STEGANOGRAPHY:
BASICS AND DIGITAL FORENSICS

SadhanaRathore (Computer Science Engineering, HRIT, Ghaziabad)

Abstract- In the present era internet is being used widely for transferring information from one place to another place. These information is being transferred within corporate sectors, family conversations, friend chat or any legal information related to different issues within different groups. But information is also being exchanged illegally for different purposes. This can be really threat-full. Steganography is one tool which can be proved very harmful viewing its applications. And on the other side of coin it can be proved very useful in digital forensics.

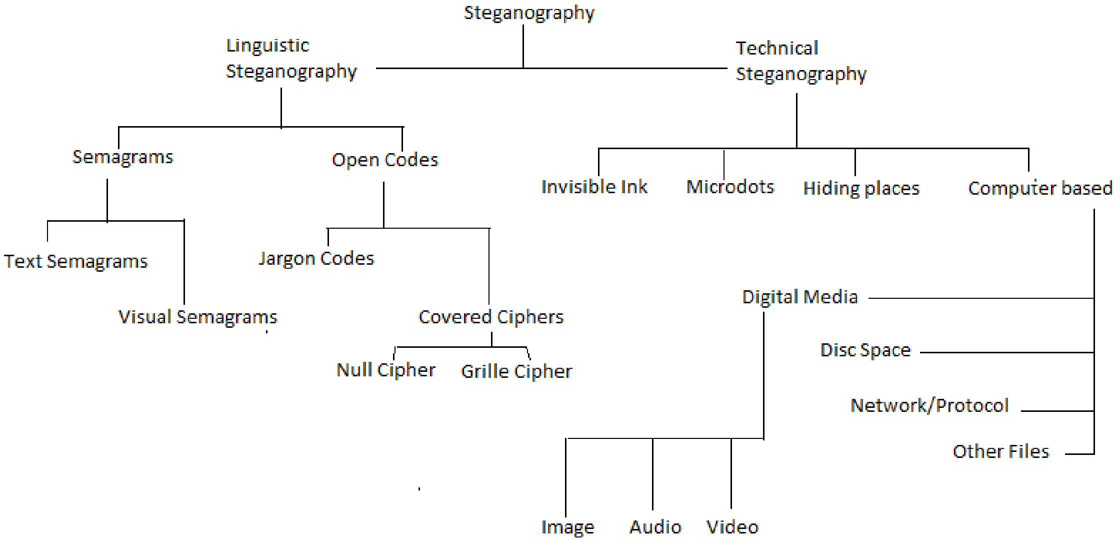
This article focus on how steganography can be used illegally and why there is a need of adding it as an important tool in forensic investigation.

1. Introduction

Steganography, a Greek word means masked writing. Steganography was first used in Greek times. In 499 BC, Greek tyrant Histiaeus, shaved the head of one of his slave. Then the message was written on his scalp. After the hair grew on his head, he was dispatched with the hidden message. In the era of discovery, fast growing techniques, use of internet, computing power, steganography has gone digital.

As a consequence messaging for public and private good are valuable belongings in the social and economic networks of relationships that drive business and community relations. A positive side is always balanced by a negative exploitation. All communication media can be used for criminal purposes and the undermining of genuine activities. The digital mediums permit open communication and, consequently, the potential of hidden message propagation (steganography). This differs from cryptography, the art of secret writing, which is intended to make a message unreadable by a third party but does not hide the existence of the secret communication. Although steganography is separate and distinct from cryptography, there are many analogies between the two, and some authors categorize steganography as a form of cryptography since hidden communication is a form of secret writing (Bauer 2002).

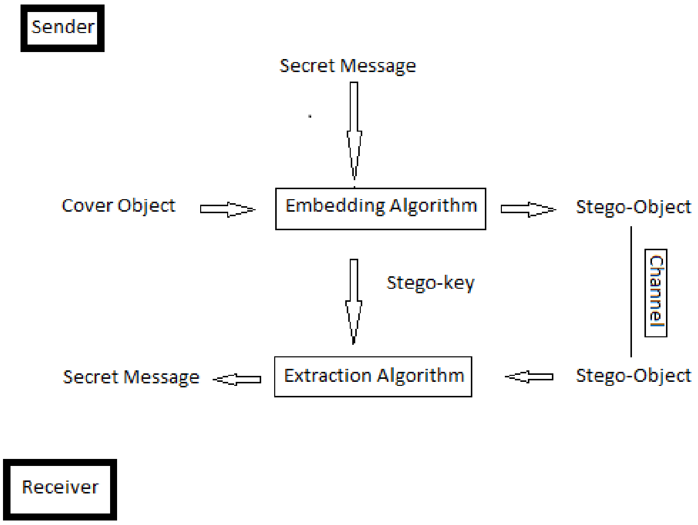
Fig.: steganography classification



- Technical steganography uses scientific approaches to hide a message, such as the use of undetectable ink or microdots and other size-reduction approaches.
- Linguistic steganography hides the message in the transporter in some non-obvious ways and is further categorized as semagrams or open codes.
- Semagrams hide information by the use of symbols or signs. A visual semagram uses innocent-looking or everyday physical objects to convey a message, such as doodles or the positioning of items on a desk or website. A text semagram hides a message by amending the appearance of the transporter text, such as indirect changes in font size or type, adding extra spaces, or different flourishes in letters or handwritten text.
- Open codes hide a message in a legitimate carrier message in ways that are not obvious to an innocent observer. The transporter message is sometimes called the unconcealed communication whereas the hidden message is the concealed communication. This category is subdivided into jargon codes and covered ciphers.
- Jargon code, as the name suggests, uses language that is understood by a group of people but is meaningless to others. Jargon codes include Warchalking (symbols used to indicate the presence and type of wireless network signal [Warchalking 2003]), underground terminology, or an innocent conversation that conveys special meaning because of facts known only to the speakers. A subset of jargon codes is cue codes, where certain prearranged phrases convey meaning.
- Covered or concealment 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. 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. 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."

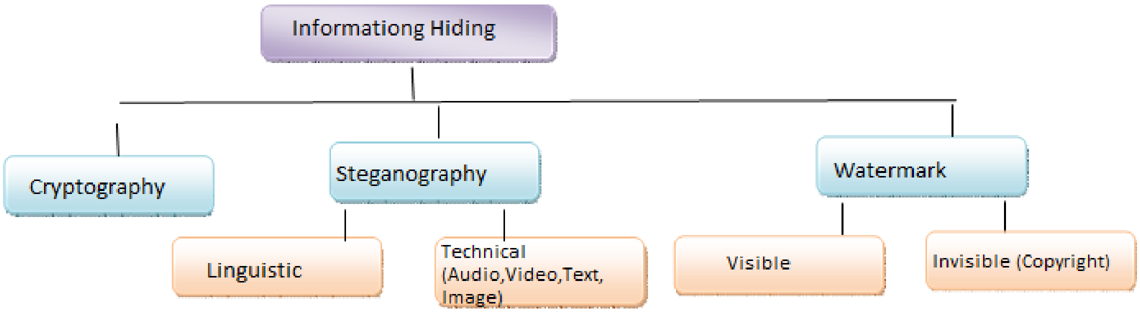
2. Steganography process

During the steganography process, the secret message will first be embedded into a cover-object with an embedded algorithm and stego-key to generate a stego-object. This stego object can then be transported via OSN (Online Social Network), email, website, blog, etc. To the intended receiver. The receiver then extracts the secret message using the extraction algorithm and stego-key.



3. Steganography, Cryptography and Watermarking

Steganography, cryptography and watermarking are well known and widely used to hide the original message.
Steganography is used to embed message within another object known as a cover work, by tweaking its properties; by using cryptography sender convert plaintext to cipher text by using encryption key and other side receiver decrypt cipher text to plain text.; digital watermarking is a technique for inserting information (the watermark) into an image (visible or invisible).



4. Crypto-steganography

Steganography is not the same as cryptography. Data hiding techniques have been widely used to transmission of hiding secret message for long time. Ensuring data security is a big challenge for computer users. Business men, professionals, and home users all have some important data that they want to secure from others. Even though both methods provide security, to add multiple layers of security it is always a good practice to use cryptography and steganography together. By combining, the data encryption can be done by a software and then embed the cipher text in an image or any other media with the help of stego key. The combination of these two methods will enhance the security of the data embedded. This combined chemistry will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel.
A pictorial representation of the combined concept of cryptography and steganography is depicted in figure

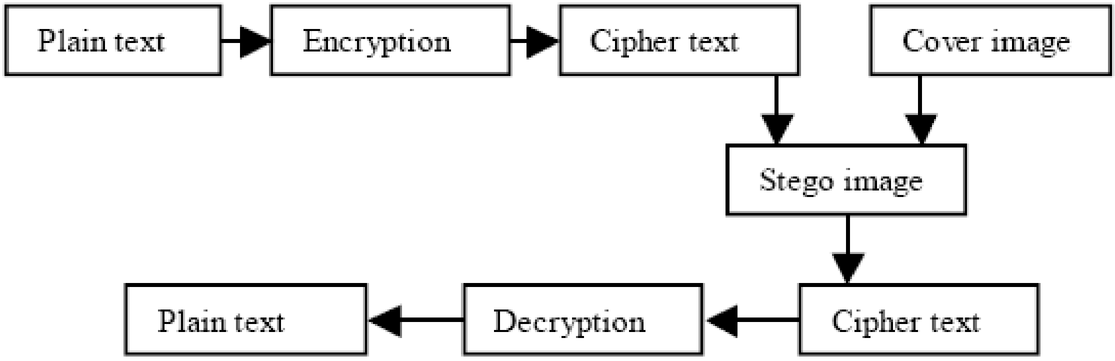


Fig. 2: Combination ofsteganograophy and cryptography

5. The Prisoners problem

Modern steganography is always illustrated by the "prisoners' problem" model. Two fictional prisoners, Alice and Bob were to perform a prison escape and they needed to communicate and plan for the escape without arousing the cell's warden (eve) attention, who monitored the communication. If eve finds out they have exchanged messages secretly, all communication will be stopped immediately and they will be placed in solitary confinement. Therefore, they must communicate in such a way that eve will not suspect there being a secret message in their communication. This is the basic principle of steganography, where an outside observer is not able to distinguish whether a communication is normal or it holds hidden messages. For example, Alice may draw a picture of a blue cow and sun, only bob knows the exact meaning of the object and the colour used whereas eve may think that it is just abstract art and therefore pass it along bob.

In the prisoners' problem there are two objects of interest. Eve can be either a passive warden or an active warden in monitoring the communication between Alice and Bob. A passive warden means that eve is only allowed to examine the picture using necessary tests to identify the existence of steganography. If eve is an active warden, however, he may change the colour of the sun or may draw an additional object into the picture to change the original meaning of the drawing. To illustrate the implication of this in digital steganography, an active warden may apply cropping, compression, or resizing, in the transportation channel. Any of these actions could destroy the hidden message and thus disable recovery by the intended recipient. This is also a good way to prevent the use of steganography. On the other hand, eve may choose to observe and try to learn the stego-key that is used between the prisoners and thereby extract the secret message so that he knows the whole story of the escape plan. Eve may even exploit stego-key and impersonate Alice communicate with Bob or vice versa to extract the secret message. In steganography, the act of identifying and extracting a secret message is called steganalysis.

6. **Digital forensics**

Digital forensics focuses on the protection and analysis of digital evidence. As defined in palmer (2008), digital forensics are “the use of scientifically derived and proven methods toward the protection, collection, authentication, identification, analysis, explanation, documentation, and presentation of digital evidence derived from digital sources for the purpose of simplification or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.” As steganography becomes more widely available and the amount of data on local machines and internet increases, the issue of detection of the use of steganography by digital forensics personnel becomes increasingly important. In theory, this should be evaluated in any type of case involving computer use. In practice, most cases will involve audio-visual files, such as in child pornography. However, cases of industrial surveillance and fraud could be encountered.

- *Approaches in forensic steganalysis*

Digital forensic experts work on many techniques, and we will limit the discussion to those applicable to steganography.

a. Detection of software

In some cases, steganography software itself may be discovered on computer equipment under investigation. The steganography application fingerprint database (SAFDB) currently contains identifying information on 625 applications associated with steganography, watermarking, and other data-hiding applications (backbone security, 2008a). Similarly, the national institute of standards and technology (NIST) maintains a list of digital signatures in the national software reference library, some of which are for steganography software. Even when software has been removed, traces can sometimes be found in places like the windows registry or in system backup files. When steganography software installation has been identified, malicious intent should be assumed until proven otherwise.

b. Detecting pairs of carrier files and stego files

In addition to detecting the software used for steganography, digital forensics experts can detect files with similar visual properties but different file sizes, hash values, and statistical properties. If files have been deleted, they may be retrieved from the recycle bin or similar trash container, or even reconstructed with special forensics tools for file recovery.

c. Using keywords

An additional method of detection uses a list of keywords to search for file names and content in program files and data files. The list should be specific with regard to steganography. For instance, the search term “steg*” can be used to identify steganography. The effectiveness and efficiency in detection, while preventing false positives and false negatives, depends on the quality of the keyword dictionary.

d. Specialized steganalysis software

In the past, most steganography detection tools targeted specific applications – frequently the same applications used for steganography. More recent software claims to detect stego files created with a wide variety of programs. One of these is stegdetect 0.6, which uses linear discriminant analysis to locate probable images with hidden content by comparing them with a set of normal images (provos, 2008). A second common tool is stego suite (Wetstone technologies, 2008), which combines increasingly intense levels of detection with content cracking tools. The third example is the recent release of steganalyzers (backbone security, 2008b), which uses the values stored in the SAFDB to identify potential stego files.

e. Physical crime scene investigation

Finally, physical crime scene investigation can reveal useful information. Passwords used for steganography tools can be written on notes stuck under keyboards, and environmental objects can generate clues about potential passwords.

7. Digital security issues

Though steganography tools may be used for genuine business applications such as protecting strategic corporate information during transmission (Schmidt et al, 2004), they have emerged as a significant issue to forensic investigators and others who are concerned with malicious and illegal uses. As steganography tools become more widely available and easier to use, protection against malicious use demands attention, and the balance between protection from illicit use and interference with legitimate use emerges as a new challenge.

8. Online/internet forensics

Now a days online/ internet networks (mostly social networks) have replaced traditional means of digital storage, sharing and communication. Collecting this type of data is also fundamental to the area of digital forensics. According to a survey conducted in 2014, through a legal database search from 2012 to 2014, there were 697 decisions in us where online media evidence played a significant role. Therefore, a forensically sound method of extracting and analysing data from online/internet network is critical.

Mostly online/internet data (OSN data) is not stored on the user's computer hard drive as it is web based content generated by users, therefore web forensics plays a significant role in identification, collection, and analysis on online/internet networks.

References:

i.) Journal of Digital Forensics, Security and Law, Vol. 3(2) (Steganography: Forensic, Security, and Legal issues)

ii.) Anderson, R. J., and Petitcolas, F. A. P. (1998). ‘On the limits of Steganography’, IEEE Journal on Selected Areas in Communications, 16(4): 474-481.

iii.) Cole, E. (2003). ‘Hiding in plain sight: Steganography and the art of covert communication’, Wiley Publishing, Inc., Indianapolis.

iv.) Johnson, N. (2008). ‘Steganography’, http://www.jjtc.com/stegdoc/steg1995.html, June 25.

v.) Petitcolas, F. (2000). ‘Information Hiding: Techniques for Steganography and Digital Watermarking’, Artech House Books.

vi.) Pfitzmann, B. (1966).'Information Hiding Terminology - Results of an Informal Plenary Meeting and Additional Proposals'. First International Workshop on Information Hiding, May 30 - June 1, Cambridge, U.K.

vii.) Wingate, J. (2007). ‘Digital Steganography: Threat or Hype?’ Homeland Defense Journal, 5(4): 60-63.

viii.) Neil F. Johnson and sushilJajodia Exploring Steganography: seeing the unseen IEEE computer, 31(2) 26-34, 1998.

ix.) N. Proros and P. Honeyman. “Hide and seek: An Introduction to Steganography “, IEEE: security & Privacy, vol. 10, pp. 32-44, 2003.

x.) I. VenkataSai Manoj, “Cryptography and Steganography”, International Journal of Computer Applications (0975 – 8887), Volume 1 – No.12

xi.) B BZaidan, A.A Zaidan, A.K. Al-Frajat and H.A. Jalab, “On the Differences between Hiding Information and Cryptography Techniques: An Overview”, Journal of Applied Sciences 10(15): 1650-1655, 2010

xii.) SashikalaChannalli and Ajay Jadhav, “Steganography An Art of Hiding Data”, International Journal on Computer Science and Engineering Vol.1(3), 2009, 137-141.

xiii.) An Overview of Steganography for the Computer Forensics Examiner (http://www.garykessler.net/library/fsc_stego.html)