Volume 5, Issue 5, May 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Secured Approach of Data Transfer through Steganography Techniques

Juhi Gupta[*1], Barkha Sain[2], Ruchi Singhal[3]
[1, 2] Assistant Professor, Computer Science Dept., Maharaja Agrasen College, Delhi University, Delhi, India
[3] Ex Systems Engineer, Tata Consultancy Services, Gurgaon, India

Abstract---In this era of Internet, where digital media data is rapidly distributed and transferred, it has become much easier to gain information, edit it, modify or duplicate the digital data. Therefore, protection of the secured data and its integrity has become a necessity in today's world. Steganography is one of the technique through which secret data is embedded inside various digital media like image, audio, video etc. so that the embedded data becomes imperceptible or invisible to the casual eye. In this paper, various steganography techniques available today have been discussed with its own advantages and disadvantages.

Keywords: Steganography, stego image, cover, steganography classification, stego key

I. INTRODUCTION

The word steganography is formed by the combination of two Greek words i.e. *steganos* meaning "covered or protected" and *graphein* which means "writing". Therefore, steganography is the science of hiding secret messages inside a file image, audio or video so that the transmitted message is invisible or indiscernible. Basically the key concept is that transmitted message should not be detectable to the casual eye. This differs from cryptography which means "secret writing". Cryptography is the study of methods of sending messages in distinct form so that only the intended recipients can remove the disguise and read the message. The message we want to send is called plain text and disguised message is called cipher text. The process of converting a plain text toa cipher text is called enciphering or encryption, and the reverse process is called deciphering or decryption. Encryption protects contents during the transmission of the data from the sender to receiver. However, after receipt and subsequent decryption, the data is no longer protected and is clear. Steganography hides messages in plain sight rather than encrypting the message, it is embedded in the data (that has to be protected)and doesn't require secret transmission. The message is carried inside data. Steganography is therefore broader than cryptography.

Steganography equation is 'Stego-medium = Cover medium + Stego key + Secret messsage'. The cover medium is the data that is visible to the world. Secret message is the embedding data that needs to be hidden which is sent secretly and stego key includes both cover and the embedded data. A stego-key is used to control the hiding process so as to restrict detection and /or recovery of the embedded data to parties who know it [1].

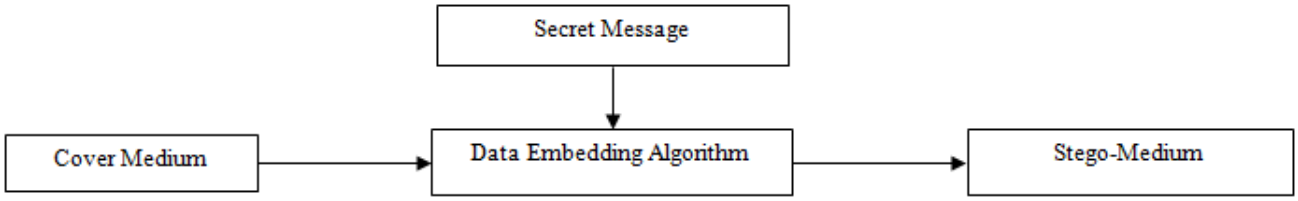

Fig. 1 Steganography Process

II. CHARACTERIZATION OF STEGANOGRAPHY SYSTEMS

There are various features that characterize the strength and weaknesses of the steganography techniques. The relative importance of each feature depends on the application [2],[3].

1. **Capacity** :In data hiding capacity relates to the total number of bits that can be hidden and then successfully recovered by the Stego system.
2. **Robustness:** Robustness is the ability of hidden embedded data to remain unchanged even if the stego-system undergoes any kind of transformation like addition of random noise, scaling, linear and non-linear filtering, rotation etc.[4].
3. **Undetectable:**The embedded algorithm used to embed secret message should be undetectable. It is undetectable if the stego image is consistent with a model of source from which images are drawn. For example, if a method uses the noise component of images for embedding, it should do so while maintaining statistical properties i.e. not making any changes to the noise in the carrier. The size of the secret message and the format of the content of the cover image directly affects undetectability [3].

4. **Invisibility** (Perceptual Transparency)**:**Basically this is based on the ability of the human visual or audio system. The embedded information is considered to be imperceptible if human beings can't distinguish between stego image and the cover image which do not contain hidden information. Data should be embedded without causing any significant degradation to the perceptual quality of the cover.
5. **Security:** The embedding algorithm is considered to be secure if the hidden message can't be removed even after being detected by the attacker.

III. CLASSIFICATION OF STEGANOGRAPHY TECHNIQUES

Steganography techniques are classified into six categories according to the cover modifications applied in the embedding process. Figure below presents this classification

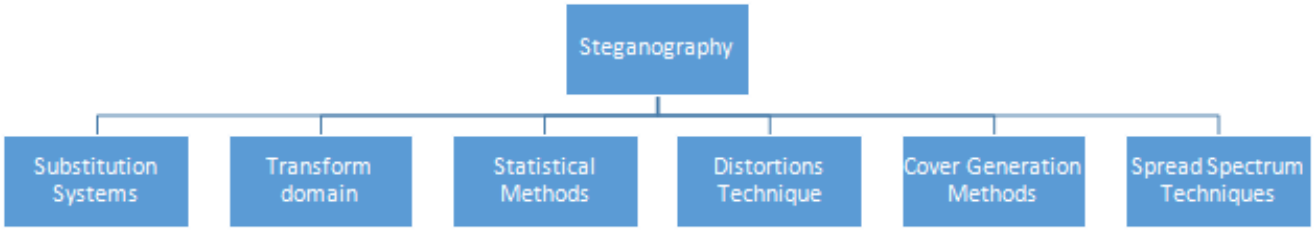

Fig. 2 Steganography Classification

1. Substitution System

In substitution techniques, redundant parts of the cover are identified and then substituted with the secret message i.e. insignificant parts of the cover are substituted with secret message bits. The redundant bits are those which can be altered in cover object without alterations being detected easily. The receiver then extracts information based on the knowledge of the points where the information is embedded. Since, no major modifications are done during the embedding process, the sender can possibly assume that hidden information will not be noticed by the passive intruder. There are various techniques which come under this category and are discussed in detail in the following subsections

1.1 Least Significant Bit Substitution (LSB)

This technique involves modification of least significant bits layer of an image. This technique is based on the fact that the least significant bits of an image can be assumed to be as noise and changing them would not have any effect on the image [5]. In this technique, the least significant bits of pixels are substituted or replaced by the message that needs to be sent. The message bits are distributed evenly through permutation before embedding, thus on average only half of the LSB's are modified. There are various steganographic tools available which are based on LSB embedding, each vary in its approach for hiding information. Some algorithms modify pixels in specific areas or some change LSB of pixels randomly, or some instead of changing the last bit they just increment or decrement the pixel value [9].

1.2 Image Downgrading and Cover Channels

This is the special type of substitution method in which image acts as both cover and secret message. Assuming equal dimension of both cover image and secret image, the sender replaces the four LSB's of cover's grayscale value with four most significant bits of the secret image. The receiver then extracts the four LSB of the stego image thereby retrieving the most significant bits of the secret image. Any degradation to the cover image is not visually noticeable, these 4 bits give rough approximation of the secret image.

1.3 Pseudorandom Permutation

This techniques involves embedding of secret bits inside the whole cover randomly i.e. the secret message bits are distributed randomly across the whole cover which increases the complexity for an intruder/attacker since there is no guarantee that the subsequent message bits are embedded in the same order. The major problem with this technique is the amount of additive noise in the image which affects the statistical properties as well as signal to noise ratio of an image.

1.4 Palette-based images

A palette-based image format has two parts : a palette which specifies N colors as a list of indexed pairs (i, c_i) i.e. every index i is assigned color vector c_i ,and the image data which assign palette index to every pixel. So, there are two ways for embedding data inside a palette based image: either the image data or palette can be manipulated. The LSB of color vectors can be substituted by secret message bits for information transfer. Alternatively, the way the colors are stored in palette, information can be encoded accordingly. There is enough capacity to embed a small message since there are N! ways to sort a palette. However, these methods which utilize the order of palette for embedding information, are not robust as the attacker can sort the entries and destroy the secret message completely.

2. Transform Domain Methods

This technique is one of the complex technique of hiding secret message inside an image. There are various algorithms and transformation which are applied on an image in order to hide message or information inside it. Transform domain methods are more robust to attacks, such as cropping, compression or some image processing, than the LSB approach as they hide information in significant areas of the cover image. This technique is mainly used to provide high security and in cases where large amount of information needs to be hidden. However, a trade-off exist between the amount of information hidden inside the image and the robustness achieved. Many of the transform domain methods are independent of the image format and may survive lossy and lossless format conversions. Variations of this technique are:

a) Discrete cosine transformation technique (DCT)
b) Discrete Fourier transformation technique (DFT).
c) Discrete Wavelet transformation technique (DWT).

3. Statistical Methods

Statistical steganography techniques embed one bit of information in a digital carrier i.e. they utilize "1-bit" steganographic schemes. This is done through alteration of cover in a way that some statistical characteristics of cover change significantly when "1" is transmitted. Otherwise the cover remains unchanged. So the receiver is able to distinguish between modified and unmodified covers. In the embedding process, cover is divided into say m disjoint blocks. If the secret bit is 1 then "1" placed into i^{th}block otherwise the block is not changed [1]. A hypothesis-testing function is then used to detect a specific bit which distinguishes modified blocks from the unmodified ones.

4. Distortions Technique

In this technique the intended recipient requires the knowledge of original cover in order to complete the decoding process which is in contrast to the substitution systems. The sender during the encoding process applies a sequence of various modifications to the original cover image which corresponds to the specific message to be transmitted. The stego image is created by applying these modifications which is transmitted to the intended receiver.So, information is described as being stored by signal distortion [8]. This sequence of modifications is then used to match the secret message which needs to be transmitted. The decoder/receiver then checks for the differences between the stego image and original cover image in order to extract the secret message. The early text based information hiding methods are of distortion type i.e. the layout of a document or arrangement of words may reveal the hidden information.

The secret message is encoded at pseudo-randomly chosen pixels. At the given message pixel, the stego image and cover image is compared and if they are different, the message bit is a "1" otherwise it is "0". The encoder then can modify the "1" value pixels while maintaining the statistical properties of the image. However, benefits of this techniques are limited by the need for sending original cover image.

5. Cover Generation Methods

The cover generation techniques generate a digital object i.e. a cover which serves the purpose of being a cover for secret transmission. This is in contrast to other steganography methods in which the secret message is added to a specific cover by applying an embedding algorithm. In this era of internet, it can be assumed that it is almost impossible for a human being to monitor and observe all the communications around the world. Therefore, today importance is being given to automated supervision systems which are capable of doing this task. These systems examines keywords and statistical profile of a message in order to check a communication. Mimic functions can be used to change the statistical profile of a message which hide its identity in such a way that it matches the profile of an innocent looking text. There are various statistical properties possessed by English language. For instance, distribution of characters across the language is not uniform say *e* occurs more frequently than *z*. This fact has been exploited in various data compression schemes such as Huffman Coding. Using Huffman compression functions, a mimic function can be constructed but these functions can only fool machines. To a human observer, this created text seems to be meaningless as it is full of typographical and grammatical errors.To overcome these limitations mimicry has been enhanced by the application of context free grammars. Context Free Grammars explain the rules of constructing sentences in languages from different parts of speech. Context Free Grammar can be used to create grammatically correct English text to hide messages. Spam mimic provides a good example of a cover generation method.

6. Spread Spectrum Technique

Spread spectrum (SS) is a form of radio frequency communication in which data sent is spread over wide frequency range intentionally. These techniques can be considered as means of transmission in which signal occupies excessive bandwidth (more than the minimum bandwidth required for transmission of data) and this band spread is achieved through code independent of data and a synchronized reception by the receiver's code which is used for dispreading and recovery of data. The main advantage of Spread Spectrum is that it makes itdifficult to detect the signal and jam which makes it ideal for hiding information. Another benefit is that it is resistant to external noise and interference thereby increasing the probability that signal will be received correctly by the receiver. Another advantage is that signals are unlikely to interfere with each other even if they are transmitted on the same frequency. Spread Spectrum techniques are of increasing importance in the field of steganography [6]. There are three variants of SS techniques:

a) Direct Sequence Spread Spectrum

In this technique data which needs to be transmitted is divided into small chunks and each piece of data is allocated to a frequency channel across the spectrum. The sender utilizes phase modulation scheme to modulate each chunk with higher data bit rate called chip rate and then added to the cover.

b) FrequencyHoppedSpreadSpectrum

In this technique, the frequency of the carrier signal is periodically modified or hopped rapidly from one frequency to another across a specific range of frequencies.The frequencies, across which the carrier jumps is the spreading code. The shifting pattern is determined by the chosen code sequence (frequency shift key – FSK). The amount of time spent on each hop is known as the dwell time and is in the range of 3ms-100ms [7]. There are two variants of frequency Hopped SS: slow hopping and fast hopping each with its own advantages and disadvantages.

c) Time Hopped Spread Spectrum

In Time Hopped Spread Spectrum technique, a short information burst (or chirp) is transmitted either in random positions or with pseudorandom pulse duration. It can be implemented in two ways i.e. in the first technique PN generator determines the actual interval in which chirp is transmitted. This ensures that any intruder intercepting the signal remains uncertain about the when the next pulse will be transmitted. In the second technique, each chirp starts at the same time in each bit period but their duration is different which is altered by PN code generator.

IV. CONCLUSION

In the past few years, steganography techniques have gained lot of attention due to increasing need for secured transmission. In this paper, an overview of various steganographic techniques proposed during last few years was presented. Many flexible, secured and simple techniques exist for embedding information in various digital media without getting detected by attackers. These techniques leave some sort of "fingerprint" in the data. Each technique with its own characteristics have been discussed in this paper.

REFERENCES

[1] Ross J.Anderson ,Fabien A.P.Petitcolas, and Markus G.Kuhn, (1999) "Information Hiding – A Survey", Proceedings of the IEEE, special issue on protection of multimedia content, pp.1062-1078.

[2] Hameed, B.B.Zaidan, Wajdi F. Al-Khateeb, A.W. Naji, Shihab A. Othman O. Khalifa, A.A.Zaidan and Teddy S. Gunawan, " Novel Framework for Hidden Data in the Image Page within Executable File Using Computation between Advance Encryption Standared and Distortion Techniques", International Journal of Computer Science and Information Security (IJCSIS), Vol. 3, No 1 ISSN: 1947-5500, P.P 73-78,3 Aug 2009, USA

[3] Hamid.A.Jalab, A.A Zaidan, B.B Zaidan, "New Design for Information Hiding with in Steganography Using Distortion Techniques", International Journal of Engineering and Technology (IJET)), ol 2, No. 1, ISSN: 1793-8236, Feb (2010), Singapore.

[4] Mahmoud Elnajjar, A.A Zaidan, B.B Zaidan, Mohamed Elhadi M.Sharif and Hamdan.O.Alanazi ," Optimization Digital Image Watermarking Technique for Patent Protection", Journal of Computing (JOC), Vol.2, Issue 2, ISSN: 2151-9617, P.P 142-148 February 2010, Lille, France.

[5] Kharrazi, M., Sencar, H. T. and Memon, N. (2004), "Image Steganography: Concepts and Practice", WSPC/Lecture Notes Series: 9in x 6in, pp.1-31

[6] Tirkel, A.Z., G. A. Rankin and R. van Schyndel, "Electronic Watermark", in Dgital Image Computing, Technology and Applications – DICTA 93, Macquarie University, 1993, pp. 666-673

[7] Sorin M. Schwartz, Frequency Hopping Spread Spectrum (FHSS) vs. Direct Sequence Spread Spectrum (DSSS) in Broadband Wireless Access (BWA) and Wireless LAN (WLAN), Alvarion Professional Education Center (ALPEC), version 7, December 2001

[8] H. S. Majunatha Reddy and K. B. Raja, (2009) High capacity and security steganography using discrete wavelet transform. International Journal of Computer Science and Security. pp. 462-472.

[9] T. Sharp, "Hide 2.1, 2001," http://www.sharpthoughts.org

