THINK INDIA JOURNAL

ISSN:0971-1260
Vol-22- Issue-12-November-2019

A Comparative Overview & Analysis Of Text And Image Steganography

Bhawna Sharma

Assistant Professor, Department of Computer Science

Govt. College, Chhachhrauli, (Haryana), India

Email ID: bhawnasharma@live.com

Abstract

Information security is an important area of research and study that is gaining importance with passage of time. The main objective of information security is to secure the information from all kinds of threats and attacks. Many kinds of techniques have been invented to secure the information and the most popular among them is steganography [1]. Although in steganography [1] the text is sent to the destination in a very secured and hidden form as no one find out the existence of message, apart from sender and intended receiver. In Steganography, we compare two methods of plain text transmission-Text steganography &Image steganography according to their performance [2][3]. Hence in this paper, a new approach has been adopted to compare text steganography and image steganography[2][3].

Keywords: *Steganography, Information Security, Text Steganography, Image Steganography*

1. Introduction

This paper's focus is on a relatively new field of study in Information Technology known as Steganography. This paper will take an in-depth look at this technology by introducing the reader to various concepts of Steganography, a brief history of Steganography and a look at some of the Steganographic techniques available today. The paper will close by looking at how we can use Steganography in an open-systems environment such as the Internet, as well as some of the tools and resources available to help us accomplish this. Steganography or Stego, as it is often referred in the IT community, literally means, "covered writing" which is derived from the Greek language. Steganography is defined by Markus Kahn [4] as follows, "Steganography is the art and science of communicating in a way which hides the existence of the communication. In contrast to Cryptography, where the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present".

ISSN:0971-1260
Vol-22- Issue-12-November-2019

2. Goal of Steganography

Steganographic technologies will play a very important role in future of Internet security and privacy on open systems such as the Internet. Steganographic research is primarily driven by the lack of strength in the cryptographic systems and the desire to have complete secrecy in an open-systems environment. This is where Steganography comes in. Steganography can be used to hide important data inside another file so that only the parties intended to get the message, knows a secret message exists. To add multiple layers of security and to help subside the "crypto versus law" problems previously mentioned, it is a good practice to use Cryptography and Steganography together. The goal of steganography is to transmit a message through some innocuous carrier i.e. text, image, audio and video over a communication channel where the existence of the message is concealed. Steganography is one of the information hiding techniques and which can be categorized into linguistic steganography and technical steganography. Linguistic steganography defined by Chapman as "the art of using written natural language to conceal secret messages". A more specific definition by Krista Bennet in explaining linguistic steganography as a medium which required not only the steganographic cover that is composed of natural language text, but the text itself can be either generated to have a cohesive linguistic structure, or the cover text that begin with natural language. On the other hand, technical steganography is explained as a carrier rather than a text which can be presented, as any other physical medium such as microdots and invisible inks. The principle of information hiding is pioneered and documented in 1972, whereby Parnas designed a software system and each module's "interface of definition was chosen to reveal as little as possible about its inner workings". Many researchers are trying to carry out research by applying this concept in information hiding. There are three aspects in information hiding systems contend with each other: capacity, security and robustness. Capacity refers to the amount of information that can be hidden in the medium, whereas security is important when a secret communication is kept being secret and undetectable by eavesdroppers. Lastly, robustness can be explained as the amount of modification the stegomedium can withstand before an adversary can destroy hidden information.

3. Plain Text Transmission Type

A. Text Steganography:

Documents themselves can hide information: document text can conceal a hidden message through the use

ISSN:0971-1260
Vol-22- Issue-12-November-2019

of null ciphers (unencrypted messages), which Camouflage the real message in an innocent-sounding missive. Open coded messages, which are plain text passages, "sound" innocent because they purport to be about ordinary occurrences. Because many open-coded messages don't seem to be cause for suspicion, and therefore "sound" normal and innocent, the suspect communications can be detected by mail filters while "innocent" messages are allowed to flow through1. For example, the following null-cipher message was actually sent by a German spy WWII[5]:

Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suet's and vegetable oils.

Decoding this message by extracting the second letter in each word reveals the following, Hidden message: *Pershing sails from NY June 1.*

Document layout may also reveal information. Documents can be marked and identified by modulating the position of lines and words.[6]Message detection improved with the development of new technologies that could pass more information and be even less conspicuous. TheGermans developed microdot technology, which FBI Director J. Edgar Hoover referred to as "the enemy's masterpiece of espionage."[5] Microdots are photographs the size of a printed period having the clarity of standard-sized typewritten pages, which permits the transmission of large amounts of data, including drawings and photographs.[5] With every discovery of a message hidden with an existing application, a new steganographic application is being devised. Old methods are given new twists. While drawings have often been used to conceal or reveal information, computer technology has, in fact, sparked a revolution in such methods for hiding messages. Space limitations prevent further discussion here. For more information on techniques for hiding information, see Peter Wayner's Disappearing Cryptography.[5]Now we describe different method of Text Steganography and compare with respect to their security level & how conveniently their method used.

B. Image Steganography:

There are many applications for techniques that embed information within digital images [7]. The dispatch of hidden messages is an obvious function, but today's technology stimulates even more subtle uses. In-band captioning, such as movie subtitles, is one such use where textual information can be embedded within the image. The ability to deposit image creation and revision information within the image provides a form of revision tracking as another possible application of digital steganography. This avoids the need for maintaining two separate media, one containing the image itself and one containing the revision data.

A block diagram of a generic blind image steganographic system is depicted in Fig.1. A message is embedded in a digital image by the Stegno system encoder, which uses a key or password [7]. The resulting

ISSN:0971-1260
Vol-22- Issue-12-November-2019

Stegno image is transmitted over a channel to the receiver, where it is processed by the Stegno system decoder using the same key. During transmission, the Stegno image can be monitored by unintended viewers who will notice only the transmittal of the innocuous image without discovering the existence of the hidden message. Within the past few years, there has been a surge of research in the area of digital image steganography. A majority of the work in the area has been performed on invisible digital watermarking. This thrust can be attributed to the desire for copyright protection, spurred by the widespread use of imagery on the Internet and the ease in which a perfect reproduction of a digital image is obtained. The objective of digital watermarking is to embed a signature within a digital image to signify origin or ownership for the purpose of copyright protection. Once added, a watermark must be resistant to removal and reliably detected even after typical image transformations such as rotation, translation, cropping, and quantization.

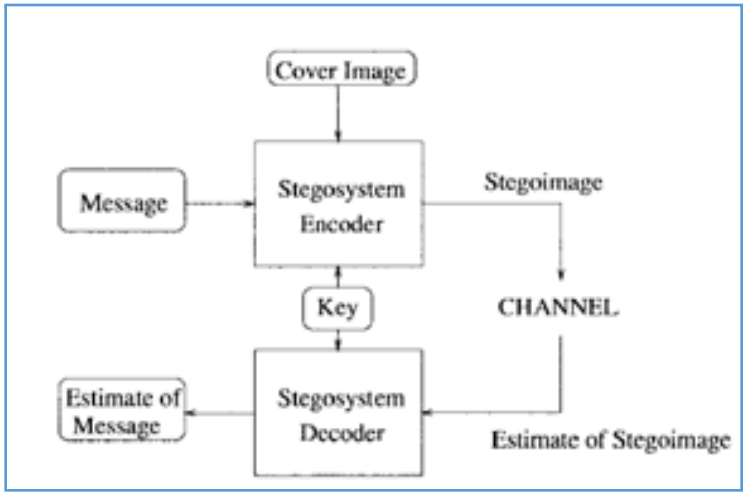

Figure 1: Overview of Steganography System

C. Still Imagery Steganography

The most widely used technique today is hiding of secret messages into a digital image. This steganography technique exploits the weakness of the human visual system (HVS) [9]. HVS cannot detect the variation in luminance of color vectors at higher frequency side of the visual spectrum. A picture can be represented by a collection of color pixels. The individual pixels can be represented by their optical characteristics like 'brightness', 'chroma' etc. Each of these characteristics can be digitally expressed in terms of 1s and 0s.

For example: a 24-bit bitmap will have 8 bits, representing each of the three-color values (red, green, and blue) at each pixel. If we consider just the blue, there will be 28 different values of blue. The difference between 11111111 and11111110 in the value for blue intensity is likely to be undetectable by the human

ISSN:0971-1260
Vol-22- Issue-12-November-2019

eye. Hence, if the terminal recipient of the data is nothing but human visual system (HVS) then the Least Significant Bit (LSB) can be used for something else other than color information.

This technique can be directly applied on digital image in bitmap format as well as for the compressed image format like JPEG. In JPEG format, each pixel of the image is digitally coded using discrete cosine transformation (DCT). The LSB of encoded DCT components can be used as the carriers of the hidden message. The details of above techniques are explained below:

1. Modification of LSB of a cover image in 'bitmap' format [10]

In this method binary equivalent of the message (to be hidden) is distributed among the LSBs of each pixel. For example, we will try to hide the character 'A' into an 8-bit color image. We are taking eight consecutive pixels from top left corner of the image. The equivalent binary bit pattern of those pixels may be like this: -

00100111 11101001 11001000 00100111 11001000 11101001
11001000 00100111

Then each bit of binary equivalence of letter 'A' i.e. 01100101 are copied serially (from the left-hand side) to the LSB's of equivalent binary pattern of pixels, resulting the bit pattern will become like this: -

1. 00100110 11101001 11001001 00100110 11001000 11101001

11001000 00100111

The only problem with this technique is that it is very vulnerable to attacks such as image compression and formatting.

2. Apply of LSB technique during discrete cosine transformation (DCT) [11] on cover image

The following steps are followed in this case: -

- The Image is broken into data units each of them consists of 8 x 8 block of pixels.
- Working from top-left to bottom-right of the cover image, DCT is applied to each pixel of each data unit.
- After applying DCT, one DCT Coefficient is generated for each pixel in data unit.
- Each DCT coefficient is then quantized against a reference quantization table.
- The LSB of binary equivalent the quantized DCT coefficient can be replaced by a bit from secret message.
- Encoding is then applied to each modified quantized DCT coefficient to produce compressed Stego Image.

ISSN:0971-1260
Vol-22- Issue-12-November-2019

Figure 2: Example of still imagery steganography. Left hand side image is the original cover image, whereas right hand side does embed a text file into the cover image make the stego image.

D. *Audio and Video Steganography[11,12,13]*

In audio steganography, secret message is embedded into digitized audio signal which result slight altering of binary sequence of the corresponding audio file. There are several methods are available for audio steganography. Some of them are as follows:

1. *LSB Coding:*

Sampling technique followed by Quantization converts analog audio signal to digital binary sequence.

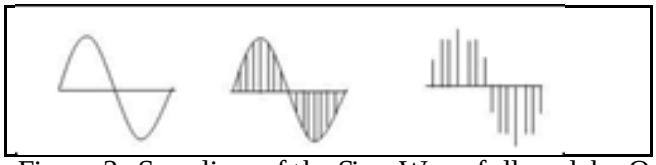

Figure 3: Sampling of the Sine Wave followed by Quantization process.

In this technique LSB of binary sequence of each sample of digitized audio file is replaced with binary equivalent of secret message.

Table 1:For example if we want to hide the letter 'A' (binary equivalent 01100101) to an digitized audio file where each sample is represented with 16bits, then LSB of 8 consecutive samples (each of 16 bit size) is replaced with each bit of binary equivalent of the letter 'A'.

ISSN:0971-1260
Vol-22- Issue-12-November-2019

Sampled Audio Stream (16 bit)	'A' in binary	Audio stream with encoded message
1001 1000 0011 1100	0	1001 1000 0011 1100
1101 1011 0011 1000	1	1101 1011 0011 1001
1011 1100 0011 1101	1	1011 1100 0011 1101
1011 1111 0011 1100	0	1011 1111 0011 1100
1011 1010 0111 1111	0	1011 1010 0111 1110
1111 1000 0011 1100	1	1111 1000 0011 1101
1101 1100 0111 1000	0	1101 1100 0111 1000
1000 1000 0001 1111	1	1000 1000 0001 1111

2. Video Steganography

Establishing hidden communication is one of the security areas which is attract more attention in recent years because of rapid growth of the Internet and expansion of communications. One of the main and relatively new hidden communication methods is steganography. In steganography the data are hidden in a cover media so that other persons will not notice that such data is there. This is a major distinction of this method with the other methods of hidden exchange of information such as cryptography. Steganography is mainly applied to media such as images, text, video clips, music and sounds [8]. MMS is a technology that allows a user of a properly enabled mobile phone to create, send, receive and store messages that include text, images, audio and video clips the name of such a technique derives from the Greek language, and it literally means "covered writing". The basic idea is that none could gather that a document is hiding a secret, while the receiver can securely extract the secret from the carrier, or cover, message.

The lightweight or feasible steganography is made by means of the exclusive use of a Smartphone. Because the actual smart phones are equipped with a camera, they locally store the photos and they have some power of computation.

The screens of such small devices are usually few hundred pixels per side, and can display, at the best, several thousand colors. The CPU of smart phones are rarely equipped with floating point co–processors and operates at a frequency that is orders of magnitude smaller with respect to the PCs. Moreover, the onboard RAM of the smart phones is orders of magnitude smaller than the one into the PCs. In the next section we present the main ideas of the steganography.

The most important issues in steganography are: *security*, *payload*, and *robustness*. The security of the steganography means that the hidden contents has to be "invisible" both perceptually and statistically, *i.e.* an eavesdropper cannot detect the presence of a secret by using any accessible means.

ISSN:0971-1260
Vol-22- Issue-12-November-2019

4. Performance Analysis

Table 2. Analysis on the basis of advantage and disadvantage

Method	Advantage	Disadvantage
Text steganography	Suitable for highly confidential data.	Not easy to develop.
Image steganography	Easy to develop &but has to take utmost care while implementing the same.	If image is little distorted /change in colour brightness, then easy to intrude.

5. Conclusion

We have explored the limits of text & image Steganography, both theory and practice. We started by outlining several techniques, both ancient and modern. We, then discussed a few possible approaches to theory of the subject. Text steganography and image steganography each are capable to hide data, it is related to content of text and how steganography is applied. Text steganography is difficult to implement, however Image steganography can easily be compromised, if not implemented in the right way.

6. References

[1] On Public-key Steganography in the Presence of an ActiveWarden", S Craver, IBM Research Report RC 20931, July 23, 1997

[2] Steganography - Wikipedia, http://en.wikipidea.org/wiki/Steganography

[3] A history of steganography - Fabien Petitcolas

[4] Johnson, Neil F., "Steganography", 2000, URL: http://www.jjtc.com/stegdoc/index2.html

[5] Echo Hiding', D Gruhl, A Lu, W Bender, in Information Hiding, Springer Lecture Notes in Computer Science

[6] Communication theory of secrecy systems", CE Shannon, in Bell Systems Technical Journal v 28 (1949)

[7] Towards Robust and Hidden Image Copyright Labeling", E Koch, J Zhao, Proceedings of 1995 IEEE Workshop on NonlinearSignal and Image Processing (Neos Marmaras, Halkidiki, Greece, June 20{22, 1995)

[8] Liability and Computer Security: Nine Principles", RJ Anderson, in Computer Security|ESORICS 94, Springer

[9] `An Introduction to the Psychology of Hearing', BCJ Moore, Academic Press 1989

ISSN:0971-1260
Vol-22- Issue-12-November-2019

[10] Auditory masking and MPEG-1 audio compression," E Ambikairajah, AG Davis, WTK Wong, IEE Electronics & CommunicationEngineering Journal v 9 no 4 (Aug 97)

[11] Digital Watermarks for Audio Signals," L Boney, AH Tew_k, KN Hamdy, in IEEE International Conference on MultimediaComputing and Systems, June 17{23, 1996 Hiroshima, Japan;

[12] Tamper Resistance a Cautionary Note", RJ Anderson, MG Kuhn, in Proceedings of the Second Use nix Workshop on ElectronicCommerce (Nov 96)

[13] `Copyright theft', J Gurnsey, Aslib Gower, 1995