University of New Haven

CSCI-6646-01 Intro to Computer Security

Fall 2022

Research Paper

Under

Dr. Sayed Hussein

STEGANOGRAPHY - A TECHNIQUE TO HIDE THE DATA

By:

SUMANTH REDDY DESIREDDY (00797429)

Abstract:

The security of data has been one of the key components of data information technology and communication since the advent of the internet. A variety of techniques have been devised to encrypt and decrypt data in order to keep the message secret. Cryptography was created as a method for protecting the confidentiality of communication. We sometimes have to reveal information, which is unfortunate. The method employed to conceal the data is called steganography.

One of the common methods for obscuring data is steganography. Steganography is the practice of obfuscating or burying a secret message within an otherwise public message. Though it seems grandiose, the word "steganography" actually has Greek roots. The Greek word "steganos" means "hidden" or "covered," and the Greek word "graph" means "to write." These words can be combined to create something that is similar to "hidden writing" or "secret writing." Steganography is a technique used by cybercriminals to cover up malicious code or stolen data in images, audio files, and other types of media.

The most famous form to hide the data that is frequently used for Steganography are digital images, as they are also the most dominant forms found on the internet.

Introduction:

The security of data has been one of the key components of data information technology and communication since the advent of the internet. A variety of techniques have been devised to encrypt and decrypt data in order to keep the message secret. Cryptography was created as a method for protecting the confidentiality of communication.

Unfortunately, sometimes we can't hide the information. One of the oldest technique used to hide the information is Steganography. Steganography is the act of concealing or hiding a mystery message within something not secret.

Steganography word is derived from Greek, literally means Covered Writing. Steganography is the art of hiding the existence of data in another transmission medium to achieve secret communication.

- The first use of steganography can be traced back to 440 BC when ancient Greece, people wrote messages on wood and covered it with wax, that acted as a covering medium
- Romans used various forms of Invisible Inks, to decipher those hidden messages light or heat were used
- During World War II the Germans introduced microdots, which were complete documents, pictures, and plans reduced in size to the size of a dot and were attached to normal paperwork
- Null Ciphers were also used to hide unencrypted secret messages in an innocent looking normal message

Objective of the Study:

When users try to keep information from someone who might not have permission to see it, they face their largest barrier. By concealing and encrypting information using images and keys, respectively, this study aims to understand how steganography, an information hiding technique, aids in solving the issues they confront. It also tests and evaluates the usefulness, validity, and usability of various techniques.

What is the Difference between Steganography and Cryptography?

The fundamental idea of Steganography as well as Cryptography is the same. Both the approaches help in preventing the visibility of sensitive messages and data to third parties. However, the two approaches employ entirely different mechanisms for accomplishing their goal. In this section, let us consider the question of what is the difference between steganography and cryptography.

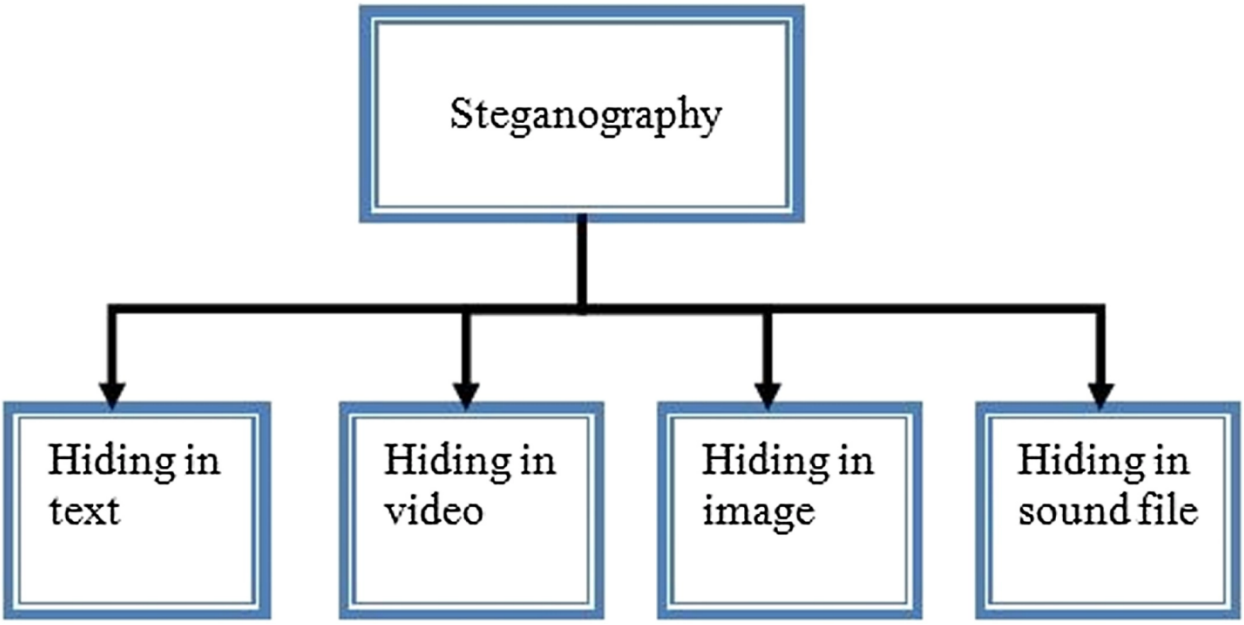
Steganography, or *cover writing*, is a method where a secret method is converted into fake looking message. This technique helps to

keep a message secret. It is pretty difficult to use and understand. The structure of data remains unaltered in Steganography. It is used in text, audio, video or images.

Cryptography, or *secret writing*, is a method where a secret method is converted in cipher text and sent to other person who then decrypt the cipher text into plain text. Cryptography can be classified as Symmetric key cryptography or Asymmetric key cryptography.

BASIS FOR COMPARISON	STEGANOGRAPHY	CRYPTOGRAPHY
Basic	It is known as cover writing.	It means secret writing.
Goal	Secret communication	Data protection
Popularity	Less popular	More commonly used.
Supported security principles	Confidentiality and authentication	Confidentiality, data integrity, authentication, and non-repudiation.
Implemented on	Audio, video, image, text.	Only on text files.
Types of attack	Steganalysis	Cryptanalysis

Different Types of Steganography:



1. Text Steganography − There is steganography in text files, which entails secretly storing information. In this method, the hidden data is encoded into the letter of each word.

2. Image Steganography − The second type of steganography is image steganography, which entails concealing data by using an image of a different object as a cover. Pixel intensities are the key to data concealment in image steganography.

Since the computer description of an image contains multiple bits, images are frequently used as a cover source in digital steganography.

The various terms used to describe image steganography include:

- Cover-Image - Unique picture that can conceal data.
- Message - Real data that you can mask within pictures. The message may be in the form of standard text or an image.
- Stego-Image − A stego image is an image with a hidden message.
- Stego-Key - Messages can be embedded in cover images and stego-images with the help of a key, or the messages can be derived from the photos themselves.

3. Audio Steganography − It is the science of hiding data in sound. Used digitally, it protects against unauthorized reproduction. Watermarking is a technique that encrypts one piece of data (the message) within another (the "carrier"). Its typical uses involve media playback, primarily audio clips.

4. Video Steganography − Video steganography is a method of secretly embedding data or other files within a video file on a computer. Video (a collection of still images) can function as the "carrier" in this scheme. Discrete cosine transform (DCT) is commonly used to insert values that can be used to hide the data in each image in the video, which is undetectable to the naked eye. Video steganography typically employs the following file formats: H.264, MP4, MPEG, and AVI.

Advantages of Steganography:

Steganography is a method that makes it easy to conceal a message within another to keep it secret. The result is that the hidden message remains hidden. A steganography approach can benefit images, videos, and audio files. Further advantages include:

- Unlike other methods, steganography has the added benefit of hiding communications so well that they receive no attention. However, in countries where encryption is illegal, sending an encrypted message that you can easily decipher will raise suspicion and may be risky.
- Steganography is a form of encryption that protects the information within a message and the connections between sender and receiver.
- The three essential elements of steganography—security, capacity, and robustness—make it worthwhile to covert information transfer via text files and develop covert communication channels.
- You can store an encrypted copy of a file containing sensitive information on the server without fear of unauthorized parties gaining access to the data.
- Government and law enforcement agencies can communicate secretly with the help of steganography corporations.

Disadvantage of Steganography:

The disadvantage of Steganography is as follows −

- There are large number of information, huge file size, therefore someone can suspect about it.
- If this approach is gone in the wrong hands such as hackers, terrorist, criminals then this can be very much critical.
- Steganography is not without its disadvantages. However, these can be rectified and once it is performed and it can strengthen the element of steganography.
- Most data hiding approach take advantage of human perceptual deficiency, but they have deficiency of their own. However, these can be independently rectified.
- The major disadvantage of steganography is that, unlike cryptography, it needed a lot of overhead to hide associatively few bits of information. Because the steganographic system is found, it is rendered useless. However, it fares no worse than cryptography and is still the preferred medium.

Real-World Attacks That Used Steganography:

In 2020, businesses in the United Kingdom, Germany, Italy, and Japan were hit by a campaign using steganographic documents.

Hackers could avoid detection by using a steganographic image uploaded on a good platform, like Imgur, to infect an Excel document. Mimikatz, a malware that steals Windows passwords, was downloaded via a secret script included in the picture.

Applications of steganography:

Although the prime objective is to share messages or information discreetly, it has found varied fields of applications such as

- Hackers using steganography techniques for malware transmission
- Intelligence agencies use them for communication.
- Printers also use micro-dots as a steganography tool to embed timestamps and date information within the document. Also, the same technique is used in bank-note printing, to prevent colour copiers from reproducing images of currency as fake-notes.

Detecting steganography:

Digital steganography is exceedingly difficult to detect, even though physical steganography may be detectable. Even if some activity is detected, let's assume that some messages are concealed within photos, attempting to monitor all transferred images and compare them to source images would lead to a great deal of false positives and false negatives. Despite this, specialists continue to employ a number of methods, such as image histogram comparisons, to find concealed messages, "conditioned" on their having reason to believe that a covert message exchange has taken place.

Conclusion:

I have briefly explained and defined steganography, which is in my opinion an effective tool to do so many things regarding security or reliability in any field of communication. What I mean that, this technique can be used in any section in real life, military, business, educational, governments and more. Also, I have shown various tools and how they function well.

References:

1. Artz, D. (2001). Digital steganography: Hiding data within data. IEEE Internet Computing, 75-80.
2. Provos, N., & Honeyman, P. (2012). Detecting Steganographic Content on the Internet.
3. Classification of Hiding Techniques Ref: F.A.P. Petitcolas, R.J. Anderson, and M.G. Kuhn, “Information Hiding – A Survey,” in Proc. Of the IEEE , vol. 87, No. 7, July 1999, pg. 1063
4. Steganography: Hiding Data Within Data. Retrieved December 6, 2014, from http://www.garykessler.net/library/steganography.htmlhttp://www.garykessler.net/library/fsc_stego.html
5. An Overview of Steganography for the Computer Forensics Examiner. Retrieved December 6, 2014, from http://www.garykessler.net/library/fsc_stego.html
6. http://en.wikipedia.org/wiki/Steganography#Network