A Short Survey on Steganography

[1]Manoj Kumar, [2]Anuj Rani
[1]ITB Blanchardstown, Dublin, Ireland
[2]ITM University, Gurgaon, Haryana, India

Abstract
Steganography is an art of hiding information in innocuous looking cover objects. The main goal of steganography is to avoid drawing intuition about transmission of message. The terms 'Steganography' and 'Steganalysis' are used in information hiding process. Steganography basically deals with hiding information in digital media while steganalysis is the method of detecting the presence of hidden message in it. The term 'Steganography' is often confused with 'Cryptography' which converts message into indecipherable form. Progress made in the field of steganography in terms of using different multimedia files such as images, audio, video, text files as cover objects for hiding information is attracting more people to work in this area.

Keywords
Steganography, Steganalysis Covert Communication, Image Steganography, Video Steganography, Audio Steganography, Protocol Steganography, Text steganography

I. Introduction

Steganography is a science that deals with covert communication [1]. This is done by hiding the message into some other media such as images, audio, video, text files. The word steganography is a combination of two words taken from Greek language; 'steganos' which means 'covered' and 'graphie' which means 'writing'. Thus, steganography means 'covered writing' or 'hidden writing'. Both steganography and cryptography are used to provide secure communication but steganography has an advantage over cryptography. In steganography, the hidden message does not get attraction of the intruder while in cryptography, intruder easily gets clue about the secret information. In steganography, the 'carrier-object 'contains the Hidden message known as 'stego-object' using some 'stego-key' which provides more security. It can be represented as: Carrier-object + hidden message + stego-key = stego-object [15].

The use of steganography originated in 440BC, when Demeratus sent a warning message about a next coming attack to Greece by writing it on a wooden block and covering it with wax. Histiaeus used another technique different from the one used by Demeratus in which he got the head of his most trusted slave shaved and tattooed a message on it. After his hair had grown the message was hidden. The purpose was to incite a revolt against the Persians. In the first and second world wars, German spies used invisible ink to print small microdots on letters [11]. Microdots are blocks of text or images that scale down the size of regular dot. To make the communication systems more secure both the steganography and cryptography were used collectively [11].

Various techniques and methods are discussed in literature for implementing steganography. These methods can either be implemented independently or in combination with each other. Steganographic techniques are basically classified into the six categories viz. substitution systems, transform domain methods, spread spectrum technique, distortion methods, statistical methods and cover generation techniques. Broadly, steganography is divided into two parts: technical steganography and linguistic steganography [17] as discussed below.

Technical steganography deals with spatial domain (image domain) and transform domain (frequency domain). In image domain, substitution of LSB by using bitwise methods has been attempted since human eyes cannot identify very small disturbance in LSB values. LSB substitution method has a limitation that the carrier-object can hide only limited information; hence when hidden information is large it is perceptible [6]. After information is embedded to the carrier-object its size increases hence compression techniques can be applied in order to reduce the size of the carrier-object. Type of the compression technique (lossless or lossy) used depends upon the file format. Lossless compression technique is mostly adopted for Windows Bitmap (BMP) and Graphics Interchange Format (GIF) with LSB substitution method while lossy compression technique is used for Joint Photographic Expert Group (JPEG) [6]. JPEG file format uses DCT (Discrete Cosine Transform) to hide the information in transform domain for the purpose of compression. Data hiding process in transform domain also uses the DFT (Discrete Fourier Transform) and DWT (Discrete Wavelet Transform) [18]. JPEG images are mostly used in communication over internet because of their better picture quality [15]. Image, audio, video, protocol and text steganography comes under the broad category of technical steganography.

Linguistic steganography uses substitution and statistical methods to hide information. In linguistic steganography, different type of symbols and unknown language is used which only certain group of people knows [17]. Linguistic steganography specially deals with hiding information in text.

Rest of the paper is organized as follows. Section II, discusses different types of techniques used for image steganography; Section III, gives a detailed description on audio steganography techniques; Section IV, gives detail on the techniques used for video steganography; Section V, discusses protocol steganography techniques; Section VI, gives an overview of techniques used for text steganography and finally Section VII, gives concluding remarks.

II. Image Steganography

For the purpose of hiding information multimedia files are mainly used as a carrier-object. Most frequently used multimedia files for data hiding are images. An image is nothing but collection of pixels where each pixel is a combination of three colors RGB (red, green and blue). The color of pixel dependent on the numeric value of associated with each color. Pixels in the image are displayed row by row horizontally. When information is hidden in the images, carrier image get less disturbed as compared to other multimedia files. Carrier image contains noise which is used by image steganography for hiding message.

Number of bits used to represent the color in a particular pixel is called bit-depth. Mainly 8-bits are used to represent pixel color [11]. Bit-depth of the gray-scale image is 8-bits that can formulate 256 different colors and bit-depth of digital images is 24-bits i.e. true color image uses the 24 bits to represent each pixel in an image. True color uses the RGB (red, green and blue) color model, that is, each color can represent 256 different shades. By using different color combinations around 16-million colors [11] can be represented.

After hiding information in an image, size of the image increases so compression techniques are required. When information is hidden in large size image, the transmission of image over the network takes more time and requires higher bandwidth. The size of the image can be reduced by compression technique. Compression techniques are grouped into two types, lossy and lossless. A number of methods for hiding information in an image [1] are discussed below.

- LSB substitution (least significant bit substitution)
- Masking and filtering
- Algorithms and transformations
- Encryption and scatter
- Redundant pattern encoding

A. LSB Substitution (Least Significant Bit Substitution)

Least significant bit substitution is a very common approach to hide the information in a carrier-object. In LSB method, the least significant bit of some bytes of image is modified according to the message bits. Human eye is not able to find little variations in the original image. Consider first three pixels of an image to be used as:

00101101 11010000 10110001
11011000 00101101 11100101
00010111 11010001 10011011

In order to hide an image inside the cover image, let the binary value of one pixel of the secret image be 11011001. The resulting pixels of the cover image are as follows:

00101101 11010001 10110000
11011001 00101101 11100100
00010110 11010001 10011011

On an average, only half of the bits have been changed.

B. Masking and Filtering

Masking and filtering are steganography techniques which uses 24-bit image as cover image. Masking technique can be used for both color image and grayscale images. The information is hidden using masking and filtering techniques in the similar way as watermark on a paper [1]. Masking is richer as compared to LSB substitution according to [7] in "seeing the unseen". In masking technique, data is hidden by changing the luminance of pixels of a particular area. Masking and filtering are basically used to provide authentication and copyright protection.

C. Algorithms and Transformations

Algorithms and transformations are the techniques used for hiding data into images. These techniques use some mathematical formula in order to hide the data and later on reduce the file size using compression algorithms. DCT (discrete cosine transforms) is used by JPEG (joint photographic expert group) images for compression. DCT of an image is faster than the other transforms like DWT (discrete wavelet transform) and DFT (discrete Fourier transform). DCT comes under the category of lossy compression because exact cosine values are not calculated [1].

D. Encryption and Scatter

Encryption and scatter technique simulates white noise of an image hence is mainly used with image steganography. White noise is a signal with flat spectral density. Message hiding process is done by scattering the whole message throughout the image on all 8-channels with a random number that is generated by previous data channel [1]. Each channel rotates and swaps with other channels. Single bit is generated as an output from all channels. It is more difficult to detect the messages hidden [1] using this method. In order to randomize data in white noise, encryption technique is also used. For performing encryption and scattering, LSB is extracted from the cover image; secret message is encrypted and applied to LSB of the cover image to create a new LSB. These new LSB's are inserted into the cover image to obtain the stego-image. The limitation of the above method is that it needs large size image to hide the message. Since the method uses white noise for information hiding, it is more secure [1].

E. Redundant Pattern Encoding

Patchwork comes under the statistical technique that uses redundant pattern encoding [11]. It is like a spread spectrum technique which spreads the information throughout the image. In the patchwork, the image is divided into patches. Pseudorandom generator is used to select the two patches for hiding information. Redundant pattern encoding makes this process more robust to cropping and rotation. Hiding smaller image increases redundancy of the cover image. This helps in recovering the secret message in case the stego image is manipulated [1].

III. Audio Steganography

In audio steganography, information is hidden in the sound signals. The secret information is hidden by using various methods like LSB substitution, phase coding, echo hiding and spread spectrum [1]. For hiding information in audio files different files such as WAV (waveform audio format), AU, MP3 [17] are used. Methods used to embed information into the digital signal use properties of Human Auditory System (HAS) [1]. HAS can sense any extra noise or disturbance in the sound file. Sound waves follow the path from outside a listener head, past the pinna and ear canal, into the cochlea, onto the basilar membrane through the inner hair cells along the auditory nerve and finally into the higher processing centers. Techniques that are used for audio steganography are [16] mentioned below.

- LSB substitution
- Spread spectrum
- Phase encoding
- Parity encoding
- Echo hiding

A. LSB Substitution

In LSB substitution, least significant bit of the digital audio signal is replaced with the message bit and this alteration cannot be human predictable. Hiding data at frequencies above 20,000 Hz is not audible to human beings [1]. Replacing two or more than two bits by message bits increases the noise levels in audio signals [1]. For generating the hidden information from audio signal receiver needs to follow the same procedure as used during hiding. LSB coding starts from the beginning of audio file and continue until the whole message is hidden. For providing security to the secret message padding of the secret message with some extra bits is done. Major disadvantage of using LSB method is the sensitivity of human ear to slight variations in different audio signals [1]. LSB coding is easy to implement and has less computational complexity.

B. Spread Spectrum

In audio steganography, simple spread-spectrum is used to spread the information throughout the audio signal. Spread spectrum is a form of radio frequency communication. Unlike LSB coding, spread spectrum technique spreads the information over the

sound file frequency spectrum [1] and makes it difficult to detect the noise. Two different techniques used in spread spectrum are DSSS (Direct Sequence Spread Spectrum) and FHSS (Frequency Hopped Spread Spectrum). In DSSS, data to be transmitted is divided into small chunks and these chunks are allocated to different frequencies in the spectrum. In FHSS, frequencies which are used for data transmission are periodically modified across a specific range of spectrum.

C. Phase Encoding

In phase encoding works on the principle of dividing the cover-object or audio signal into blocks and embedding the message into phase spectrum of the first block. This technique embeds the message into phase spectrum of digital signal rather than introducing the disturbance into the audio signal [1]. Phase encoding follows the procedure [1]

1. Original cover signal is broken into equal size segments that also equals to size of message to be encoded.
2. DFT (discrete Fourier transform) is applied to all segments of the audio signal to create the phase matrix.
3. Insert the secret message into the phase vector of first segment of signal.
4. Calculate the difference between the original signal and signal after inserting the data.
5. Formulate the new matrix on the basis of new phase shift.
6. Using the new phase matrix and original matrix sound signal can be reconstructed by applying the DFT in reverse process and combining the block segments.

D. Parity Encoding

Parity encoding breaks the signal into separate regions instead of breaking it into individual samples. In this method, each bit of message is hidden into parity bit of the sample regions. When parity bit of the sample region is not matched with the message bit, LSB of the sample region flips. By using this process the sender has more choice to encode the message [1].

E. Echo Hiding

In echo hiding, message is embedded in the sound file by introducing an echo into the discrete signal. Three parameters of this artificial echo are used to hide the embedded data. These are delay, decay rate and initial amplitude. When the delay between original sound and echo sound decreases, it becomes hard for human beings to distinguish between the two sounds. It provides high transmission rate like spread spectrum. Only one bit information is encoded into one produced echo. The original signal of sound is first divided into blocks [1]. When encoding process is completed all the blocks are combined back together to make a single signal. In order to decode the stego-signal, receiver first breaks the signal into same blocks sizes used during the encoding process. To extract the message spectrum coefficient is used [1].

IV. Video Steganography

This technique hides information in the video signal. Video files are a combination of images and audio files. As the information in video signal flows continuously, small distortion in the original file might not be observed by humans [17]. For hiding the information into video DCT (discrete cosine transforms) is used. DCT alters the value of certain parts of the image. The main advantage of using video signal is the huge size which can hide large amount of data without noticeable distortions [16]. Video steganography is used to overcome the problem of capacity because it is a collection of images and audio. Any image or audio signal can be used for hiding data.

In the algorithm proposed in [13], video steganography was used to communicate on war so that prisoners can communicate secretly using the video steganography. In [12] a method is proposed to overcome the problem of capacity. The method uses wavelet compression and bit plane compression segmentation steganography. The method proposed in [14] uses video error correction steganography since transmission of data always lead to errors and video transmission handle these errors without resending the data with errors. The method discussed in [4] proposes video steganography using LSB (least significant bit). In this method video is divided into frames of images. The output image is also a collection of all images that are not visually affected. In this method data storage capacity is increased but no more security is provided. The algorithm proposed in [19] discusses a combined approach of steganography and cryptography. For providing security the algorithm in [19] uses the Public Key Infrastructure (PKI) method. For providing data integrity, PKI is used and it also provides high processing as compared to the hash function.

V. Protocol Steganography

Protocol steganography is used by people who want to communicate secretly. In this information hiding is done by the use of networking protocols. Protocol header is used for hiding information. Header of the protocol has some extra fields like options available for hiding information. The term 'protocol steganography' deals with hiding information and transmitting it using network protocol [16]. Protocol steganography maintains the properties of both cover-traffic and cover payloads. In protocol steganography for embedding and extraction of data two different approaches such as conventional embedding process and evolutionary extraction of information have been used.

VI. Text Steganography

In text steganography the information is hidden into the text. Text steganography involves changes in words format and can also use the context-free grammar. Various different methods are used for information hiding in text by modifying LSB of the text file. Sometimes, single sentence is used many times or other symbols may be used [17]. Various techniques are used to modify the layout of text; certain rules are used like using a particular character or altering the white spaces. Another way of hiding text is openly available books, magazines and newspaper etc. that uses the code like page number, line number and particular occurrence of a character [1]. There are many ways to hide the data in text using the linguistic structure of the text for hiding the data. Text steganography is divided into following sub-categories [8]:

- Syntactical steganography
- Lexical steganography
- Ontological steganography
- Other steganographic technique

A. Syntactical Steganography

As the name suggests this type of steganographic technique deals with the syntactic structure of the text. Context free grammar is used to make the sentences syntactically correct. NICETEXT algorithm is used in syntactical steganography in which the cover-object is used as original syntax and using some syntax the algorithm generate some frames [11]. Steganalysis algorithm can be easily developed for detecting the presence of hidden information [8].

B. Lexical Steganography

In the lexical steganography, text or words are used to hide data. In this technique, words can be replaced by their synonyms or other words whose meaning is approximately same as the original word [8].

C. Ontological Steganography

In this technique for embedding information an explicit model is used to check the equivalence of text instead of using only the synonyms of the words. It sometimes produces incorrect words like NICETEXT algorithm [8].

D. Other Steganographic Technique

In [10], another technique for hiding data in specific characters of the different words is proposed. In [2, 9], concept of line shifting steganography is proposed where line is shifted vertically to some specified angle. In [3], a method for hiding data into random characters and words is proposed. In [5], the proposed algorithm hides information by adding some white space in the text.

VII. Conclusion

This paper gives state-of-art review on various steganographic techniques by providing a detailed study on steganography. Steganography can be provided at different levels of privacy for communication. Steganography is also used in law firms to collect evidences against illegal objects. Secrecy of steganographic algorithm depends on selecting proper mechanism. Various steganographic tools have been developed for each type of steganography. For the detection of hidden information, many steganalysis tools have been developed. Specialist of computers, researchers and information security professional pay more attention to the field of information hiding rather than on developing steganalyzers.

References

[1] Adhiya K.P., Patil S.A.,"Hiding Text in Audio Using LSB Based Steganography", Information and Knowledge Management, Vol. 2, No. 3, pp. 8-15, 2012.

[2] Alatter A.M., Alatter O.M.,"Watermarking electronic text documents containing justified paragraphs and irregular line spacing", Proceedings of SPIE--Vol. 5306, Security, Steganography, and Watermarking of Multimedia Contents VI, June 2004, pp. 685-695, 2004.

[3] Bennett K.,"Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text", TechnicalReportTR2004-13, Purdue CERIAS, May 2004.

[4] Eltahir, M.E., Kiah M.L.M., Zaidan B.B., Zaidan A.A.,"High rate video streaming steganography", International Conference on Information Management and Engineering, ICIME '09, pp. 550 - 553, 2009.

[5] Huang D., Yan H.,"Interword Distance Changes Represented by Sine Waves for Watermarking Text Images", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 11, No. 12, pp. 1237-1245, 2001.

[6] Ibrahim A.,"Steganalysis in Computer Forensics", Australian Digital Forensics Conference, 2007.

[7] Johnson, N. F., Jajodia, S.,"Exploring steganography: Seeing the unseen", Computer, Vol. 3, No. 2, pp. 26–34, 1998.

[8]. Li B., He J., Huang J., Shi Y.Q. (2011), "A Survey on Image Steganography and Steganalysis", Journal of Information Hiding and Multimedia Signal Processing, Vol. 2, No. 2, pp. 142-172.

[9] Low S.H., Maxemchuk N.F., Brassil J.T., Gorman' O, "Document marking and identification using both line and word shifting", Proc. Infocom'95, Boston, MA, Apr.1995, pp. 853-860, 1995.

[10] Moerland T.(2003),"Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, http://www.liacs.nl/home/tmoerl/privtech.pdf.

[11] Morkel T., Eloff J.H.P., Olivier M.S.,"An overview of image steganography", Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria, South Africa.

[12] Noda, Furuta T., Niimi M., Kawaguchi E.,"Application of BPCS steganography to wavelet compressed video", International Conference on Image Processing: (ICIP, 2004), IEEE, Singapore, pp. 2147-2150, 2004.

[13] Petitcolas F.A.P., Anderson R. J., Kuhn M. G., "Information Hiding- A Survey", Proc. of the IEEE special issue on protection of multimedia content, Vol. 87, No. 7, pp. 1062–1078, 1999.

[14] Robie, D.L., Messereau R.M.," Video error correction using steganography", Proc. of International Conference on Image Processing, Vol. 1, pp. 930 – 933, 2001.

[15] Richer, P.,"Steganalysis: Detecting hidden information with computer forensic analysis", SANS/GIAC Practical Assignment for GSEC Certification, SANS Institute, pp. 1-11, 2003.

[16] Sharma V.K., Shrivastava V.,"A steganography algorithm for hiding image in image by improved LBS substitution by minimize detection", Journal of Theoretical and Applied Information Technology, Vol. 36, No. 1, pp. 1-8, 2012.

[17] Singh N., Bhati B.S., Raw R.S.,"Digital image Steganalysis for computer forensic investigation", Computer Science and Information Technology (CSIT), pp. 161-168, 2012.

[18] Wang H., Wang S.,"Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM-Voting Systems, Vol. 47, No. 10, pp. 76-82, 2004.

[19] Zaidan, A., B. Zaidan,"Novel approach for high secure data hidden in MPEG video using public key infrastructure", International Journal of Computer and Network Security, Vol. 1, No. 1, pp. 71-76, 2009.

[20] P. E. Debevec, J. Malik,"Recovering high dynamic range radiance maps from photographs", in Proceedings of SIGGRAPH, 1997, pp. 369-378, 2009.

[21] G. Piella,"A general framework for multi-resolution image fusion: from pixels to regions", Information Fusion, Vol. 4, 2003, pp. 259-280.

Manoj kumar received his B.Tech. From kurukshetra university in 2008. He worked as a BTS engineer for two years in corporate sector. He completed his M.Tech. From ITM University. He is now pursuing Master of Science in computing from ITB, Dublin, Ireland. His area of research is information security and digital forensics. He is now working on Rule Based Machine Translation.

Anuj Rani is doing M.Tech. (Computer Science) from ITMU (Institute of Technology and Management University), Gurgaon, India. Her interest areas include data mining.