STEGANOGRAPH(Y)SM- A Concealed world

Manpreet Kaur[1], Raman Chadha[2]

Computer Science Engineering, CGCTC Jhanjeri, Punjab

Abstract **- Steganography is meant for confidential communication as well as secret data sharing between sender and a receiver using various media files. Today, it's being broadly used over Internet. Due to the rapid development in Technology and Communication and the use of Internet at alarming rate, the security of the data and information is a major concern these days. Every day, confidential data has been jeopardize and unauthorized access of data has crossed the limits. Steganography provide us to conceal the presence of confidential data, difficult to detect the embedded data and enhancing the stealthiness of the encrypted data. The crucial information is being encrypted into media file such as images, audio, text as well as video as it is the art of hiding information. As steganography is very close to cryptography and its applications so both are widely used techniques that encrypt data in order to cipher or hide their existence. This paper focuses on various pros and cons of steganography, overview to its techniques and relationship with cryptography**.

Keywords— confidential, cryptography, cipher, steganography, stealthiness, unauthorized

I. INTRODUCTION

Steganography, when it was first used in English in the sixteenth century, referred to cryptography — writing in codes and ciphers (a secret or disguised way of writing).Steganography has been widely used, including both in historical times and nowadays. Some known examples are:-

- Text hidden on wax-covered tablets
- Tattooed message on the head of a messenger
- Invisible ink (used in WW II)
- Generation of Null ciphers

Another form of steganography is in null ciphers, or unencrypted text messages. For example, one could hide a text message within a paragraph of words, so that by isolating every 20th word, the secret message can be detected. The paragraph itself would sound innocent to escape detection. This form of steganography was often used in wars among spies. Recently, computerized steganography has become popular. Using different methods of encoding, secret messages can be hidden in digital data, such as .bmp or .jpg images, .wav audio files, or e-mail messages.[1]

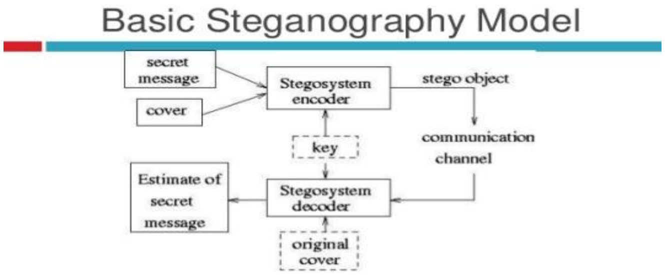

Fig:1.1 Basic Model of steganography

Steganography is a process of hiding covert information into a carrier. A carrier is the original message or a file in which hidden information will be stored inside of it..In Steganography a steg or stego file is the embedded file which is supposed to be transmitted over transmission medium. Data can be hidden in a wide range of media files, like video and audio etc. Files on a computer's hard disk can also be made invisible to those who do not have the file name and its corresponding password. The key concept behind steganography is that the message to be transmitted is not detectable to the casual eye. In fact, people who are not intended to be the recipients of the message should not even suspect that a hidden message exists.

It is the method of transmitting secret messages through innocuous carriers in such a way that the very existence of the embedded message is undetectable Examples of cover carriers: images, audio, video, text data. There are two variants of Steganography systems :

- *Digital steganography*:- The word "Digital" describes electronic technology that generates, stores and processes data that is sound, image, video or data file in contrast to such a file in another medium, such as a photograph printed on a photo paper . Digital steganography is used to hide a message in a cover where that hidden message is the object of communication.

- *Digital watermarking*: The term "Watermark" is a small piece of embedded information which can proof copyrighted material. For example Fingerprint is very similar, but is intended to track the concrete copy of copyrighted data. Digital watermarking is used to embed copyright, ownership and license information in a cover, here that cover is object of communication. [3]

Embedding Process of Steganography:-

Fig 1.1 shows the whole process of steganography. In this process to supply a secret message, the original image, that is the cover image, is slightly modified by the embedding algorithm to obtain the stego image. The embedding process may depend on a secret stego key

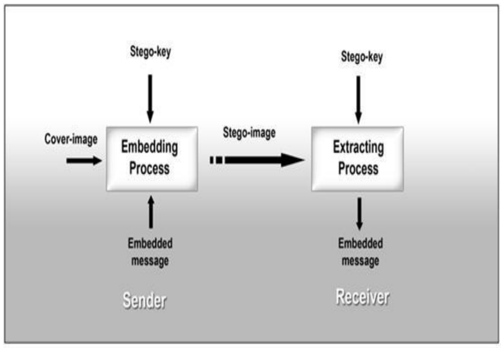

Fig 1.2 Process of Steganography

The purpose of stego keys is used to control the embedding process, such as the selection of pixels or coefficients carrying the message, etc. the secret information is encoded in another form by using a secret key before sending, which can only be decoded with secret keys. In the Steganography system, before the concealing process, the sender must select the appropriate message carrier i.e. Video, audio, image or text and select the effective covert messages as well as the robust password (that supposed to be known by the receiver also). Then the most appropriate Steganographic algorithm must be selected that able to encode the message. Then the sender may send the stego file by email or by other modern techniques. The Stego file is the carried message with the covert information. After receiving the message by the receiver, he can decode that stego file by using the extracting algorithm and with the use of that same password used by the sender.

II .OVERVIEW OF EMBEDDING TECHNIQUES

The various embedding techniques in Steganography process have various features that characterises their strengths and weaknesses. Features like:

- Embedding capacity: Embedding capacity is the amount of data that can be added into the cover-media without decomposing its integrity.
- Invisibility: It is necessary that to avoid suspicion the embedding should occur without significant degradation or loss of perceptual quality of the cover media.
- Robustness: It refers to the ability of embedded data to remain intact if the stego-image undergoes various transformations such as scaling, rotation, cropping or compression.
- Tamper resistance: It refers to the difficulty to alter or forge a message once it is embedded in a cover-media, such as replacing a copyright mark with the one claiming legal ownership.
- Computational complexity: Computational complexity of steganography technique employed for encoding and decoding is another consideration and should be given importance

Categories of Steganography: -Johnshon and Katzenbeisser group steganographic techniques into six categories:-

In all methods of steganography, something is done to conceal a message; naturally, these actions or techniques are used in whole process. The six categories of steganography are:

1. Substitution system techniques

2. Transform domain techniques

3. Spread spectrum techniques

4. Statistical method techniques

5. Distortion techniques

6. Cover generation techniques

Substitution System: - In Substitution system it will replaces redundant bits of a cover with the bits from the covert message. Several steganography tools that are available use the Least-Significant Bit (LSB) method of encoding the secret message. LSB works like this: In a digital cover (picture, audio, or video file), there is huge amount of redundant space; so the advantage of that is to hide another message, on the bit level, within the digital cover.

For example, the following string of bytes represents part of a cover, a picture:

10000100 10000110 100001001 10001101

01111001 01100101 01001010 00100110

Each byte is comprised of eight bits; these bits make up a color value in our picture, a shade of red, or blue, etc. Now, the bits that make up the byte go from left to right in order of importance to the color value they are representing. For example, changing the first bit in our first string from a 1 (10000100) to a 0 (00000100) will drastically change the color, as opposed to changing the last number from a 0 (10000100) to a 1 (10000101). It is that last bit that is considered the least significant, because changing its value has little effect on the information the byte is representing.

The LSB technique is commonly used in steganography applications because the algorithm is quick and easy to use; LSB also works well with gray-scale as well as color images.[7]

Transform Domain Techniques: - This technique is also very effective and a little trickier to explain. Basically, transform domain techniques hide message data in the "transform space" of a signal. (If you are saying "Huh?" to yourself, hold on, I will explain.) Every day on the Internet, people send pictures back and forth, and most often they use a JPEG format. JPEGs are interesting in that they compress themselves when they close. In order for this to take place, they have to get rid of excess data, excess bits that would otherwise prevent them from compressing. During compression, a JPEG will make an approximation of itself to become smaller; that change, that approximation, is transform space, and that change can be used to hide information.

Spread-Spectrum Techniques:-it is further divided into two techniques

- Direct Sequence:-In direct sequence spread spectrum, the stream of information to be transmitted is divided into small pieces. Each of the pieces is allocated to a frequency channel of the spectrum. The data signal, at the point of transmission, is combined with a higher data-rate bit sequence that divides the data according to a predetermined spread ratio. Redundant data-rate bit sequence code helps the signal resist interference and enables the original data to be recovered if any of the data bits are damaged during the transmission.

- Frequency Hopping This technique divides a broad slice of the bandwidth spectrum into many possible broadcast frequencies. In general, frequency-hopping devices use less power and are cheaper, but the performance of direct sequence spread-spectrum systems is usually better and more reliable.

Statistical Methods:-Statistical methods use what is called a "1-bit" steganographic scheme. This scheme embeds one bit of information only in a digital carrier, and thus creates a statistical change, even if it is only a slight one.

Distortion Techniques:-This method of steganography creates a change in a cover object to hide information. The secret message is recovered when the algorithm compares the changed, distorted cover with the original.

Cover Generation Methods:-Cover generation methods are probably the most unique of the six types. Typically, a cover object is chosen to hide a message in, but that is not the case here. A cover generation method actually creates a cover for the sole purpose of hiding information. Spam Mimic is an excellent example of a cover generation method.

III. TYPES OF STEGANOGRAPHY

Steganography can used for almost all digital file formats, but the formats those are with a high degree of redundancy are more suitable. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display. The redundant bits of an object are those bits that can be altered without the alteration being detected easily [4]. Image and audio files especially comply with this necessity, while research has also uncovered other file formats that can be used for information hiding. There are four categories of file formats that can be used for Steganography shown in fig. 3.

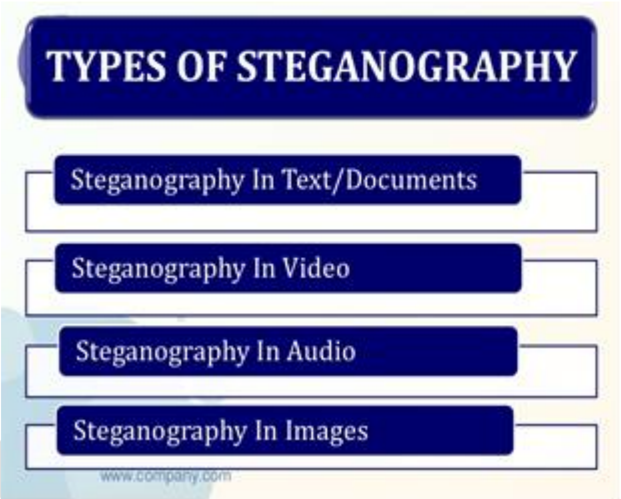

Fig:-2.1 Types of Steganography

Steganography can be divided into two broad categories namely technical steganography and natural language steganography. Technical Steganography is a technique of hiding information inside a medium such as image, audio, and video. Natural language Steganography is the art of using natural language to conceal secret message. It focuses on hiding information in text by using steganography and linguistic steganography.

.*Image Steganography*:-The most common cover objects used for steganography are images. The scope of image steganography is large because of the various image formats available such as BMP,JPEG, PNG, GIF etc. In this common approaches are used :- LSB modification ,Masking Filtering and Transformations via algorithms Composed of hiding information inside of the LSB of an image Leads to a few requirements. Image must have suitable "noise" Image must be of sufficient size Must be able to "hide in plain sight".[2]

*Audio Steganography:-*Audio steganography, the hiding of messages in audio "noise" and in frequencies which humans can't hear, is another area of information hiding that relies on using an existing source as a space in which to hide information. Human Auditory System (HAS) has a large dynamic range that it can listen through .Perceives over a range of power >1,000,000:1and Range of frequencies > 1,000:1It makes it hard to add remove data from original sources. HAS has a weakness, though: sound differentiation.[6]

Text Steganography:- Text steganography is the method of hiding information within text messages. The huge availability of electronic textual information and the difficulty of serious linguistic analysis make this an interesting medium for steganographic information hiding. Text is also one of the oldest media used in steganography. In other words .it is the formatting of an existing text, changing words within a text, or generating random character sequences.

Video steganography:-Combines ideas of both image and audio stego. In this frames are coded similarly to jpeg images therefore have DCT coefficients. It can use LSB manipulationto hide information in DCT coefficients.

III. PROS AND CONS OF STEGANOGRAPHY

Steganography can be used for wide range of applications such as, in defence organisations for safe circulation of secret data, in military and intelligence agencies, in smart identity cards where personal details are embedded in the photograph itself for copyright control of materials. Whereas misuse of this technique stated in major attack in US. The United Nations Office on Drugs and Crime (UNODC) released a publication titled "The use of the Internet for terrorist purposes" in September 2012 that describes use of steganography by terrorists for covert communications.. For instance terrorists may use this technique for their secret secure communication or anti-virus systems can be fooled if viruses are transmitted in this way.

IV. COMPARINGSTEGANOGRAPHY AND CRYPTOGRAPHY

Steganography and cryptography are closely related. Cryptography embeds messages so it can't be understood. Steganography on the other hand, hide the message so there is no knowledge of the existence of the message. With cryptography, comparison is made between portions of the plaintext and portions of the cipher text. In steganography, comparisons may be made between the cover-media, the stego-media, and possible portions of the message. The end result in cryptography is the cipher text, while the end result in steganography is the stego-media. The message in steganography may or may not be encrypted. If it is encrypted, then a cryptanalysis technique is applied to extract the message

V. CONCLUSION

In this paper a overview for the main techniques and various types of Steganography were presented in to six categories followed by various uses and mis-uses of steganography techniques is mentioned. After the study of all techniques it is assumed that as already various latest and improved techniques are developing. Researchers may further develop the new and quick algorithms as each single technique leave a option for further in depth researches that can be helpful to detect various stegos in one go and which is also easier to implement and less costly.

REFERENCES

[1]. Wikipedia.org/wiki/Steganography

[2]. Yangren-er.Zhengzhiwei,Taoshun,Dhingshilei- (ICMTMA) - Image steganography with DES encryption preprocessing - IEEE conference publications- 2014

[3]. Shaveta Mahajan, Arpinder Singh-(IJARCSSE)- A Review of Methods and Approach for Secure Stegnography- 2012.

[4]. Rakhi, Suresh Gawande A REVIEW ON STEGANOGRAPHY METHODS –IJAREEIE-2013.

[5]. JasleenKour, DeepankarVerma- Steganography techniques-a review paper –IJERMT-2014.

[6]. AshimaWadhwa - A Survey on Audio Steganography Techniques for Digital Data Security-IJARCCSE-April 2014.

[7]. Thangadurai, K. ;Sudha Devi, G. -An analysis of LSB based image steganography techniques-(ICCCI) –IEEE conference publications- 2014