MJRET
Open Access
Multidisciplinary Journal of Research in Engineering and Technology
Journal homepage: www.mjret.in
ISSN:2348 - 6953

STEGANOGRAPHY: THE ART OF COVERT COMMUNICATION

Sudhanshi Sharma[1], Umesh Kumar[2]
Computer Engineering, Govt. Mahila Engineering College,
Ajmer, India
[1]sudhanshisharma91@gmail.com,[2]ume2222@gmail.com

Abstract: *This paper presents a base study of Steganography. Steganography is an important area of research in recent years involving a number of applications. In another words we can say that it is technique of hidden communication in which existence of secret hidden remains invisible. Here we have critically compared various information security methods and also have covered Steganography overview, its major types, classification with less detail of Steganalysis, which is the art and science of defeating Steganography.*

Keywords: *Cryptography, Fingerprinting, Steganalysis, Steganography, Watermarking.*

1. INTRODUCTION

In the present word of communication, internet is the most popular medium now a day. But message transmission over the internet is facing some problem such as data security, copyright control etc. Security has become a critical feature for thriving networks. So we need secret communication methods. *Cryptography* and *Steganography* are well known and widely used technique that manipulates information (message) in order to cipher or hide their existence [1].

Cryptography scrambles a message by using certain cryptographic algorithms for converting (encrypt) the secret data (information) into unintelligible (cipher text) form by using a secret key it can only be decoded (decrypted) by the party that possesses the associated key. When encrypted message crushed by someone, it is known as cryptanalysis or code breaking [2, 3].

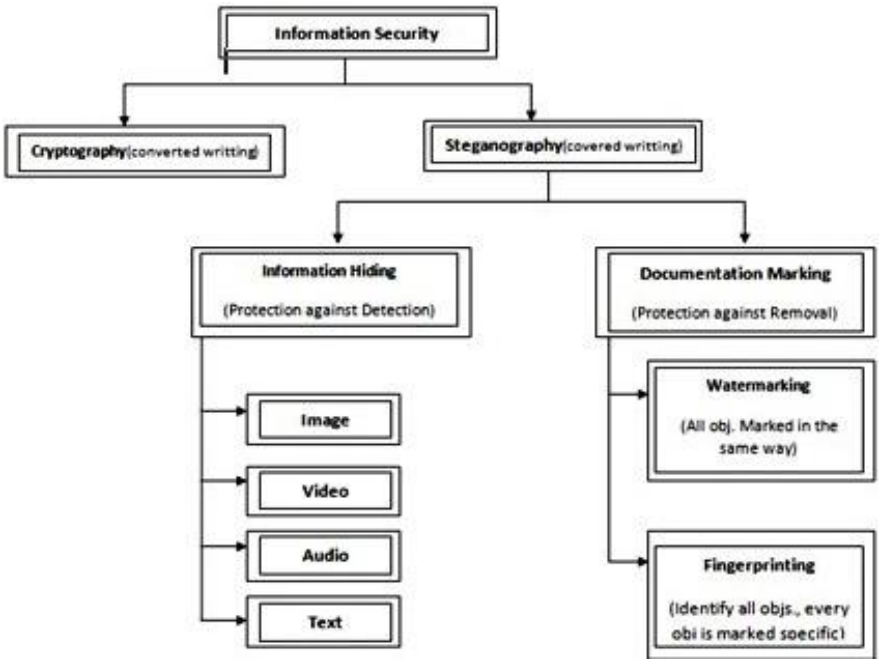
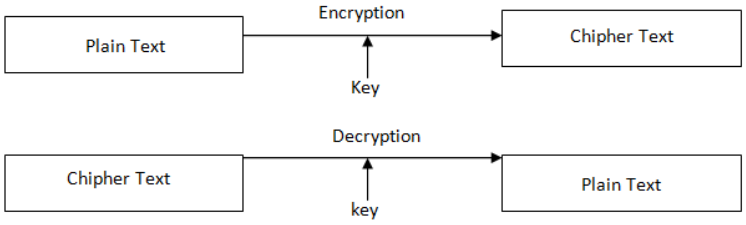


Fig.1: Types of Information Security



Cryptographic Flow

Fig.2: Cryptographic Flow

Steganography is the activity of hiding the existence of communication. The process used in Steganography makes it tough to observe that there is a secret message inside an innocent file (cover image). By using this method anyone can hide the message itself, and the fact that you are sending the message. In this context the cover medium hide the secret information, which may be encrypted using the stego-key & get the resultant file i.e. stego-medium [2, 3].

Two other technologies that are adjacent to Steganography, one is *Watermarking* and another is *Fingerprinting*. These technologies are basically focused on the protection of intellectual property. In watermarking all the instance of an object are “signed” in the same way. The use of watermarking is usually a signature of signifies source or ownership for intend of copyright protection. On the other hand, distinct marks are implant on different copies of the carrier object that are provided to distinct customers. This allows the intellectual property owner to recognize customers who crack their licensing agreement by giving the stuff to third parties. In fingerprinting and watermarking the fact that data is hidden inside the files may be known by people. Sometimes it may even be visible. While in Steganography the invisibility of the information is essential [3].

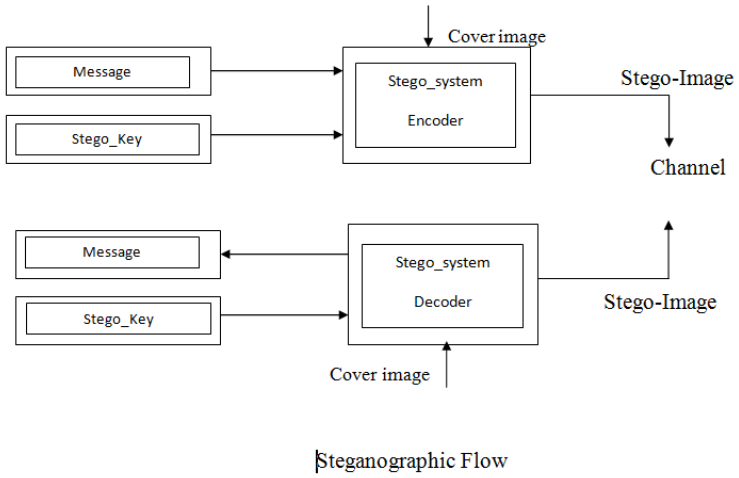


Fig.3: Steganographic Flow

2. COMPARISON OF STEGANOGRAPHY, WATERMARKING AND ENCRYPTION

Comparison among Steganography, watermarking and cryptography as following: [4]

Criterion/Method	Steganography	Watermarking	Encryption
Carrier	any digital media	mostly image/audio files	usually text based, with some extensions to image files
Secret data	payload	watermark	plain text
Key	optional		necessary
Input files	at least two unless in self-embedding		one
Detection	blind	usually informative (i.e., original cover or watermark is needed for recovery)	blind
Authentication	full retrieval of data	usually achieved by cross correlation	full retrieval of data
Objective	secrete communication	copyright preserving	data protection
Result	stego-file	watermarked-file	cipher-text
Concern	delectability/ capacity	robustness	robustness
Type of attacks	steganalysis	image processing	cryptanalysis
Visibility	never	sometimes (see Fig. 2)	always
Fails when	it is detected	it is removed/replaced	de-ciphered
Relation to cover	not necessarily related to the cover. The message is more important than the cover.	usually becomes an attribute of the cover image. The cover is more important than the message.	N/A
Flexibility	free to choose any suitable cover	cover choice is restricted	N/A
History	very ancient except its digital version	modern era	modern era

Table.1: Comparison of Information Security Techniques

3. STEGANOGRAPHY

The term Steganography came into use in 1500s after the appearance of Trithemius book on the subject steganographia. The word Steganography technically means covered or hidden writing. Its existence can be found back to 440 BC. The term Steganography was invented at the termination of the 15th century, the use of Steganography was ancient. In the past, messages were hidden on the back of wax writing tables, written on the stomachs of rabbits or tattooed on the scalps of salves. Invisible ink & microdots has been in demand for centuries for fun by children & students and for serious work by spies & terrorists [5].

The majority of today steganographic system uses multimedia object like image, audio, video etc as cover medium because people usually send out digital images over internet communication as email, whatsapp, facebook etc. In present time Steganography utilize the chance of hiding data into digital multimedia object and at the network packet level too.

Hiding information into a medium requires following elements:

1. The cover medium (C) that will hold the secret message.
2. The secret message (M) may be plain text, digital image file or any type of data.
3. The steganographic techniques.
4. A stego-key (K) may be used to hide and unhide the message.

3.1 Classification of Steganography

There are two general approaches to classify steganographic system. The first approach is based on the type of cover file while the second approach is based on the hiding method or layout of modification used in the embedding process [6].

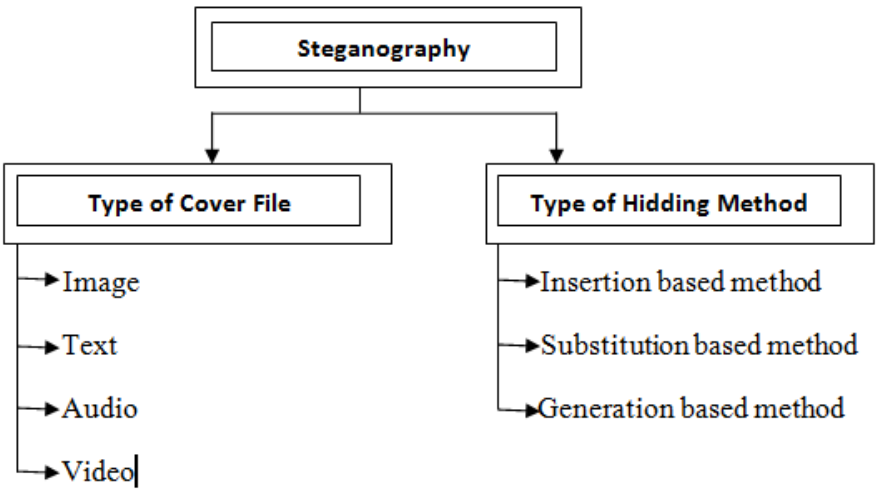


Fig.4: Classification of Steganography

Since many kid of digital media can be used as cover file of Steganography. However the properties of these cover files vary from one to another & these properties control how the secret data can be hidden in those cover file.

Image Steganography: Taking the cover object as image in Steganography is known as image Steganography. Generally in this technique pixel intensities are used to hide the information.

Video Steganography: It is a technique to hide any kind of files or information into digital video format. Video (combination of pictures) is used as carrier for hidden information. Generally discrete cosine transform (DCT) alter values (e.g. 5.668 to 6) which is used to hide the information in each of the image in the video, which is not noticeable by the human eye. Video Steganography uses such as H.264, MP4, MPEG, AVI or the other video formats.

Audio Steganography: When talking audio as a carrier for information hiding it is called audio Steganography. It has become very significant medium due to voice over IP (VOIP) popularity. Audio Steganography uses digital audio formats such as WAVE, MIDI, AVI, MPEG or etc for Steganography. The methods are commonly used for audio Steganography are: LSB coding, Parity coding, Phase coding, Spread coding, Spread coding and Echo hiding.

Text Steganography: General technique in text Steganography, such as number of tabs, white spaces, capital letters, just like Mores code and etc is used to achieve information hiding.

Protocol Steganography: When taking cover object as network protocol such as TCP, UDP, ICMP, IP etc. Where protocol is used as carrier is known as network protocol Steganography. In the OSI network layer model there exist covert channels where Steganography can be achieved in unused header bits of TCP/IP fields. Regardless of the cover type used for data hiding. Steganography can be classified according to the method used to hide secret data. Accordingly there are three ways to hide secret data in cover files:-

Insertion Based Method: This method depends on finding some areas in cover files which are usually ignored by applications that read this cover file and then embedding the secret data in these areas. Since this method inserts the secret data inside the cover file. The size of the stego file would be larger than the size of cover file. As a result, the contents of the cover file would not be changed after the embedding process since this method relies on accumulating or adding the secret data to the cover file.

Substitution Based Method: Unlike the insertion based method, this method does not add the secret data to the cover file data. However, substitution based method depends on finding some insignificant regions or information in cover file and replacing this information with the secret data. Therefore, the size of both the stego file and the cover file are similar since some of the cover data is just modified or replaced without any additional data. However, the quality of cover file can be degrading after the embedding process. Additionally, the limited amount of insignificant information in cover file restricts the size of secret data that can be hidden.

Generation Based Method: Unlike both methods explained above, this method does not need a cover file since it uses secret data to generate appropriate stego files. One of the Steganography detection techniques depends on comparing cover files with their stego files. Therefore, one advantage of the generation based Steganography is preventing such kind of detection since only stego file are available and there is no cover files used. The major limitation of this method is the limited stego files which can be generated. Moreover, the

generated stego files might be unrealistic files for end users (e.g. an image contains different shapes and colour without any sense or a text without any meaning) therefore, the main media for such technique are random looking image and English text files.

4. STEGANALYSIS

Steganalysis is a new research area with few write-ups appearing before the late-1990s. Steganalysis is "the approach of identifying Steganography by looking at variation between bit patterns and abnormally large file sizes". It is a process of recognizing and interpreting unusable covert messages. The purpose of Steganalysis is to discover doubtful information streams, find out whether or not they have hidden information encoded into them, and try to retrieve that secret message. [7]

The problem of Steganalysis is that:

1. The doubtful information stream, such as a file or a signal, may or may not have hidden information encoded into them.
2. The secret data, if any, may have been encrypted before being inserted into the file or signal.
3. Some of the suspicious file or signal may have unconnected data or noise encoded into them for making analysis extremely time consuming.
4. Until it is possible to completely retrieve, decrypt and explore the hidden information, usually one has only a doubtful information stream and cannot be assured that it is being used for transferring secret information.

4.1 Types of Attacks

Attacks and analysis on hidden information may take various forms: detecting, obtaining, and defusing, destroying or modifying hidden data. An attack process is based on what data is available to the steganalyst (A person skilled at finding messages hidden using steganography) [7]. The possible attacks on a stego media can be one of the following:

1. ***Steganography-only attack:*** Only the Steganography medium is accessible for evaluation.
2. ***Known-carrier attack:*** The original cover (the carrier) and Steganography medium both exist for analysis.
3. ***Known-message attack:*** The hidden data is identified.
4. ***Chosen-Steganography attack:*** The Steganography media and algorithms or tools are both known.
5. ***Chosen-message attack:*** A recognized message and Steganography tool or algorithms are used to produce Steganography media for future analysis and comparison. The aim of this attack is to find out related patterns in the Steganography medium that may point to the use of particular Steganography tools or algorithms.
6. ***Known-Steganography attack:*** The Steganography tool or algorithm as well as the carrier and Steganography medium, all are known.

5. APPLICATION OF STEGANOGRAPHY

The sudden advent in the Steganography technologies suggests the great demand of robust Steganography systems. These systems cover vast application areas. A few most common

applications are Owner Identification, Copy Protection, Broadcast Monitoring Medical applications, Fingerprinting, Data Authentication etc.

6. CONCLUSION

Steganography is related to Cryptography. These both techniques are used for security purposes but they both have different approaches or implementation. Steganography hides the information in information, so it hides the existence of the communication. Another way is to deform the secret data into an unusable or non-interpretable form is called cryptography. At last if some secret data having the owner identification is hidden in the medium to claim the originality of the medium, this process is called watermarking. Steganography classify by two types: according to type of cover image (text, audio, video, image, and network) & according to the method used to hide data (insertion, substitution, generation). Attacks on methods of Steganography are called Steganalysis. Now a day's Steganography has a vast application area in digital world.

REFERENCES

[1]. Arvind Kumar, Km. Pooja, "Steganography- A Data Hiding Technique", International Journal of Computer Applications (0975-8887) Volume-9 No. 7, November 2010.

[2]. Sujuy Narayana, Gaurav Prasad, "Two New Approaches for Secured Image Steganography Using Cryptography Techniques and Type Conversions", Signal & Image Processing: An International Journal (SIPIJ), Vol. 1, No. 2, December, 2010.

[3]. M. Sitaram Prasad, S. Naganjaneyulu, Ch. Gopi Krishna, C. Nagaraju, "A Novel Information Hiding Technique for Security By Using Image Steganography", Journal of Theoretical & Applied Information Technology (JATIT) © 2005-2009.

[4]. Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, "Digital Image Steganography: Survey and Analysis of Current Methods", Elsevier, Signal Processing, 2009, pp. 727-752.

[5]. U. Rizwan, H. Faheem Ahmed, "A New Approach In Steganography Using Different Algorithms and Applying Randomization Concept", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 1, Issue 9, November 2012.

[6]. Mehdi Hussain, Mureed Hussain, "A Survey of Image Steganography Techniques", International Journal of Advanced Science & Technology, Vol. 54, May, 2013.

[7]. Vijay Kumar Sharma, Vishal Shrivastava, "A Steganography Algorithm for Hiding Image in Image by Improved LSB Substitution by Minimize Detection", Journal of Theoretical and Applied Information Technology, Vol. 36, No. 1, February, 2012.