A REVIEW ON STEGANOGRAPHY AND ITS TECHNIQUES TO ENHANCE SECURITY

Kamalinder Kaur
Assistant professor
Computer scienceme and engineering
Chandigarh Engineering College,landran (Punjab) Mohali, India
er.kamalinder@gmail.com

***Abstract*—Steganography is the art and science of escaping information under unremarkable cover. In this paper the various techniques used to hide the message inside the images. The steganography systems are using secret key for cryptography. Steganography quality measures and techniques are often used to attain security as they are basic features of the information hiding system to hide the message.**

Keywords—c Steganography, Capacity, Robustness, Discrete Wavelet Transform

I. INTRODUCTION

Steganography, originates from the Greek words stegos, meaning hiding cover which means writing, is the art and science of hiding the fact that communication is taking place. Steganography refers to the science of invisible communication. Steganography and cryptography are closely related. Cryptography scrambles messages so they cannot be understood. Steganography on the other hand, will hide the message so there is no knowledge of the existence of the message in the first place. In some situations, sending an encrypted message will arouse suspicion while an invisible message will not do so. In this case, when the steganography fails and the message can be detected, it is still of no use as it is encrypted using cryptography techniques. Therefore, the principle defined once by Kerchoff's for cryptography. This principle states that "the security of the system has to be based on the assumption that the enemy has full knowledge of the design and implementation details of the steganography system".

The techniques are needed to hide some information in digital content and its presence cannot be known to others, Unlike cryptography, where the goal is to secure communications from an eaves-dropper, steganography techniques strive to hide the very presence of the message itself from an observer .The main goal of steganography is to communicate securely in a completely undetectable manner.

The modern formulation of steganography is often given in terms of the prisoner's problem [4] where Alice and Bob are two inmates who wish to communicate in order to hatch an escape plan. However, all communication between them is examined by the warden, Wendy, who will put them at the slightest suspicion of covert communication, in the general model for steganography, illustrated in Fig.1; we have Alice wishing to send a secret message *m* to Bob. In order to do so, she "embeds" *m* into a cover-object c, and obtains a stego-object s. The stego-object *s* is then sent through the public channel.

Cover-object: refers to the object used as the carrier to embed messages into. Many different objects have been employed to embed messages into for example images, audio, and video as well as the structures, and html pages to name a few.

Stego-object: refers to the object which is carrying a hidden message. So given a cover object, and a messages the goal of the steganographer is to produce a stego object which would carry the message.

And it follows the techniques to hide the data from the truders during the network.

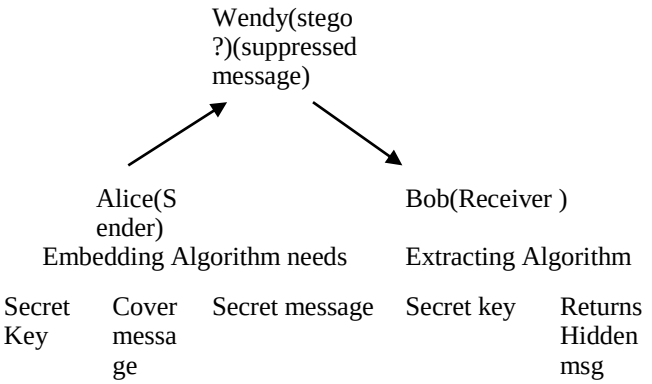

Fig1: General model of Steganography [4]

The modern steganography system is using secret key attempts to be detectable only if secret information is known namely, a secret key. In this case, cryptography should be involved, which holds that a cryptographic system's security should rely solely on the key material. For steganography to remain undetected, the unmodified cover medium must be kept secret, because if it is exposed, a comparison between the cover and stego media immediately reveals the changes.

Three basic types of stego systems are available:

1. Pure stego systems - no key is used.
2. Secret-key stego systems - secret key is used.
3. Public-key stego systems - public key is used.

The steganography is used to cover the undetected material under the cover which is to be kept secret so that the secret may not be exposed and the data remains secured during the network and that is to be passed during network .

II. STEGANOGRAPHY TECHNIQUES

Image is a collection of number that constitutes different high intensities in different areas of image. The numeric representation forms grid and the individual points referred as pixels. The image steganography techniques are as follows for covering the images .

A. SPATIAL DOMAIN EMBEDDING

The best widely known steganography algorithm is based on modifying the least significant bit layer of images, hence known as the LSB technique. This technique makes use of the fact that the least significant bits in an image could be thought of random noise and changes to them would not have any effect on the image. In the LSB technique, the LSB of the pixels is replaced by the message to be sent.

The message bits are permuted before embedding, this has the effect of distributing the bits evenly, thus on average only half of the LSB's will be modified. Popular steganographic tools based on LSB embedding [10], [11], [12], vary in their approach for hiding information. Some algorithms change LSB of pixels visited in a random walk, others modify pixels in certain areas of images, or instead of just changing the last bit they increment or decrement the pixel value.

In Spatial Domain Methods 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) Labelling 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 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 Maintaining the Integrity of the Specifications. 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) iv) Embedding in coefficient bits

5. 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.

B. TRANSFORM DOMAIN EMBEDDING

Another category for embedding techniques for which a number of algorithms have been proposed is the transform domain embedding category. Most of the work in this category has been concentrated on making use of redundancies in the DCT (discrete cosine transform) domain, which is used in JPEG compression. But there has been other algorithms which make use of other transform domains such as the frequency domain Embedding in DCT domain is simply done by altering the DCT coefficients for example by changing the least significant bit of each coefficient. One of the constraints of embedding in DCT domain is that many of the 64 coefficients are equal to zero, and changing two many zeros to non-zeros values will have an effect on the compression rate. That is why the number of bit one could embed in DCT domain, is less that the number of bits one could embed by the LSB method. Also the embedding capacity becomes dependent on the image type used in the case of DCT embedding, since depending on the texture of image the number of non-zero DCT coefficients will vary. Although changing the DCT coefficients will cause unnoticeable visual artifices, they do cause detectable statistical changes.

The Patchwork algorithm (developed at the MIT) selects random pairs of pixels, and increases the brightness of the brighter pixel and decreases the brightness of the other. This algorithm shows a high resistance to most non-geometric image modifications. If it is important to provide a

protection against filtering attacks, then the information hiding capacity is limited [4].

C. WAVELET TRANSFORMATION

A high-capacity image steganography technique that depends on wavelet transform with acceptable levels of imperceptibility and distortion in the cover image and high level of overall security. The information-hiding process in a Steganographic system starts by identifying a cover object's redundant bits (those that can be modified without destroying that medium's integrity). The embedding process creates a stego object by replacing these redundant bits with data from the hidden message. Capacity refers to the amount of information that can be hidden in the cover object, security to an eavesdropper's inability to detect hidden information, and robustness to the amount of modification the stego medium can withstand before an adversary can destroy hidden information [6].

A Wavelet is simply, a small wave which has its energy concentrated in time to give a tool for the analysis of transient, non-stationary or time-varying phenomena. A signal can be better analyzed if expressed as a linear decomposition of sums of products of coefficient and functions. A two-parameter system is constructed such that one has a double sum and coefficient with two indices. The set of coefficients are called the DWT of a signal. In Wavelet transform, the original signal (1-D, 2-D, 3-D) is transformed using predefined wavelets (haar, daubechies).

The wavelets are orthogonal, these wavelets can be defined through the scaling filter w. Biorthogonal wavelets can be defined through the two scaling filters wr and wd, for reconstruction and decomposition respectively. It is shown that when subjected to distortion from compression, the corresponding hidden message can still be correctly identified at each resolution in the DWT domain. Wavelet filters should be selected and used in the transformation and inverse-transformation

III. STEGANOGRAPHY QUALITY MEASURES

1. Peak Signal-to-Noise Ratio- The invisibility of the hidden message is measured in terms of the Peak Signal-to-Noise Ratio. The PSNR block computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is often used as a quality measurement between the original and a compressed image. The higher the PSNR, the better the quality of the compressed or reconstructed image.

2. The Mean Square Error- the MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error. The lower the value of MSE, the lower the error.

3. Capacity- when a lot of information should be embedded into a cover image, what is usually related to the current picture.

4. Imperceptibility- It is important when a secret communication occurs between two parties and the fact of a secret communication is kept to be secret.

5. Robustness-watermarking, fingerprinting and all copyright protecting applications demand robust steganographic method, i.e. where the embedded information cannot be removed without serious degradation of the image.

IV. CONCLUSION

The work on the steganography is going today to achieve high capacity, robustness and security on the hidden messages, which are embedded into images so that the active warden cannot detect its presence when it is being transmitted between the two parties. The security is a major issue which can be further enhanced on stego to hide the content. It can be made more secure by using different dictionary word indexing scheme .

REFERENCES

[1] Ali Al-Ataby1 and Fawzi Al-Naima2- A Modified High Capacity Image Steganography Technique Based on Wavelet Transform The International Arab Journal of Information Technology, Vol. 7, No. 4, October 2010.

[2] Bender,W-Gruhl,D-Morimonto,"Techniques for data hiding" ,Massachusetts Institute of Technology, Media Laboratory Cambridge, Massachusetts 02139 USA, from the proceedings of the SPIE, San Jose CA , Feb. 1995.ason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*

[3] Digital Image processing second edition by Rafel C. Gonzalez & Richard E. Woods Published by Pearson Education.

[4] G. Simmons, "The prisoners problem and the subliminal channel," *CRYPTO*, pp. 51, 1983.

[5] JR.Krenn, "Steganography and Steganalysis" Jan 2004.

[6] Lin T. and Delp J., "A Review of Data Hiding in Digital Images," in Proceedings of the Image Processing, Image Quality, and Image Capture Conference, Georgia, pp. 274- 278, 1999.

[7] Francesco Queirolo, Steganography in Images"

[8] Mehdi Kharrazi1, Husrev T. Sencar2, and Nasir Memon2, Image Steganography:Concepts And Practice Department of Electrical and Computer Engineering, Department of Computer and Information Science Polytechnic University, Brooklyn, NY 11201, USA.

[9] Misiti M., Misiti Y., Oppenheim G., and Poggi J., *Wavelet Toolbox for Use with MATLAB*, User Guide Math Works Inc., 2000.

[10] F.Collin,"http://www.winsite.com/bin/info?500000032023".

[11] G.Pulcini\stegotif,"http://www.geocities.com/SiliconValley/9210/gfree.html".

[12] Anil Kumar , Rohini Sharma,"A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique",International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7,July 2013.

[13] Dr. Fadhil Salman Abed "A Proposed Method of Information Hiding Based on Hybrid Cryptography and Steganography ", IJAIEM, Volume 2, Issue 4, April 2013 Wikipedia.org.

[14] T.Sharp,\Hide2.1,2001http://www.sharpthoughts.org

[15] Hassan Elkamchouchi, Wessam M. Salama, Yasmine Abouelseoud, "Data hiding in a digital cover image using chaotic maps and LSB technique", Computer Engineering and Systems (ICCES) 2017 12th International Conference on, pp. 198-203, 2017.

[16] Shashank Gupta, Rachit Jain, "An innovative method of Text Steganography", Image Information Processing (ICIIP) 2015 Third International Conference on, pp. 60-64, 2015.

[17] Abdullah AlWatyan, Wesam Mater, Omar Almutairi, Mohammed Almutairi, Aisha Al-Noori, Sa'ed Abed, "Security approach for LSB steganography based FPGA implementation", Modeling Simulation and Applied Optimization (ICMSAO) 2017 7th International Conference on, pp. 1-5, 2017.

[18] M. Murali Krishna, Nirmal Roberts, "Enhancement of embedding capacity and security in reversible steganography", Wireless Communications Signal Processing and Networking (WiSPNET) International Conference on, pp. 803-807, 2016

[19] Giridhar Maji, Sharmistha Mandal, Soumya Sen, Narayan C. Debnath, "Dual image based LSB steganography", Recent Advances in Signal Processing Telecommunications & Computing (SigTelCom) 2018 2nd International Conference on, pp. 61-66, 2018