Recent Research Reviews Journal (ISSN: 2583-7079)
https://irojournals.com/rrrj

Survey on Computer Forensics and its most using Technique Steganography

Vijayakumar Thangavel

Department of ECE, M.P.Nachimuthu M.Jaganathan Engineering College, Chennimalai, India

E-mail: vijayprahu@gmail.com

Abstract

A subfield of digital forensic science called computer forensics deals with evidence discovered on computers and digital storage devices. Computer forensics aims to detect, preserve, retrieve, analyse and communicate facts and views regarding the digital information by performing a forensically sound examination of digital media. The purpose of this study is to provide a brief discussion of computer forensics and related methods. Steganography is one of the most widely utilised of these approaches, and it will also be briefly discussed below.

Keywords: Computer Forensics, Steganography, Types of Forensics, Applications of Steganography.

1. Introduction

Personal computers were more widely available to customers at the beginning of the 1980s, which expanded their usage in criminal behaviour. Several more "computer crimes" were identified at the same time. During this period, the field of computer forensics developed as a way to locate and examine digital evidence for use in court. Since then, there has been an increase in computer crime and computer-related crime. Rajeev Chandrasekhar, Minister of State for Electronics and Information and Technology, told the Parliament that India experienced 3.91 lakh cyber security incidents in 2022 alone [3].

The area of forensic science known as computer forensics deals with digital data that may be used as evidence in court. When a digital computer was hacked in the early 1990s, the field of digital forensics was born. Michael Anderson, the founder of computer forensics, served as the chief leader of the FBI CART program, formerly known as the "Magnet Media Program."

The investigations of Michael Jackson, German Airlines Flight 9525, and other instances were successfully resolved by the use of computer forensics [4].

There are five key characteristics of computer forensics. Identification, preservation, analysis, documentation, and presentation fall under this category. First, identification entails locating the evidence that can be kept at a location (in any format) where electronic devices like cell phones, PDAs, personal computers, etc. are present. Additionally, that data has been protected, kept, and segregated. It could forbid utilising the digital gadget by unauthorised employees. Therefore, it should be altered or copied from the original device. Then, forensic lab staff rebuild data fragments and reach judgments based on the available evidence. It will be possible to recreate and evaluate the crime scene with the aid of a record of every single observable piece of data. The investigators' whole body of knowledge is documented. In a court of law, all the documented results are presented in order to support future inquiries [5].

Figure 1. Characteristic of Computer Forensics [5]

2. Types of Computer Forensics

Disk forensics, Database forensics, Malware forensics, Email forensics, Mobile forensics, Memory forensics, and Network forensics are some of the several forms of computer forensics.

Table .1 Types of Computer Forensics

Disk Forensics	Involves examining active, altered, or deleted files to find raw data in the device's primary or secondary storage.
Database Forensics	It focuses on the research and analysis of databases and the associated metadata.
Email Forensics	It deals with emails, especially removed emails, calendars, and contacts, and their recovery and analysis.
Malware Forensics	It is concerned with locating suspicious code and researching viruses, worms, etc.
Memory Forensics	Focuses on obtaining raw data from the system's memory (system registers, the cache, and RAM) and then analysing it for more research.
Mobile Forensics	It generally focuses on the inspection and evaluation of phones and smartphones, and it aids in retrieving contacts, call history, incoming and outgoing SMS, etc., as well as other data that may be there.
Network Forensics	Monitoring and examining computer network traffic falls under the category of computer forensics.

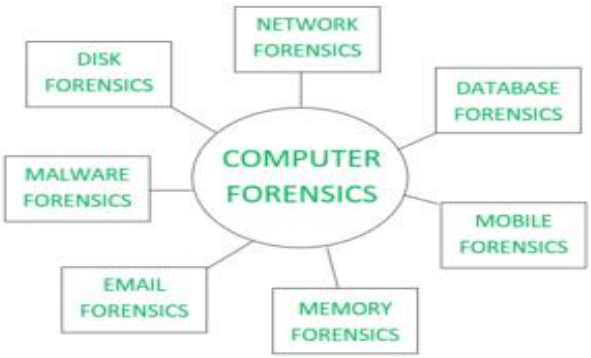

Figure 2. Types of Computer Forensics [5]

3. Techniques of Computer Forensics

Computer forensics investigations frequently come after the conventional digital forensics process, which includes acquisition, inspection, analysis, and reporting. Although in the early days of computer forensics investigators used to focus on live data owing to a lack of tools, nowadays investigations are primarily done on static data instead of live data or live systems. Now, various techniques are used in computer forensics [6]. They are: -

3.1 Cross Drive Analysis (CAD)

An investigator can swiftly locate and correlate data from several data sources or data spread across numerous drives using the cross-drive analysis (CDA) approach. Multi-drive correlation utilising text searches, such as email addresses, SSNs, message IDs, or data from credit cards, is one of the methods already in use.

3.2 Live Analysis

It is used to inspect computers that access the operating system, utilising several forensics and system administration tools to obtain data from the device. The gathering of volatile data for forensic investigation, such as software-installed packages, hardware details, etc., is crucial. When the investigator is working with encrypted files, this method is helpful. The investigator should get all the volatile data stored on the device, like user login history, open TCP and UDP ports, services that are now in use and operating, etc., if the system is still alive and running when it is given to the investigator.

3.3 Deleted Files Recovery

It's a method for getting back deleted files. With the use of forensic program like CrashPlan, OnTrack EasyRecovery, Wise Data Recovery, etc., the erased data may be retrieved or desired out.

3.4 Stochastic Forensics

It is a technique for forensically reconstructing digital actions with inadequate digital artefacts, allowing for the analysis of new patterns brought on by the stochastic nature of contemporary computers.

3.5 Steganography

Steganography is a method for concealing hidden information on top of or inside of something, which might be anything from a file to a picture. Computer forensics investigators could compare the hash values of the modified and original files to address this. The hash values of the two files will differ even if they appear to be identical upon eye inspection.

From all these techniques, steganography is the most widely used in different fields for investigations. A cybercriminal can hide vital data included within a digital picture or other file. To the untrained eye, it can appear identical before and after, but the hash or string of data behind the image will change. This technique is used in steganography.

4. Steganography

4.1 Classifications of Steganography

Steganography is a technique for concealing secret information by enclosing it in a regular, non-secret file or communication; the information is subsequently retrieved at the intended location. Steganography can be used in addition to encryption to further conceal or safeguard data. The Greek term “steganos” (meaning hidden or covered) is where the name "steganography" comes from.

Although the name "steganography" wasn't really used until the last decade of the 15th century, it has been around for many years. Messages were formerly buried on the backs of waxed writing tables, scribbled on rabbits' bellies, or tattooed onto the slaves' scalps. Since ancient times, people have used invisible ink for both serious espionage by detectives and terrorists as well as for fun by kids and schoolchildren. After the development of photography, microdots and microfilm became common in war and spy films [1].

While the hidden communication is concealed by steganography, the reality that two people are conversing with one another is not. A secret message is often placed in a carrier—a type of transport medium—during the steganography process. To create the steganography medium, the hidden message is included in the carrier. A steganography key can be used in the steganography method for randomization or encryption of the concealed message.

steganography_medium = hidden_message + carrier + steganography_key

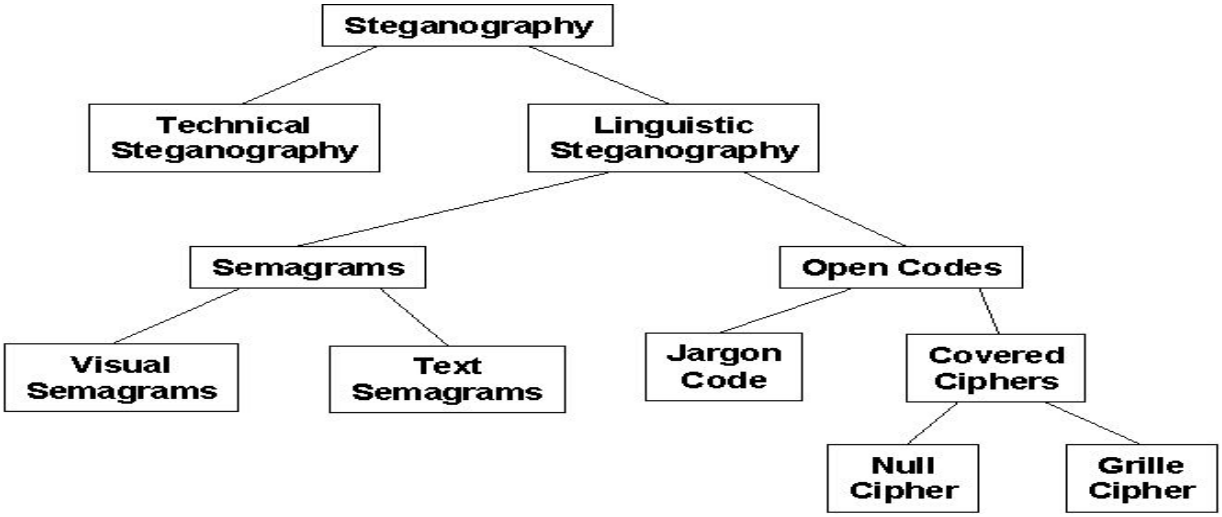

Figure 3. Classification of Steganography [1]

Technical steganography employs scientific techniques to conceal a message; linguistic steganography, which is subdivided into semagrams or open codes, conceals the message in the carrier in various obscure manners. Semagrams employ signs and symbols to conceal information. Open codes conceal a message in a valid carrier message in ways that are not immediately apparent to an untrained observer. This category will be further separated into visual semagrams and text semagrams. It is divided into covered clippers and Jargon code. Language used in jargon code is recognised by a small number of individuals but has no significance to others. Covered or concealment ciphers hide a message openly in the carrier medium so that it can be recovered by anyone who knows the secret behind how it was concealed.

4.2 Applications of Steganography

Even though steganography hides the hidden message, in actuality, two people are not speaking to each other. Finding a concealed message in a carrier—a transport medium—is a common step in the steganography process. The steganography channel is created by embedding the secret message within the carrier. For the encryption of the secret message and for randomised steganography design, a steganography key is required. There are many applications for steganography [7].

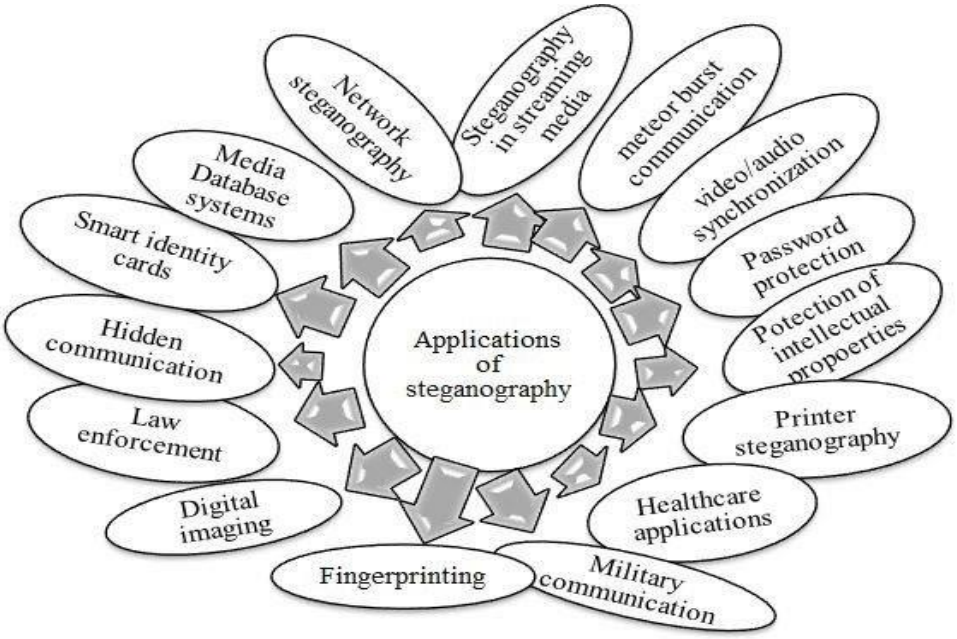

Figure 4. Applications of Steganography [8]

Steganography has gained a lot of potential due to technological advancements in digitalization. Steganographic communication is more appropriate in situations where encryption-based communication is constrained since its fundamental idea is the secrecy of the transmission. Steganography is now used in many IoT-enabled commercial applications, smart cities, medical imaging, and military applications, among others. Images, text, DNA, videos, music, and other digital objects are used as carrier signals in the steganographic process. Researchers have selected photos as the carrier signal for concealing hidden information because of the innocence of digital images. Additionally, a picture is considerably more ideal for encoding hidden information when it has redundant pixels. The practice of obscuring private data inside a photograph is referred to as image steganography (IS).

4.3 Uses of Steganography

Steganography is a technique for concealing data and a means of attempting to conceal the presence of embedded data. It is a better form of communication security than encryption, which merely conceals the message's content and not its existence. The following are some of the uses for steganography [9]:

- It may be a solution that enables us to transmit information and news without restriction or concern that the messages would be intercepted and linked to us.

- Steganography may also be used to merely store data on a spot. For examples, information sources that can be kept as cover sources include private banking information and some military secrets. When it is necessary to reveal the secret data from the cover source since it will just show the banking information, it will be difficult to verify the existence of military secrets inside.
- Some users in modern e-commerce transactions are protected by a username and password, but there is no practical way to verify that the user is the true card holder. Biometric finger print browsing, with particular session IDs steganographically inserted within the fingerprint pictures. It may make opening e-commerce transaction verification a highly safe option.
- Another important use of steganography is the transfer of responsive data. The fact that listeners can tell when they are using encrypted communication that may be observed by anyone is a possible problem in the encryption. Steganography makes it possible to transmit response information to listeners without having any of the information known to others.
- Watermarking may often be done via steganography. Although steganography is not certainly included in the watermarking idea, To store watermarks in data, a variety of steganographic techniques are used. The primary distinction is that watermarking virtually adds new data to the cover source, whereas the goal of steganography is to conceal data. A watermark will prevent users from seeing changes to photos, audio, or video files; therefore, a steganographic technique can be utilised to hide these modifications.

4.4 Advantages and Disadvantages of Steganography

4.4.1 Advantages

Steganography has the benefit that it may often be used to deliver messages covertly without the transmission being detected. This method included security, capacity, and resilience, the three essential components of steganography that make it useful in developing secret communication and exchanging data invisibly through text files. It may identify both the sender of the message and the recipient by employing encryption. It is protected in two ways: first, the file itself is secret; second, the information within is encoded. While steganography may be

claimed to secure both communications and connecting parties, cryptography just protects the content of a message [2].

4.4.2 Disadvantages

The Steganography technique can be extremely dangerous if it falls into the hands of hackers, terrorists, or criminals. Steganography's main drawback is that, in contrast to cryptography, it requires a lot of costs to cover logically small bits of information. The steganographic system is been ineffective since it was discovered. It performs no worse than cryptography, nevertheless, and continues to be the chosen medium. Someone may have suspicions since there is a lot of material and a significant file size [2]. The use of steganography has drawbacks. However, these may be fixed, and it will make the steganography element stronger.

5. Conclusion

This study researched computer forensics, which primarily uses diverse methods utilised in a variety of sectors to secure data. The most popular method in computer forensics is steganography. Steganography is mostly utilised in courts to make evidence visible in order to resolve cases. In the fields of the military, police, and forensics departments, it is quite beneficial. It will hide the data in various formats. Discussing steganography's classifications, usage, and applications comes from this study effort. Additionally, there are advantages and disadvantages to employing this strategy, which are also covered here.

Reference

[1] Kessler, Gary C. "An overview of steganography for the computer forensics examiner." Forensic science communications 6, no. 3 (2004): 1-27.

[2] Sahu, Aditya Kumar, and Monalisa Sahu. "Digital image steganography and steganalysis: A journey of the past three decades." Open Computer Science 10, no. 1 (2020): 296-342.

[3] https://en.wikipedia.org/wiki/Computer_forensics

[4] https://www.udemy.com/course/digital-forensic-from-scratch/

[5] https://www.geeksforgeeks.org/introduction-of-computer-forensics/

[6] https://www.geeksforgeeks.org/computer-forensics-techniques/

[7] https://www.tutorialspoint.com/what-are-the-application-of-steganography

[8] https://www.tutorialspoint.com/what-is-the-uses-of-steganography

[9] https://www.tutorialspoint.com/what-are-the-advantage-and-disadvantage-of-steganography#:~:text=The%20advantage%20of%20steganography%20is%20that%20it%20can%20be%20generally,the%20sender%20and%20the%20receiver