MAT JOURNALS

Journal of Android and IOS Applications and Testing

Volume 1 Issue 3

# A Review on Steganography – Hidden Information

***Susmita Thombre, Apurva Mohite***

Department of Computer Science & Engineering, MGM's Jawaharlal Nehru Engineering College, Aurangabad, MH, India

**E-mail:** thombresusmita@gmail.com

***Abstract***

*Steganography is that the art of and science of writing hidden messages in such the simplest way that nobody, except for sender and supposed recipient suspects the existence of message. Many alternative carrier file formats is used, however, digital pictures are the foremost common one. For concealing secret data in pictures, there exists an outsized sort of steganography techniques some are a lot of complicated than others and every one of them have various sturdy and weak points. Steganography is thought of as data importing. Each recipient and sender should skills to rewrite the hidden message. This can be done by exploitation key. Totally different applications could need absolute physical property of the key data. This project report intends to provide an outline of image steganography, its uses and techniques. It additionally tries to spot the wants of an honest steganography algorithmic program and shortly reflects on that steganographic techniques are a lot of appropriate that applications. Steganography is that the observe of concealing non-public or sensitive data inside one thing that seems to be nothing resolute the standard. Steganography is commonly confused with cryptanalysis as a result of the two is similar within the manner that they each are will not to defend necessary data. The distinction between two is that steganography involves activity data, therefore, it seems that no data is hidden the least bit. If an individual or persons views the item that the data is hidden inside he or she is going to have not any concept that there is any hidden information, thus the person would not conceive to decipher the knowledge. What Steganography primarily will is exploit human perception, human senses do not seem to be trained to seem for files that have data inside them, though this software package is on the market which will do what is known as Steganography. The foremost common use of steganography is to cover a file within another file. Steganography tools for activity data includes any kind of data file and image files and, therefore, the path wherever the user desires to avoid wasting image and extruded file.*

***Keywords:*** *Steganography, information, image, message, application*

## METHODOLOGY

User has to run the applying. The user has two tab choices–encrypt and decrypt. If user choose encrypt, application offer the screen to pick out image file, info file and choice to save the image file. If user choose decrypt, application offers the screen to pick out solely image file and raise path wherever user need to save lots of the secrete file. This project has two strategies–write and rewrite. In coding the secrete info is activity in with any sort of image file. Decryption is obtaining the secrete info from image file.

The encrypt module is used to hide information into the image; no one can see that information or file. This module requires any type of image and message and gives the only one image file in destination.

The decrypt module is used to get the hidden information in an image file. It take the image file as an output, and give two file at destination folder, one is the same image file and another is the message file that is hidden it that [1].

## GRAPHICAL REPRESENTATION

The graphical representation of

Steganography system is as follows:

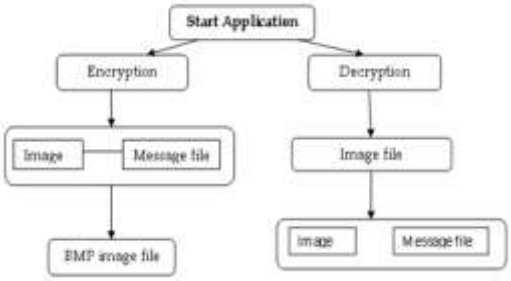



***Fig. 1:*** *Graphical Representation.*

This project report intends to give an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good steganography algorithm and briefly reflects on which Steganography techniques are more suitable for which application.

## HISTORY

- 480 B.C.: Wooden Tablets and Beeswax
- 494 B.C.: Head Tattoo
- 1558: Hidden Messages in Hard Boiled Eggs
- 1585: Beer Barrel
- 1680: Musical notes
- 1800s: Newspaper Code
- 1915: Invisible Link
- 1941: Microdots
- 1980s: Thatcher's Watermarking
- 1990s: Digital Steganography
- 2003: Network Steganography
- VoIP Steganography

## INTRODUCTION

The word steganography virtually means that lined writing as derived from Greek. Steganography is that the art of concealing the existence of knowledge while not on the face of it innocuous carriers. In broad sense, term steganography is employed for concealing message inside a picture. Steganography is that the art and science of human action during a means that hides the existence of the communication. In distinction to cryptography, wherever, the "enemy" is allowed to sight, intercept and modify messages while not having the ability to violate bound security premises secure by a cryptosystem, the goal of steganography is to cover message within alternative "harmless" messages during a means that does not permit any "enemy" to even sight that there is a second secret message gift. Steganography is in the literature also referred to as transmission security of short TRANSEC [2, 3].

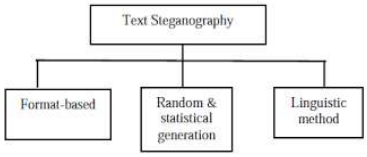
### Microdots

- The Germans developed microdots technology.
- Microdots are photographs the size of printed period having clarity of standard-sized typewriting pages.
- The first microdots were discovered masquerading as a period on a typed envelope carried by German against in 1941.
- The message was not hidden, nor encrypted.
- It was just small as to not draw attention to itself (for a while).
- Besides being so small, microdots permitted the transmission of large amounts of data including writing and photographs.

Recently, computerized steganography has become popular. Using different methods of encoding, secret messages can be hidden in digital data, such as .bmp or .jpg images, .wav audio files, or e-mail messages. These methods are described below. Authors are able to watermark their property in this manner. Unfortunately, steganography is also suspected to play a role in the communication among terrorist groups around the world. In the past year, several suspected that Osama Bin Laden may have been posting images on EBay with hidden messages inside to send to different terrorist groups [4]. Recent attempts to detect the presence of such images on EBay have not uncovered anything, though.

**Types of Steganography**

- Message in Text.




- Messages in Still Images.
- Messages in Audio (data is hidden in layer lll of encoding process of mp3 file. Messages in audio are always sent along with ambient noise).
- Messages in Video (embedding information into multimedia data).
- Hidden Messages on Messenger's Body (hidden by the hair that afterwards grew over it, and exposed by shaving the head).

**Examples**

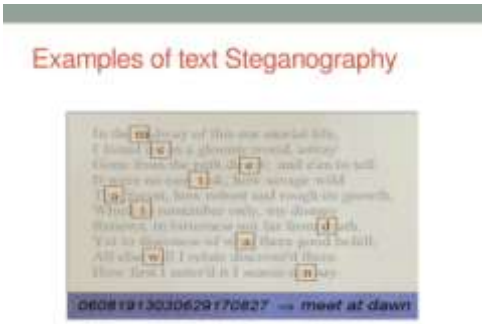


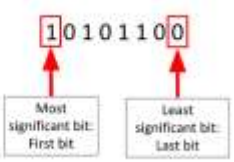

***Fig. 2:*** *Text Steganography.*

**LSB Method**

- Most common form of digital steganography.
- In a RGB, information is hidden in the LSB[s] of the RGB values of each pixel.
- In a 24-bit bitmap, each pixel represented by 3 bytes.

  8 bits representing red value= 2^8=256 shades of RED
  8 bits representing green value= 2^8=256 shades of GREEN
  8 bits representing blue value= 2^8=256 shades of BLUE

  16,777,216 possible colors
  - Effectively have 3-4 bits of data to hide information in for every pixel
  - Required for ASCII character

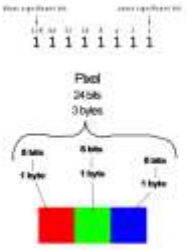



**Color Perception**

- Changing the LSB of Red value by 1 (in 24 bit color depth) is undetectable by the human eye.

  Nokia 808 pure view: 41 megapixel camera phone.

41 megapixels (3 pixel/byte) = 13.66MB of data can be hidden in a single image.




**Digital Steganography**

- The art of hiding data in a file so that only the sender and intended recipient suspect the presence of hidden data.
- A form of security through obscurity.
- Very easy to accomplish.
- Hardest to detect and decrypt.
- BMP, JPG, TXT, HTML/XML, PDF, PNG, GIF, AU, WAV, MP3, AVI, TIF, DLL, EXE.
- With digital steganography hackers can embed all sorts of an unsuspecting user. Typically an image file is attached to an email with an attractive header, the user clicks on it and the embedded file goes executed.


***Fig. 3:*** *Digital Steganography.*

**Network Steganography**

- Modifying network packet's header or payload.
- In TCP/IP networks, unused bits in the IP and TCP header may be used.
- Packet based length steganography.
- Manipulation of the MTU (maximum transmission unit).
- VOIP- Lost Audio Packets Steganography Method (LACK).
- Transmitter intentionally delays packets by an "excessive" amount of time.

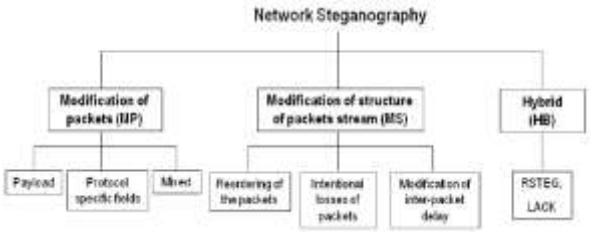
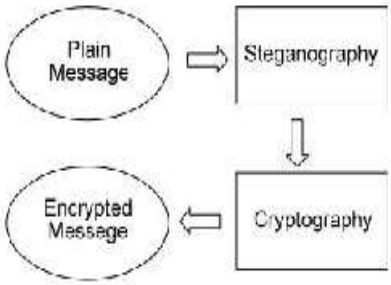



***Fig. 4:*** *Network Steganography.*

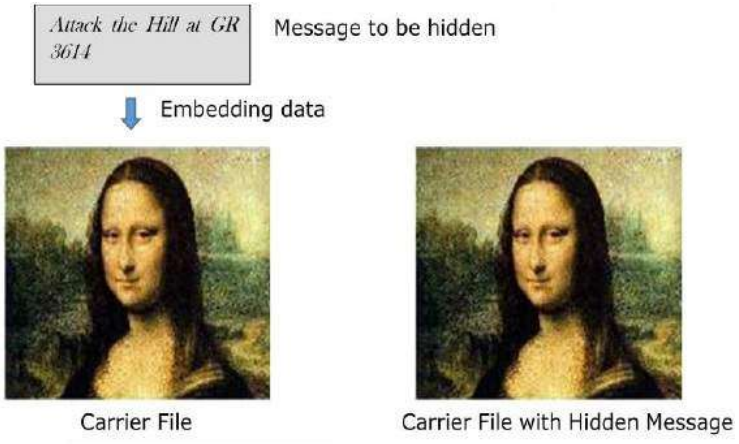
**Steganography vs. Cryptography**

- Steganography can be viewed as akin to cryptography.
- Both have been used throughout recorded history as means to protect information.
- At times these two technologies seem to converge while the objectives of two differ.




- Cryptographic techniques "scramble" messages so if intercepted, the messages cannot be understood.
- Steganography, an essence, "camouflages" a message to hide its existence and make it seem "invisible" thus concealing the fact that a message is being sent altogether.

- Camouflage is also a nice steganography tool that lets you hide any type of file inside of file



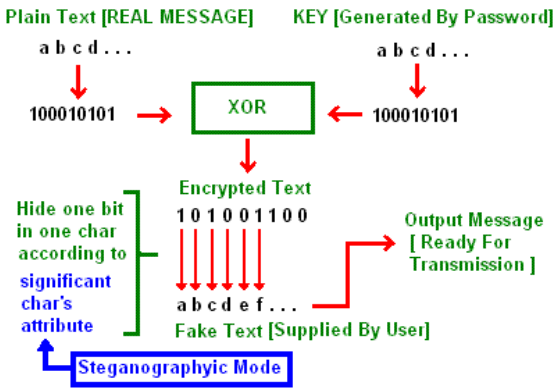

**Advantages of Steganography**

- It can be used for safeguarding data, such as in the field of media where copywriting ensures authentically.
- It can be used by intelligence agencies for sending secret data.
- Action or process of writing in shorthand and transcribing the shorthand on a typewriter.
- It is used in the way of hiding not the information but the password to reach that information.

**Applications**

- Used in modern printers**:** Some modern computer printers use steganography, including HP and Xerox brand color laser printers. These printers add tiny yellow dots to each page. The barely-visible dots contain encoded printer

serial numbers and date and time stamps.
- Confidential communication and secret data storing.
- Protection of data alteration.
- Access control system for digital content distribution.
- Media database system.
- Confidential communication and secret data storing.
- Protection of data alteration.
- Access control system for digital content distribution.
- Media Database systems.




## Fields of Applications

- Defense and Intelligence.
- Medical.
- On-line Banking.
- On-line Transactions.
- To Stop Music Piracy.
- Other Financial and Commercial Purposes.

## Techniques

- Hidden messages within wax tablet-in ancient Greece, people wrote messages on wood and covered it with wax that bore an innocent covering message.
- Hidden messages on messengers body-also used in ancient Greece. Herodotus tells the story of a message tattooed on the shaved head of a slave of Histiaeus, hidden by the hair that afterwards grew over it, and exposed by shaving the head. The message allegedly carried a warning to Greece about Persian invasion plans. This method has obvious drawbacks, such as delayed transmission while waiting for the slave's hair to grow, and restrictions on the number and size of messages that can be encoded on one person's scalp.
- During World War II, the French Resistance sent some messages written on the backs of couriers in invisible ink.
- Hidden messages on paper written in secret inks, under other messages or on the blank parts of other messages.
- Messages written in Morse code on yarn and then knitted into a piece of clothing worn by a courier.
- Messages written on envelopes in the area covered by postage stamps.
- In the early days of the printing press, it was common to mix different typefaces on a printed page due to the printer not having enough copies of some letters in one typeface. Because of this, a

message could be hidden using two (or more) different typefaces, such as normal or italic.

- During and after World War II, espionage agents used photographically produced microdots to send information back and forth. Microdots were typically minute (less than the size of the period produced by a typewriter). World War II microdots were embedded in the paper and covered with an adhesive, such as collodion. This was reflective, and thus, detectable by viewing against glancing light. Alternative techniques included inserting microdots into slits cut into the edge of post cards.
- During WWII, Velvalee Dickinson, a spy for Japan in New York City, sent information to accommodation addresses in neutral South America. She was a dealer in dolls, and her letters discussed the quantity and type of doll to ship. The stegotext was the doll orders, while the concealed "plaintext" was itself encoded and gave information about ship movements, etc. Her case became somewhat famous and she became known as the Doll Woman.
- Jeremiah Denton repeatedly blinked his eyes in Morse Code during the 1966 televised press conference that he was forced into as an American POW by his North Vietnamese captors, spelling out "T-O-R-T-U-R-E". This confirmed for the first time to the U.S. Military (naval intelligence) and Americans that the North Vietnamese were torturing American POWs.
- Cold War counter-propaganda. In 1968, crew members of the USS Pueblo intelligence ship held as prisoners by North Korea, communicated in sign language during staged photo opportunities, informing the United States they were not defectors, but captives of the North Koreans. In other photos presented to the US, crew members gave "the finger" to the unsuspecting North Koreans, in an attempt to discredit photos that showed them smiling and comfortable.

## CONCLUSION

- Steganography is the art of hiding sensitive data without generating unneccessary curiosity and suspition among foreign party.
- Steganalysis is the technique to detect steganography.
- Steganography ancient but still very much in use
- Assure the integrity of hiden message in the case of packet loss will be the future work.
- Cryptography: security through encryptography.
- Steganography: security through obsecurity.

## REFERENCES

1. Wayner, Peter. Disappearing cryptography: information hiding: steganography &

watermarking. Amsterdam: *MK/Morgan Kaufmann Publishers*; 2002.

2. Wayner, Peter. Disappearing cryptography 3rd Edition: information hiding: Steganography & watermarking. *Amsterdam: MK/Morgan Kaufmann Publishers*; 2009.
3. Petitcolas, Fabien A.P., Katzenbeisser, Stefan. Information hiding techniques for steganography and digital watermarking. *Artech House Publishers*; 2000.
4. Johnson, Neil, Duric, Zoran, Jajodia, Sushil. Information hiding: Steganography and watermarking: attacks and countermeasures. *Springer*; 2001.