/tutorial/steg/steg.pdf

6. Masoud Nosrati, Ronak Karimi, Mehdi Hariri "An introduction to steganography methods", World Applied Programming, Vol (1), No (3), August 2011. 191-195 ISSN: 2222-2510 ©2011

7. https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2004-13.pdf

8. Saritha Namboodiri, Shilpa Rajan "Steganography in Putative Protein Coding Regions of Eukaryotic DNA: A Novel Approach", International Journal of Advanced Research in Computer Science and Software Engineering 3(9), September - 2013, pp. 523-533

9. http://shodhganga.inflibnet.ac.in/bitstream/10603/141644/9/09_chapter%201.pdf

10. https://www.researchgate.net/profile/Merrill_Warkentin/publication/315910035_Steganography_Forensic_Security_and_Legal_Issues/links/5909d633a6fdcc49616f038c/Steganography-Forensic-Security-and-Legal-Issues.pdf

11. Jayati Bhadra, A.M. Bojamma, Prasad .C.N., M.N. Nachappa "An Insight to Steganography" - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 10, December 2014. found online at (http://www.ijiset.com/v1s10/IJISET_V1_I10_06.pdf)

12. Chin-Chen Chang, Yuan-Chang Lin, and Yuan-Hui YU, "A new Steganographic method for color and grayscale image hiding", Computer Vision and Image Understanding, 20 December 2006.

13. Mr. Falesh M. Shelke, Miss. Ashwini A. Dongre, Mr. Pravin D. Soni3 "Comparison of different techniques for Steganography in images" - International Journal of Application or Innovation in Engineering & Management (IJAIEM). Volume 3, Issue 2, February 2014 ( https://www.ijaiem.org/volume3issue2/IJAIEM-2014-02-27-062.pdf )

14. Navneet Kaur, Sunny Behal "A Survey on various types of Steganography and Analysis of Hiding Techniques" - International Journal of Engineering Trends and Technology (IJETT) – Volume 11 Number 8 - May 2014 (http://www.ijettjournal.org/volume-11/number-8/IJETT-V11P276.pdf)

15. Kamred Udham Singh Int. "Video-Steganography: Text Hiding In Video By LSB Substitution" Journal of Engineering Research and Applications www.ijera.com ISSN: 2248-9622, Vol.4, Issue 5 (Version1), May 2014, pp.105-108 http://www.ijera.com/papers/Vol4_issue5/Version%201/S4501105108.pdf