Steganography Techniques for Hiding Text

Ritu verma[1], Anju Vishwakarma[2], Rupendra Sahu[3]

[1]Parthivi College of Engineering and Management, Sirsakala bhilai-3
Dist- Durg, Pin code – 490021
rituverma87.pcem[at]gmail.com

[2]Parthivi College of Engineering and Management, Sirsakala bhilai-3
Dist- Durg, Pin code – 490021
anjuvish1405[at]gmail.com

[3]Parthivi College of Engineering and Management, Sirsakala bhilai-3
Dist- Durg, Pin code - 490025
rupendrasahu012[at]gmail.com

Abstract: ***Steganography is the art and science of hiding information by embedding it in some other data. Here we are using image as a means for covering information. Steganography conceals the fact that a message is being sent. It is a method to covert channels, spread spectrum communication and invisible inks which adds another step in security. A message in ciphertext may arouse suspicion while an invisible message will not. This paper introduces steganography by explaining what it is, providing a brief history with illustrations of some methods for implementing steganography, and comparing available software providing steganographic services. Though the forms are many, the focus of the software evaluation in this paper is on the use of images in steganography.***

Keywords: Steganography, cipher text, Encryption, Decryption

1. Introduction

The word steganography literally means *covered writing* as derived from Greek. It includes a vast array of methods of secret communications that conceal the very existence of the message. Among these methods are invisible inks, microdots, character arrangement (other than the cryptographic methods of permutation and substitution), digital signatures, covert channels and spread-spectrum communications. Steganography is the art of concealing the existence of information within seemingly innocuous carriers. Steganography has been exploited throughout history by individuals, military, secret intelligence, and governments to stealthily communicate and transmit information without drawing any attraction. It has numerous applications which range from secret communication, to digital watermarking, data integrity, copyright protection, and data tampering. The motivation behind developing image Steganography methods according to its use in various organizations to communicate between its members as well as, it can be used for communication between members of the military orintelligence operatives or agents of companies to hide secret messages or in the field of espionage. The main goal of using the Steganography is to avoid drawing attention to the transmission of hidden information.

2. Types of Steganography

[1]. ***Text Steganography*:** It consists of hiding information inside the text files. In this method, the secret data is hidden behind every nth letter of every words of text message. Numbers of methods are available for hiding data in text file. These methods are
i) Format Based Method ii) Random and Statistical Method iii) Linguistics Method.

[2]. **Image Steganography**: Hiding the data by taking the cover object as image is referred as image steganography. In image steganography pixel intensities are used to hide the data. In digital steganography, images are widely used cover source because there are number of bits presents in digital representation of an image.

[3]. **Audio Steganography:** It involves hiding data in audio files. This method hides the data in WAV, AU and MP3 sound files. There are different methods of audio steganography. These methods are i) Low Bit Encoding ii) Phase Coding iii) Spread Spectrum.

[4]. **Video Steganography:** It is a technique of hiding any kind of files or data into digital video format. In this case video (combination of pictures) is used as carrier for hiding the data. Generally discrete cosine transform (DCT) alter the values (e.g., 8.667 to 9) which is used to hide the data in each of the images in the video, which is unnoticeable by the human eye. H.264, Mp4, MPEG, AVI are the formats used by video steganography.

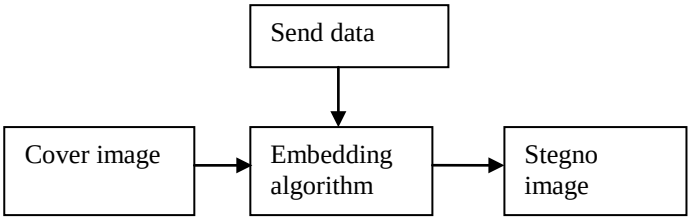

Figure1 : Steganography

3. Steganography Techniques

1. Spatial Domain Methods: In this method the secret data is embedded directly in the intensity of pixels. It means some

pixel values of the image are changed directly during hiding data. Spatial domain techniques are classified into following categories: i)Least significant bit (LSB) ii) Pixel value differencing (PVD) iii) Edges based data embedding method (EBE) iv) Random pixel embedding method (RPE) v)Mapping pixel to hidden data method vi) Labeling or connectivity method vii) Pixel intensity based.

i) LSB: this method is most commonly used for hiding data. In this method the embedding is done by replacing the least significant bits of image pixels with the bits of secret data. The image obtained after embedding is almost similar to original image because the change in the LSB of image pixel does not bring too much differences in the image.

ii) BPCP: In this segmentation of image are used by measuring its complexity. Complexity is used to determine the noisy block. In this method noisy blocks of bit plan are replaced by the binary patterns mapped from a secret data.

iii) PVD: In this method, two consecutive pixels are selected for embedding the data. Payload is determined by checking the difference between two consecutive pixels and it serves as basis for identifying whether the two pixels belongs to an edge area or smooth area.

2. Spread Spectrum Technique: The concept of spread spectrum is used in this technique. In this method the secret data is spread over a wide frequency bandwidth. The ratio of signal to noise in every frequency band must be so small that it becomes difficult to detect the presence of data. Even if parts of data are removed from several bands, there would be still enough information is present in other bands to recover the data. Thus it is difficult to remove the data completely without entirely destroying the cover .It is a very robust technique mostly used in military communication.

3 Statistical Technique:
In the technique message is embedded by changing several properties of the cover. It involves the splitting of cover into blocks and then embedding one message bit in each block. The cover block is modified only when the size of message bit is one otherwise no modification is required.

4 Transform Domain Technique: In this technique; the secret message is embedded in the transform or frequency domain of the cover. This is a more complex way of hiding message in an image. Different algorithms and transformations are used on the image to hide message in it. Transform domain techniques are broadly classified such as
i) Discrete Fourier transformation technique (DFT)
ii) Discrete cosine transformation technique (DCT)
iii)Discrete Wavelet transformation technique (DWT)
iv) Lossless or reversible method (DCT)

4 Embedding in coefficient bits.

4. Distortion Techniques: In this technique the secret message is stored by distorting the signal. A sequence of modification is applied to the cover by the encoder. The decoder measures the differences between the original cover and the distorted cover to detect the sequence of modifications and consequently recover the secret message.

6. Masking and Filtering: These techniques hide information by marking an image. Steganography only hides the information where as watermarks becomes a potion of the image. These techniques embed the information in the more significant areas rather than hiding it into the noise level.
Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image. This method is basically used for 24-bit and grey scale images.

4. Flow chart of Image Steganography

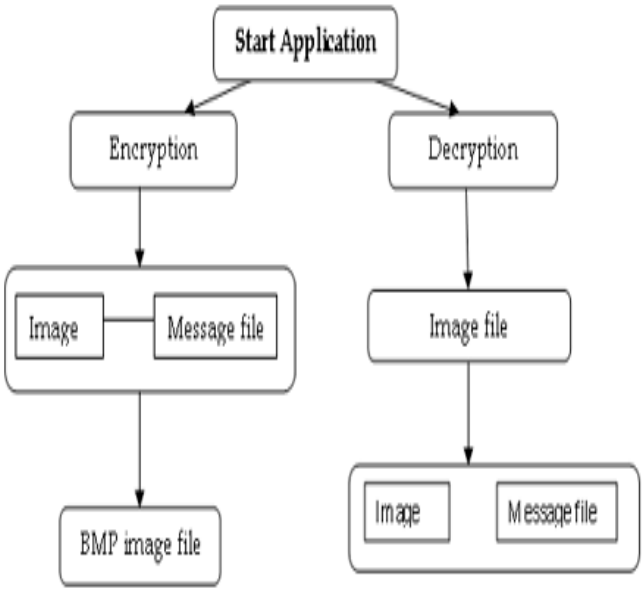

Figure2: Flow chart of Image Steganography

5. Conclusion and Future Work

Main aim of this paper is to hiding digital data into digital images. LSB is the most widely used technique for steganography. Researchers have also used the techniques like water marking, distortion technique, spatial technique, ISB, MSB in their work and provided a strong means of secure information transmission. In future, techniques to improve security for data hiding by using randomization will be used to extend this work.

References

[1] S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain "*A New Approach for LSB Based Image Steganography using Secret Key*", International Conference on Computer and Information Technology (ICCIT), Pages No. 286 – 291, 22-24 Dec., 2011.

[2] Kousik Dasgupta, J. K. Mandal, Paramartha Dutta, "*Hash Based Least Significant Bit Technique for Video Steganography (HLSB)*", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, Issue No. 2, April, 2012.

[3] Mamta Juneja, Parvinder Singh Sandhu, "*Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption*", International Conference on Advances in Recent Technologies in Communication and Computing, Pages No. 302 – 305, 27-28 Oct., 2009.

[4] Min-Wen Chao, Chao-hung Lin, Cheng-Wei Yu, Tong Yee Lee, "*A High Capacity 3D Steganography Algorithm*", IEEE Transactions on Visualization and Computer Graphics,Vol. 15, Issue No. 2, Pages No. 274 – 284, March-April, 2009.

[5] D.C. Wu, and W.H. Tsai, "A Steganographic method for images by pixel-value differencing", PatternRecognition Letters, Vol. 24, pp. 1613-1626, 2003.

[6] R.Z. Wang, C.F. Lin, J.C. Lin, "Image hiding by optimal LSB substitution and genetic algorithm",Pattern Recognition Vol. 34, pp. 671-683, 2001.

[7] W. bender, D. gruhl, N. Morimoto, A.Lu, "Techniques for data hiding", IBM Systems Journal Vol.35(3-4),pp. 313-336, 1996.

[8] H.C. Wu, N.I. Wu, C.S. Tsai and M.S. Hwang, "Image steganographic scheme based on pixel valuedifferencing and LSB replacement method", IEEE Proceedings on Vision, Image and Signalprocessing, Vol. 152, No. 5,pp. 611-615, 2005.

[9] F.A.P peticolas, R.J Anderson and M.G. Kuhn, "Information Hiding – a Survey" proceedings of the IEEE, VOL. 87, PP. 1062-1078, 1999.

Author Profile

Ritu Verma received her BE degree in Computer Science & Engineering from C.S.V.T.U, Bhilai-3 in 2012 and pursuing Mtech in CSE from R.G.P.V, Bhopal, and M.P. From 2013 to 2015.Her area of interest is image processing. She is having four international conferences in her credit.

Anju Vishwakarma pursuing BE dergree in Computer Science & Engineering from C.S.V.T.U, Bhilai-3 from 2012 to 2016.

Rupendra Sahu pursuing BE dergree in Computer Science & Engineering from C.S.V.T.U, Bhilai-3 from 2012 to 2016.