Methods for hiding the data in computer forensics

Miss. Payal P. Wasankar
ME(CSE) 1st Year
P.R.Patil College Of Engineering, Amravati

Prof. P.D. Soni
P.R.Patil College Of Engineering, Amravati

Abstract

It is important for computer professionals to understand the technology that is used in computer forensics. Computer forensics basically include the recovery of deleted data. This paper present study about how to hide the useful information by using steganography and cryptography, and also introduce Steganalysis for computer forensic investigation. In the process of Steganalysis, it detects the hide data or message and decodes the hidden data or message.

Keywords: Computer forensic, security, Steganography, Steganalysis, watermarking, Cryptography

1. Introduction

Two basic types of data are collected in computer forensics. **Persistent data** is the data that is stored on a local hard drive (or another medium) and is preserve when computer is turned off. **Volatile data** is any data that is stored in memory, that will be lost when computer losses power or is turned off. And the data and 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 the technique to secure the information or messages is called Steganography. Steganography is the art of communicating in a way which hides the existence of communication. The goal of steganography is to hide the messages inside other harmless messages in a way that it does not allow any enemy to even detect that there is a second message present.

2. Steganography

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]. Information hiding and cryptography. Information hiding has two part steganography and watermarking. Steganography further divided into two parts are as:

2.1 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.

---

### 2.2 Linguistic Steganography

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

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) <strong>Semagrams:</strong></td>
<td>Semagrams use some symbols and signs to hide the information. It is further categorized into two ways:</td>
</tr>
<tr>
<td>i) <strong>Visual Semagrams:</strong></td>
<td>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.</td>
</tr>
<tr>
<td>ii) <strong>Text Semagrams:</strong></td>
<td>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.</td>
</tr>
<tr>
<td>b) <strong>Open Code:</strong></td>
<td>This hides a message within a legitimate carrier message in the ways that are not obvious to an unsuspecting observer.</td>
</tr>
<tr>
<td>i) <strong>Jargon:</strong></td>
<td>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.</td>
</tr>
<tr>
<td>ii) <strong>Covered Cipher:</strong></td>
<td>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.</td>
</tr>
<tr>
<td>- Null Cipher</td>
<td>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.”</td>
</tr>
<tr>
<td>- Grille Cipher</td>
<td>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.</td>
</tr>
</tbody>
</table>

---

3. **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]:-

#### 3.1 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.

#### 3.2 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:-

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>i) <strong>Fingerprint:</strong></td>
<td>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.</td>
</tr>
<tr>
<td>ii) <strong>Imperceptible:</strong></td>
<td>A digital watermark is called imperceptible if the original cover signal and the marked signal are perceptually indistinguishable.</td>
</tr>
<tr>
<td>iii) <strong>Visible:</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

---

4. **Steganalysis**

Steganalysis is simply the detection of steganography by a third party. This is a relatively new field, since the new technology behind steganography is just becoming popular. There are two main types of steganalysis:

- **Visual analysis and statistical (algorithmic) analysis.**

  **Visual analysis** tries to reveal the presence of hidden information through inspection with the naked eye or with the assistance of a computer, which can separate the image into bit planes for further analysis.

  **Statistical analysis** is more powerful and successful,
because it reveals the smallest alterations in an image’s statistical behavior. There are several statistical tests which can be run on an image: average bytes, variations of the bytes, skew, kurtosis, average deviation and differential values.

5. Cryptography
Cryptography is the process of transforming plain text or original information into an unintelligible form (cipher text) so that it may be sent over unsafe channels or communications. The transformer process is controlled by a data string (key). Anyone getting hold of the cipher text while it is on the unsafe channel would need to have the appropriate key to be able to get to the original information. The authorized receiver is assumed to have that key. [9] Cryptography is study of methods of sending message in disguised form so that only the intended recipients can remove the disguised message. It is the art of converting message into different form, such that no one can read them without having access to ‘key’. The message may be converted Using ‘code’ or a ‘cipher’. Cryptology is the science underlying cryptography.

6. Cryptography v/s steganography
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].

7. Investigation analysis
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.

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

9. References