Overview Of Techniques Of Stegnography On Various Media

Ms. Arpana Chaturvedi, , Jagannath International Management School, Vasant Kunj,
Email: pcord.bca@jagannath.org
Ms.Poonam Verma, Jagannath International Management School, Kalkaji
Email:newjimsgn@gmail.com

Abstract

The need of the hour is to maintain secret in the transactions of the e-commerce. The number of people buying and selling business transactions on Web is increasing at a phenomenal pace, which requires the special form of security to be added. The security of common public key was based on the Non polynomial complete problems. Those problems that are not assured to be solved by any universal machine. The steganography is the art of concealing the existence of information and it combines both the networking protocols use and security protocols.

The word steganography, derived from the Greek language, literally means covered writing. This concept includes a high volume of methods of secret communication that hides the very existence of the message. Steganography is the technique of taking one piece of information and hiding it within another. Computer files, whether they are images, sound recordings, text and word processing files, or even the medium of the disk itself, all contain unused areas where data can be stored. The files can then be exchanged with no indication of the additional information that is stored within.

Keywords: *Text Steganography, Image steganography, Audio Steganography and Video Steganography*

1. Introduction:

Steganography is used to conceal information that needs to be protected from the unauthorized users. Various techniques were developed, prior to the development of steganography, where the secret message was written in invisible ink so that actual message remains hidden from the unauthorized users.[2] Steganography is basically classified into fragile and robust where each one has its own features. Fragile steganography file is a file where the secret message gets destroyed in case the file is modified however robust steganography, the information is difficult to implement and not easily destroyed.

Steganography in the earlier times were implemented on the text, however in the recent times, this has propagated to various medias. In this era of booming e-commerce , there is dire need of use of multimedia data, digital signature authentication and validation of electronic documents, digital data storage and linkage for binding of digital images with personal attribute information. Steganography is required to be implemented for secure communication of the data.

2. Multimedia:

A lot of research has been carried out on the formats of the multimedia and one of the commonly used file formats by people, hiding data in images, text and audio has been very significantly carried out[5] and some of the popular multimedia tools are as follows:

1. Blindside is a BMP Stego optional encryption where the Blindside analyses the colour differentials in the image, and will only alter pixels that it knows will not be noticeable to the human eye.
2. Cameleon is a GIF based Stego with a novel adaptive encoding algorithm for 24-bit true-color images.
3. Camouflage is a program that permits to hide the files by scrambling them and behaves like a normal file.
4. *Gifshuffle* hides data in GIF's by shuffling color map. *Gifshuffle* is a command-line-only program for windows which conceals messages in GIF images by shuffling the color-map. The picture remains visibly intact, only the order of color within the palette is changed.

3)Graphics Steganography:

Various techniques are used on the graphics and these techniques can be majorily classified into four techniques:

3.1) Spatial Domain
3.2) Transform Domain
3.3) Distortion Technique
3.4) Masking and Filtering

Each of these technique use various techniques and they can be listed as below:

3.1) Spatial Domain Technique:

1. Least significant bit (LSB) :
   Embedding into the Least Significant bit allows to change the color value by one. In case the bit is embedded into the third bit plane can change the color value by 3.
2. Pixel value differencing (PVD):
   It uses the difference between the two consecutive located bits available from two non overlapping blocks and the quantization table used has a range value of 0 to 255.
3. Edges based data embedding method (EBE) :
   All the edge pixels in the image are used to hide the data in the least significant bits.
4. Random pixel embedding method (RPE)
   The hidden message is embedded randomly on any selected pixel. The random generator is based on the Fibonacci algorithm.
5. Mapping pixel to hidden data method :
   The message is hidden embedding pixels using some mathematical function and then it finds the 8 neighborhood of the each selected pixel and map each two bit of the secret message in each of the neighbor pixel according to the features of that pixel in a specified manner.[6]
6. Labeling or connectivity method :

Connectivity defines how many pixels are connected to the other pixels. There are basically two connectivity modes and they are 4-connected and 8-connected. The dark region of an image is selected and the data is hidden in the least 8 bits of that region.

7. Pixel intensity based method :

   All the three color planes are converted into the binary values. The plane having the least number of ones in the Most Significant Bit is considered to be the index plane whereas the other two are considered to be the data planes.[7] Depending on the number of ones in the MSB, the bits in the data plane is embedded.[10]

8. Histogram shifting methods:

   Histogram is constructed using the host image histogram.

3.2) Transform Domain Technique:

1.Discrete Fourier transformation technique (DFT).
2. Discrete cosine transformation technique (DCT).
3. Discrete Wavelet transformation technique (DWT).
4. Lossless or reversible method (DCT)
5. Embedding in coefficient bits

3.3) Distortion Technique

In distortion techniques the information is stored by signal distortion. These techniques require the knowledge of the original cover image during the decoding process. The encoder applies series of modifications to the cover image and the decoder functions to check for the various differences between the original cover image and distorted cover image to recover the secret message.

3.4) Masking and Filtering:

This technique is usually applied on 24 bits or grayscale images, uses a different approach to hiding a message. It hides information by marking an image, similar to paper watermarks. This technique actually extends an image data by masking the secret data over the original data as opposed to hiding information inside of the data. These techniques embed the information in the more significant areas of the image than just hiding it into noise level. Watermarking techniques can be applied on the image without the fear of its destruction due to lossy compression as they are more integrated into the image

4) Text

- Text is hidden in the characters of the words, which requires large amount of plain text.
- HTML tags are not case sensitive, hence the data can be easily embedded into the tags of a webpage.
- The characters can be hidden using whitespaces. Less number of whitespaces may specify a 0 and more number of whitespaces between words may determine.
- Semantic Hiding: Uses synonyms to hide the message.

5) Video

There are various techniques of video steganography. The best technique is to hide the secret data without reducing the quality of the cover video, so that it cannot be detected by naked eyes. The embedded video is known as the “stego” video which is sent to the receiver side by the sender.

5.1) LSB (Least Significant Bit) method
5.2) Non-uniform rectangular partition
5.3) Compressed video steganography
5.4) Anti-forensics technique
5.5) Masking and filtering

5.1)LSB (Least Significant Bit) method:

LSB is one of the most effective method of embedding data. The pixel values of the cover video are extracted in bytes and the LSB are substitutes by the bits of the secret message that will be embedded.[3] As the LSB bits are only changed, thus no distortion occurs and hence the video appears to be original video.[1]

5.2) Non-uniform rectangular partition :

This method is used for only the uncompressed videos. In non-uniform rectangular partition, data hiding is done by hiding an uncompressed secret video file in the host video stream. The main criteria is that the cover file and the secret file should be of equal size. Each of the frames of both the secret as well as cover videos is applied with image steganography with some technique. The secret video file will be hidden in the leftmost four least significant bits of the frames of the host video.

5.3)Compressed video steganography:

This method is done entirely on the compressed domain. Data can be embedded in the block of I frame with maximum scene change and in P and B block with maximum magnitude of motion vectors. The AVC encoding technique yields the maximum compressing efficiency.

5.4)Anti-forensics technique:

Anti-forensic techniques are actions taken to destroy, hide and/or manipulate the data to attack the computer forensics. Anti-forensic provides security by preventing unauthorized access, but can also be used for criminal use also. Steganography is a kind of anti- forensic where we try to hide data under some host file. Steganography along with anti- forensics makes the system more secure.

5.5) Masking and filtering ;

Masking and filtering are used on 24 bits/pixel images and are applicable for both colored and gray scale images. It is like watermarking over an image and doesn’t affect the quality of that image. Unlike other steganography techniques, in data masking the secret message is so processed such that it appears similar to a multimedia file. Data masking cannot easily be detected by traditional steganalysis.

Conclusion:

This paper gave an insight to the recent researches taking place in the field of information security. In the next paper, we would propose to optimize the video steganography techniques.

References:

[1] Yang, Chunfang., Liu, Fenlin., Luo, Xiangyang., and Zeng, Ying., "Pixel Group Trace Model-Based Quantitative Steganalysis for Multiple Least-Significant Bits Steganography", IEEE Transactions on Information Forensics and Security, Vol. 8, No. 1, January 2013.

[2] Swati malik, Ajit "Securing Data by Using Cryptography with Steganography" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013

[3] Ishwarjot Singh „J.P Raina,“ Advance Scheme for Secret Data Hiding System using Hop field & LSB" International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 7–July 2013.

[4] Shabir A. Parah, Javaid A. Sheikh, G.M. Bhat, "Data Hiding in Intermediate Significant Bit Planes, A High Capacity Blind Steganographic Technique", International Conference on Emerging Trends in Science, Engineering and Technology , pp.192-197, July 2012.

[5] Michel K. Kulhandjian, Dimitris A. Pados, Ming Li, Stella N. Batalama, and Michael J. Medley, "Extracting spread-spectrum hidden data from digital media ", IEEE transactions on information forensics and security, vol. 8, no. 7, july 2013.

[6] Chang, Chin-Chen., Lin, Iuan-Chang., and Yaun-Hui YU., " A new Steganographic method for color and gray scale image hiding", Computer Vision and Image Understanding, ELSEVIER, Vol. 107, No. 3, pp. 183-194,2007.

[7] Adnan Gutub, Ayed Al-Qahtani, Abdulaziz Tabakh, "Triple-A: Secure RGB Image Steganography Based on Randomization", International Conference on Computer Systems and Applications (AICCSA-2009), pp: 400-403, 10-13 May 2009.

[8]digsteganography.blogspot.com/2009/09/ digital-steganography.htmlNetwork Security: Digital Steganography

[9] Digital Steganography for Information Security Anthony T.S. Ho, Siu-Chung Tam, Siong-Chai Tan and Lian-Teck Yap Kok-Beng Neo and Sim-Peng Thia DataMark Technologies, Singapore

[10] Efficient Method For Hiding Data By Pixel Intensity, M.Shobana et al. / International Journal of Engineering and Technology (IJET)