# DIGITAL IMAGE STEGANALYSIS FOR COMPUTER FORENSIC INVESTIGATION

Nanhay Singh, Bhoopesh Singh Bhati, R. S. Raw

Ambedkar Institute of Advanced Communication Technologies and Research, Delhi, India
nsingh1973@gmail.com,
bhoopeshcse@yahoo.com,
rsrao08@yahoo.in

***ABSTRACT***

*This paper presents study about how to hide the useful information and give the superficial knowledge of Steganography, compare encryption, and cryptography. This paper describes the present, past and future of Steganography. In this paper, we introduce Steganalysis for computer forensic investigation. Digital forensics is helpful in investigation of the cyber-crime and computer crime. With the help of Steganalysis, it detect the hide message which is transfer in the network. Furthermore, we have described the security system classification.*

***KEYWORDS***

*Steganography, Steganalysis, Steganography History, Digital Image Forensics, Cryptography*

## 1. INTRODUCTION

Information security is most challenging issues nowadays. Information or message is being exchanged over various types of network. Communication channel is not secure due to the presence of hacker who is waiting for a chance to gain access the confidential data then use this technique to secure the information or messages is called Steganography. Steganography is a process of concealing the massages in a cover without leaving a remarkable trace is known as Steganography. To detect the hidden message in Steganography is Steganalysis. It is an art and science of detecting messages hidden using Steganography. It is used to detect and to identify suspected packages, determine whether they have a payload encoded into them, or not and, if possible, recover that payload. Steganalysis is the technique for searching and finding the occurrence of message which is hidden [11]. Steganalysis as destroying the information which is kept secret it can be performed even if there is no idea of secret information. However forensic is about searching the information. Sometime it is reasonable to do so. It is due to the reason because sometime finding secret information is very tough and sometime not possible without having knowledge of concept which was used for stegnography. Even if you discover the tool which was used for stegnography finding the secret information is still very tough because most technique employ the cryptographic technique to scramble the secret text. This scheme was possible in classical Steganography system where the security depends on the secrecy of encoding

David C. Wyld, et al. (Eds): CCSEA, SEA, CLOUD, DKMP, CS & IT 05, pp. 161–168, 2012.
 DOI : 10.5121/csit.2012.2217

technique [12]. Many researchers have looked for the way to represent the steganography and future of steganography. Some of them have said that Steganalysis is the technique for digital forensic investigation.

### 1.1 Historical Evolution of Steganography

The Steganography means the covered or the hidden writing. In 480 BC a Greek by the name of Demaratus sent a message to the Spartans with a warning of a pending invasion by Xerxes. In 15th century the use of Steganography dates came back after several millennia.

Nowadays the emphasis has been on various forms of digital Steganography. Commonly there are a number of digital technologies that the community is concerned with, namely text files, still images, movie images, and audio. It is beyond the scope of this paper to go into the details of Steganography methods in two ways one is the image domain and second is the transform domain

The future of Steganography is bright for security purpose. Steganography techniques have obvious uses, some legitimate. The business case for protection of property, real and intellectual is strong. Other uses for Steganography range from the trivial to the abhorrent. There are claims that child pornography may be lurking inside innocent image or sound files. While this is entirely possible, a search on the internet for confirmation of this claim was unsuccessful. Steganography could be used, especially for considering the broad term “criminal communications.” If one includes Steganography techniques other than computer related, the potential grows even more.

The rest of the paper is organized as follows: Section 2 consist of steganography, Categorization of security system and comparison between encryption and steganography. Section 3 details Digital Image Steganalysis for Computer Forensic Investigation.. Finally, concluding remarks are drawn in section 4.

## 2. STEGANOGRAPHY AND STEGANALYSIS

Steganography is the way to provide the security when data is transferred in the network. Steganography word came out from Greek, literally means covered writing [1]. It is an art of hiding information in the way to prevent the detection of hidden messages. In this way we hide the information through some multimedia files. These multimedia files can be audio, image or video. The purpose of Steganography is to covert communication to hide the confidential information from unauthorized user or the third party. In this process if the feature is visible, the point of attack is evident thus the goal here is always to give chances to the very existence of embedded data. The security issues and top priority to an organization dealing with confidential data the method is used for security purpose as the burning concern is the degree of security. The security system is categorized into two parts [2]:-

### 2.1 Information Hiding

Steganography is a technique to hide the information in digital media. Besides hiding data for confidentiality, this approach of information hiding can be extended to copyright protection for digital media; audio, video, and images. Therefore, the confidentiality and data integrity are required to protect it against unauthorized access and use. This has resulted in an explosive growth of the field of information hiding.

Information hiding is classified through Steganography and watermarking. Watermarking is an application where the message contains information such as owner identification and a digital time stamp, which is usually applied for copyright protection. Information hiding is categorized into the following ways [7]:-

I. Steganography
II. Watermarking

## I. Steganography

Steganography is hiding the information through multimedia application like images, audio and digital. The host data is corrupted but hidden data in invisible when an unauthorized person analysis those data. The Steganography goal is securely communication channel is completely unpredictable. Steganography technique is classified into two further types [10]:-

i. Technical Steganography
ii. Linguistic Steganography

### i. Technical Steganography

In this technique, we use invisible ink or microdots and other sizes reduction methods. This is a scientific method to hide data .Technical Steganography is used in the following technique:-

**a)** **Video Steganography:** In this technique, we can easily hide large data file in the video Steganography. Video file is generally a collection of images and sounds. Any small but otherwise noticeable distortion might go by unobserved by humans because of the continuous flow of information.

**b)** **Audio Steganography**: In this technique, secret messages are embedding in digital sound. The secret message is embedded by slightly altering the binary sequence of a sound file. Existing audio Steganography software can embed messages in WAV, AU and even MP3 sound files.

**c)** **Text Steganography:** In text Steganography the message is hidden in the text and we use the different method to hide the message in text by changing the last bit of the message. Sometime one sentence in ten times and use blank space in alphabet terms is used.

**d)** **Image Steganography:** In this technique, hide information; straight message insertion may encode every bit of information in the image. The messages may also be scattered randomly throughout the images. A number of ways exist to hide information in digital media.

**e)** **Protocol Steganography:** In this technique, Steganography can be used in the layer of OSI network model and cover channels protocols. Steganography is referred to the techniques of embedding information within messages and network control protocol used in network transmission. The information is adding in TCP/IP header and sends in the network.

**ii. Linguistic Steganography:**

This technique hides the message within the carrier in some non-obvious ways. It is categorized into two ways:-

a) **Semagrams:** Semagrams use some symbols and signs to hide the information .it is further categorized into two ways:

   a. **Visual Semagrams:** A visual semagram uses innocent-looking or everyday physical objects to convey a message, such as doodles or the positioning of the items on a web site.
   b. **Text Semagrams:** This hides a message by modifying the appearance of the carrier text, such as subtle changes in font size or type, adding extra space, or different flourished in letters or handwritten text

b) **Open Code:** This hide a message within a legitimate carrier message in the ways that are not obvious to an unsuspecting observer [6].

   a. **Jargon:** This is one type of language which is meaningless to other but can be understood by group of people. Only Jargon codes include symbols used to indicate the presence and type of wireless network signal, underground terminology, or an innocent conversation that conveys special meaning because of the facts that are known to the speakers only. A subset of jargon codes are cue codes, where certain pre-arranged phrases convey meaning.
   b. **Covered Cipher***:* Covered or concealed ciphers hide a message openly in the carrier medium so that it can be recovered by anyone who knows the secret for how it was concealed.
      - **Null Cipher** A null cipher hides the message according to some prearranged set of rules, such as "read every fifth word" or "look at the third character in every word."
      - **Grille Cipher** A grille cipher employs a template that is used to cover the carrier message; the words that appear in the openings of the template are the hidden message.

## II. Watermarking

In watermarking applications, the message contains information such as owner identification and a digital time stamp, which is usually applied for copyright protection. This is categorized into two parts [6]:-

**i. Fragile watermark:**

Fragile watermark is watermark that is readily altered when the host image is modified thorough a liner or non-liner transformation. It is used to the authentication of image. This is used to verify the image.

**ii. Robust Watermarking**:

Robust watermarks are used in copy protection applications to carry copy and no access control information to form correct order and get the digital water marking. A digital watermark is called perceptible if its presence in the marked signal is noticeable. It is categorized into three parts:-

a) **Fingerprint:** In Fingerprint, the owner of the data set embeds a serial number that uniquely identifies the user of the data set. This adds to copyright information to make it possible to trace any unauthorized use of the data set back to the user
b) **Imperceptible:** A digital watermark is called imperceptible if the original cover signal and the marked signal are perceptually indistinguishable.
c) **Visible:** In this visible digital watermarking, the information is visible in the picture or video. The image on the right has a visible watermark. When a television broadcaster adds its logo to the corner of transmitted video, this is also a visible watermark.

## 2.2 Cryptography

In the cryptography technique, the sender encrypts the data with the help of encryption algorithm and keys when it is sent into the network. When receiver receives the data is decrypt with the help of keys and get the original data. Steganography is not as same as cryptography. Basically the purpose of cryptography and Steganography are to provide secret communication. Basically, cryptography offers the ability of transmitting information among persons in a way that prevents a third party from reading it. Cryptography can also provide authentication for verifying the identity of someone or something [3].

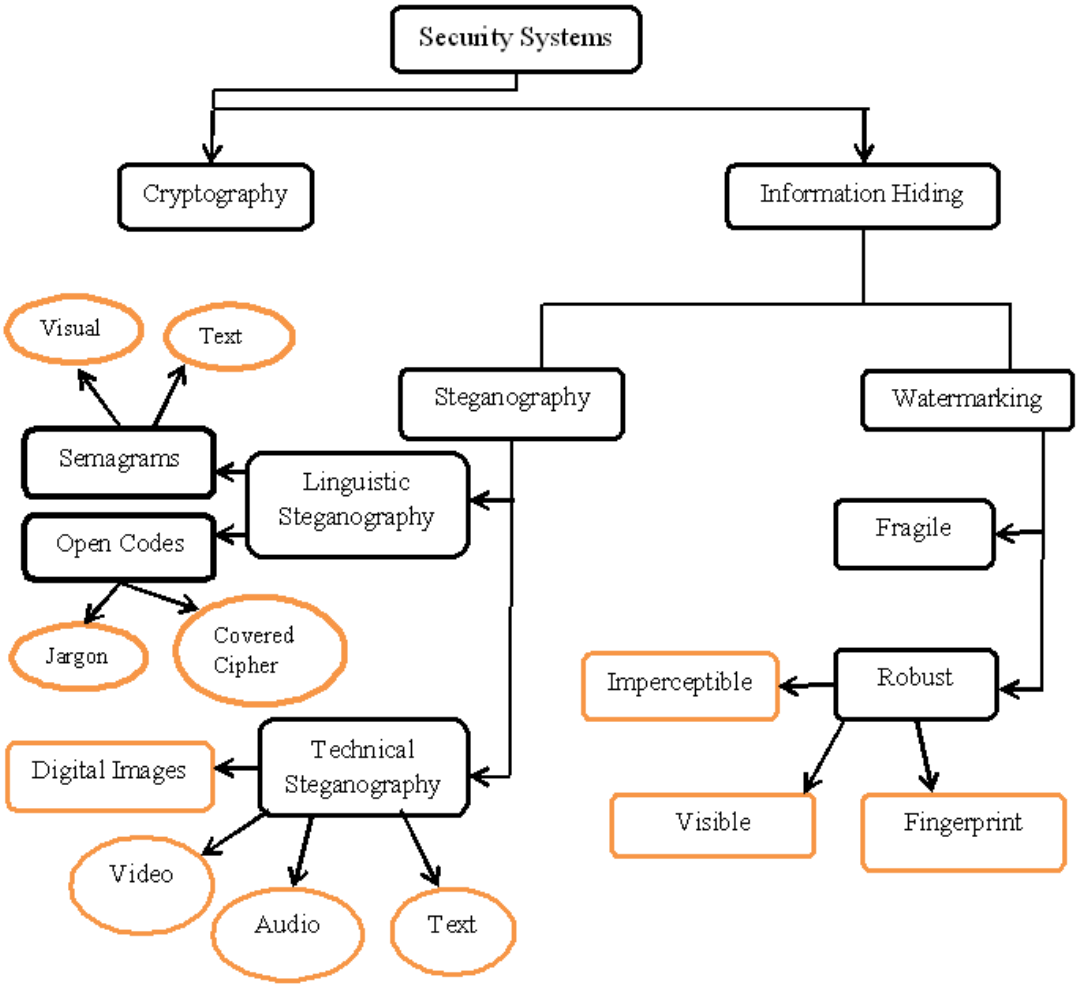


Figure 1: (Classification of Security System) [8] [9]

### A. Cryptography V/S Steganography

| Comparison | Steganography | Cryptography |
|---|---|---|
| Developed | Technology still being developed for certain formats | Most algorithms known to government departments |
| Message Type | Unknown message passing | Known message passing |
| Attack | Once detected message is known | Strong algorithm are currently resistant to brute force attack |
| Carriers | Many Carrier Formats | Large Expensive Computing Power |
| Technology | Little Known Technology | Common Technology |

Table 2: (Cryptography v/s Steganography) [7]

## 3. DIGITAL IMAGE STEGANALYSIS FOR COMPUTER FORENSIC INVESTIGATION

Nowadays the computer crime and cybercrime are big challenges. The criminal hide the message and data in images then it is difficult to recognize. Then the digital forensics is an investigation the crime in the organization which is done by the criminal. Digital forensics is used to investigation of Steganography slack points. Its examiners are very familiar with data that remains in the file slack or unallocated space as the remnants of previous files, programs can be written that can access slack unallocated space directly. Sometimes small amount of data can also be hidden in unused portion of file headers [4].

Digital forensics does investigation on network channel like as TCP/IP protocol because this pass the messages and causes some crimes like criminal communications, fraud, hacking electronic payments, gambling and pornography, harassment, viruses, pedophilia. Today's technology is being much more advanced hence increases crime rate on new technologies for their new applications. To investigate this level of crime, we use forensic computing technique.

## 4. CONCLUSION & FUTURE WORK

In this paper, we have provided a comprehensive study of Steganography. We have clarified differences between Steganography and watermarking. In this work, we have explained some successful applications exist in Steganography and also suggested the subtask of security system & future of steganography. We investigated the role of Steganalysis for digital forensic. Studies says that digital image steganalysis is very useful for computer forensic investigation.

## REFERENCES

[1] Gonzalez, Fernando Perez, and Hernandez, Juan R. "A Tutorial On Digital Watermarking" URL:http://www.gts.tsc.uvigo.es/~wmark/carnahan99.pdf Seen on Dec. 2011.

[2] B. Pfitzmann, "Information Hiding Terminology," Proc. First Int'l Workshop Information Hiding, Lecture Notes in Computer Science No. 1,174, Springer-Verlag, Berlin, 1996, pp. 347-356.

[3] William Stallings, Cryptography and Network Security, Principles and Practice, Third edition, Pearson Education, Singapore, 2003.

[4] C. Jasmin, M. Baca, "Steganography and its implication on forensic investigation", INFOTEH Jahorina, B & H, 2010.

[5] O. Kurtuldu and N. Arica, "A new steganography method using image layers," in Computer and Information Sciences, 2008. ISCIS'08. 23rd International Symposium on, 2008, pp. 1-4.

[6] Wayner, P. Disappearing Cryptography - Information Hiding: Steganography & Watermarking, 2nd. ed. San Francisco: Morgan Kaufmann; 2002.

[7] Nelson, B., Phillips, A., Enfinger, F., and Steuart, C. Guide to Computer Forensics and Investigations. Boston: Thomson Course Technology, 2004.

[8] WetStone Technologies Web Site. "Stego Watch." URL:http://www.wetstonetech.com/stegowatch_ns.html. Seen on Jan 2012.

[9] B. Li, Y.Q. Shi, and J. Huang, "Steganalysis of YASS," in Proceedings of the 10th ACM workshop on Multimedia and security, Oxford, UK, Sep. 2008, pp. 139–148.

[10] Al-Khateeb, H.; "Introduction to Modern Steganography", 11 Jan, 2012, http://blog.creativeitp.com/posts-and-articles/cryptography/introduction-to-modern-steganography/

[11] Silman, J. Steganography and steganalysis: an overview. Retrieved September, 8, 2007, from http://www.sans.org/reading_room/whitepapers/stenganography/553.php

[12] Krenn, R. Steganography and steganalysis. Retrieved September 8, 2007, from http://www.krenn.nl/univ/cry/steg/article.pdf

## Authors

**Dr. Nanhay Singh,** working as Associate Professor in Ambedkar Institute of Advanced Communication Technologies & Research, Govt. of NCT, Delhi-110031 (Affiliated to Guru Gobind Singh Indraprastha University, Delhi) in the Department of Computer Science & Engineering. He received his Ph.D (Computer Science and Technology) & M.Tech. (Computer Science & Engineering) from the Kurukshetra, University, Kurukshetra, Haryana. He has rich experience in teaching the classes of Graduate and Post-Graduate in India.He has contributed to numerous International journal & conference publications in various areas of Computer Science. He published more than 11 Research Paper in International Journals and Conferences. . He has also written an International book Titled as "Electrical Load Forecasting Using Artificial Neural Networks and Genetic Algorithm", in Global Research Publications New Delhi (India). His area of interest includes Distributed System, Parallel Computing, Information Theory & Coding, Cyber Law, Computer Organization

**Bhoopesh Singh Bhati,** received B.Tech. Degree in Computer Science & Engineering from the G.G.S.I.P. University after completing Polytechnic and Pursuing M.Tech. degree in Information Security from Ambedkar Institute of Advanced Communication Technologies & Research, Delhi, India

**Dr. R. S. Raw,** received his Ph.D (Computer Science and Technology) from the School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi, India in 2011. He has obtained his B. E. (Computer Science and Engineering) from G. B. Pant Engineering College (HNB Srinagar-Garhwal Central University), Pauri-Garhwal, UK, India and M. Tech (Information Technology) from Sam Higginbottom Institute of Agriculture, Technology, and Sciences, Allahabad (UP), India in 2000 and 2005, respectively. He has worked as an Assistant Professor at Computer Science and Engineering Department, G. B. Pant Engineering College, Uttarakhand Technical University, since March 2001 to June 2003 and March 2005 to July 2011. Currently he is working as an Assistant Professor in the department of Computer Science and Engineering of Ambedkar Institute of Advanced Communication Technologies & Research, Delhi, India since August, 2011. Dr. Raw has published research papers in International Journals and Conferences including IEEE, Elsevier, Springer, Inderscience, American Institute of Physics, IERI Communications Letters, AIRCC, etc. His current research area are Mobile Ad Hoc Network and Vehicular Ad Hoc Network.