International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 06, June-2015

Review of Spatial and Frequency Domain Steganographic Approaches

Jasvir Singh
Department of Electronics and Communication Engineering

Gaganjot Kaur (A.P)
Department of Electronics and Communication Engineering
BFCET, Deon, Bathinda, Punjab

Manveer Kaur Garcha
Department of Information Technology
Chandigarh Engineering College
Landran,
Chandigarh, Punjab

***Abstract*— Now days, by the fast evolution of internet it is very important to protect secret information from cyberpunks while communication. Steganography is the technique that exerts for invisible broadcasting, in which unfrequented data or information is transmitted and collected. In digital image steganography, conveyance is achieved by embedding the data into cover-image for producing the steganographic-image. Till date number of techniques has been proposed for embedding the secret message in multimedia object like images. This paper is aimed at reviewing couple of techniques in the spatial as well as frequency domain. These techniques are comparing in terms of robustness and imperceptibility using peak signal to noise ratio.**

Keywords — Steganography; entropy; robustness; imperceptibility.

I. INTRODUCTION

In this age of digitization communication is very essential in every progressive field. All sectors that are influenced by communication aspire to preserve confidential concerns. Steganography occupies a crucial role in exchanging the sensitive information across the network. It can be defined as data hiding technique in which confidential textual detail are concealed by displaying the irrelevant multimedia object.

In this era of technology, it is really very difficult to protect the confidential information across the internet from illegitimate recipients. So in order to protect the sensitive information, number of techniques has been proposed till date. Steganography is one of them. The word steganography comes from Greek wordbook which is a synthesis of two words, namely, "Stegano" signifying "covered" and "Graphie" signifying "writing". Thus the term can be defined as the method of concealed writing. In the field of information hiding, steganography is the extensively used secret communication technique in which confidential data is concealed from the viewer by hiding it in some multimedia object like image, audio or video. The significance of the topic lies in the fact that steganography outmatches its sister data hiding disciplines because it hides the existence of message from unintended recipients rather than making the contents of message meaningless like cryptography.

Steganography is not newfangled idea; its background is dates back to ages. This technique was initiated by ancient Greeks. They were accustomized to shave the head of their slaves and tattoo the messages on their heads. After the hair had grown back, the slaves were sent to their allies without the enemy's knowledge. This method had obvious disadvantage of delayed transmission and limited size. Later people used to hide message written on wood underneath wax known as wax tablets. Wax tablets were then sent to intended receiver and wax was peeled off extract the hidden message. During World War I and II, Germans used null ciphers for sharing the hidden text. Invisible inks were used to write text on paper during American Revolution. These messages were retrieved by exposing that paper to rays or fires.

The general process of steganography is shown in Fig.1 Cover file is any multimedia object and secret message is the confidential information to be transmitted. Embedding process is an operation of inserting the secret message inside cover file to generate stego-file. Stego-file is the cover file with secret message present in it, but the two are indistinguishable to human eye. This stego-file is then transferred over the network. At the receiver end, stego-file is input to extraction operation for plucking out the secret message from it. Secret key used can by a simple password or asymmetric key depending on the use case in which it is used. Secret key is used in extraction only in case if it is used while embedding. In digital image steganography, the cover file to be used can be any random image.

II. REQUIRED PROPERTIES OF STEGANOGRAPHIC TECHNIQUES

Though Steganography is not a new technique it is still under research and development because of its quality and quantity trade off. Quality is related to the cover image and quantity is related to the maximum length of message that can be embedded in the cover image. when a lengthy message is embedded in the image it degrades the quality more as compare to shorter messages so it can be said quality is inversely to quantity. Quantity is measured in bits per pixel (bpp) and quality can be measured using any performance metric like peak signal to noise ratio (PSNR) or structural similarity index measure (SSIM).

Robustness is another factor that may significantly affect the steganographic algorithm. This term is related to the survival of message when the steganographic image is prone to various intentional or unintentional attacks like cropping, noising, compression etc. if the message survive under attacks, the technique is referred to as robust else it is called fragile technique.

Imperceptibility is the most important factor to be considered while embedding a message in the image. This means that the changes to cover image after embedding message should not be visible to the viewer. If the changes are perceptible to the human eye, this will reveal the presence of anything in it; thus breaking the confidentiality rule of steganography.

III. DIGITAL IMAGE STEGANOGRAPHIC TECHNIQUES

Digital image steganographic techniques are broadly categorized as spatial domain techniques and frequency domain techniques. Spatial domain techniques are those in which message bits are directly embedded into pixel values like least significant bit (LSB) substitution method; where as in frequency domain, the cover image is first transformed to another domain like discrete wavelet transform (DWT) for embedding the message.

A. Spatial Domain Techniques

The general flow chart of spatial domain techniques is shown in Fig. 2.

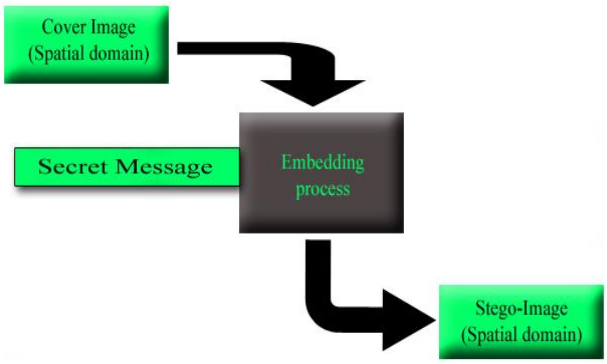

Fig. 2. Steganography process in spatial domain

Least significant bit (LSB) substitution is the most basic approach to steganography which acts as the base for many other techniques. Mishra et al. (2012) used a spatial domain LSB substitution for embedding a piece of information in an image. However, in order to achieve higher security of message as compared to basic LSB method, Arnold transformation was successively applied twice in two different phases. The system was tested and validated against a series of standard gray scale images and the results obtained were found to be highly promising.

Cheng and Tseng (2009) proposed two hybrid least significant bit substitution methods. The first method coupled the optimal least significant bit substitution and optimal pixel adjustment process to improve the quality of steganographic image. The second method was the variation of the first one which replaces the optimal LSB substation with the worst LSB substitution. Based on these collaboration techniques, better steganographic quality was achieved. Experimental results presented in the paper showed that proposed method was superior to previous works.

Sharma and Kumar (2013) proposed a steganographic algorithm based on least significant bit substitution to hide text file inside the digital image. All the three layers of an RGB image were used alternatively to embed data in the least two significant bits of selected pixel. In order to increase the storage capacity (i.e. length of message that can be embedded inside image), a compression algorithm was used that compresses the data to be embedded. The used compression algorithm works in a range of 1 bit to 8 bits per pixel ratio. And the developed system was able to maintain the accuracy and confidentiality of data. Furthermore, two cover images were used. Message was embedded in the first cover image which was then covered by second cover image. This hides the degradation of first cover image that were caused due to embedding of message.

Kaur et al. (2013) introduced a steganographic approach based on jump table with the identical matching concept. It is the Sami-blind embedding and extraction approach. The pixels of alternative RGB layers are used for embed the secret message. If no identical match found at any place of pixel than least significant bits are replaced with the secret message bits. The concept of secret key extraction and image blocking was also introduced in this approach. The results in terms of PSNR and CC were promising for this approach.

B. Frequency Domain Techniques

In frequency domain, the image is first transformed to its frequency distribution. Unlike in the spatial domain where changes are made to pixel values directly, in frequency domain the rate is dealt at which the pixel values change in spatial domain. Whatever processing is to be done is carried in frequency domain and the resultant image is subjected to inverse transform to obtain the required image. Discrete cosine transform (DCT), discrete fourier transform (DFT), discrete wavelet transform (DWT) etc are the examples of frequency domain.

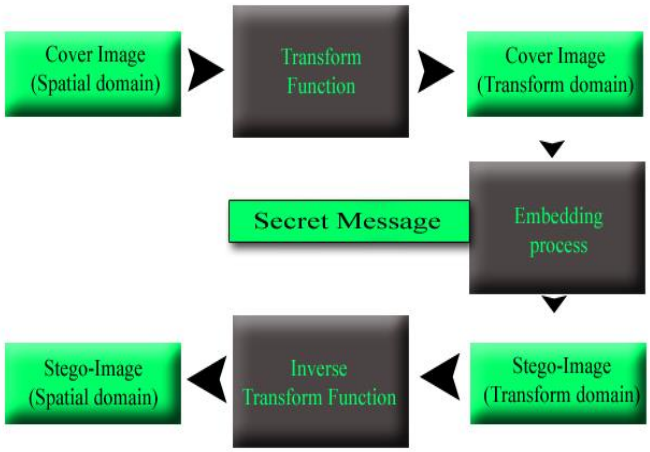

Fig. 3: Stegnography process in transform domain

Mali et al. (2013) proposed entropy based technique using block level entropy thresholding. In this method, cover image was divided into 8×8 non overlapping blocks. After selecting block DCT was computed for selected block. Secret message was embedded on block by middle frequency selection. This method gave much preferable robustness, good PSNR results and provides high security [14].

Patil et al. (2013) presented frequency domain steganographic method based on entropy thresholding

scheme. In this method, large volume of data was embedded in image. After computing 64 DCT coefficients for each non overlapping block, entropy of four most significant bits and least significant bits was computed. This proposed technique was data hiding method with which one can adjust quality factor and embedding capacity dynamically [15].

IV. RESULTS AND DISCUSSION

In this paper, by observation of various methods it can be defined that the field of steagnography got progression in past years in terms of metrics like MSE, PSNR, data hiding capacity and robustness. The techniques in which message is embedded in spatial domain possess superior results for PSNR and MSE, but have medium rate of data hiding. The techniques in which data is embedded in frequency domain posses good results for robustness and data hiding capacity but slight insufficient results for PSNR and MSE. The values of such metrics for some existing methods are listed in Table 1.

Table 1 Results for proposed methods

METHODS	Average MSE	Average PSNR (dB)	Robustness	Capacity
Existing Method 1.[7]	0.000425	50	Low	low
Existing Method 2.[8]	0.000250	60	Low	high
Existing Method 3. [13]	0.00030	85	Low	high
Existing Method 4.[14]	0.000400	55	high	low
Existing Method 5.[15]	0.000225	65	high	low

REFERENCES

[1] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," IEEE Security and Privacy Magazine, vol. 1, 2003.
[2] C. Christian, "An information theoretic model for steganography," Proceedings of 2nd Workshop on Information Hiding, MIT Laboratory for Computer Science, vol. 1525, pp. 306-318, 1998.
[3] T. Morkel, "Image Steganography Applications for Secure Communication," Universiteit van pretoria, May 2012.
[4] W. Peter, "Disappearing cryptography: Information hiding: Steganography and watermarking," San Francisco, 1992.
[5] S. Channalli and A. Jadhav, "Steganography: An Art of Hiding Data," International Journal on Computer Science and Engineering, vol. 1, 2009.
[6] S.F. Mare, M. Vladutiu, L. Prodan, "Decreasing change impact using smart LSB pixel mapping and data rearrangement," 11th International Conference on Computer and Information Technology, pp.269-276, 2011.
[7] M. Mishra, S. Kumar and S. Mishra, (2012), "*Security enhanced digital image steganography baed on successive Arnold transformation*", Advances in Intelligent Systems and Computing, vol. 167, pp. 221-229.
[8] V. Sharma and S. Kumar, "A new approach to hide text in images using steganography," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, April 2013
[9] R. Ji, H. . Yao, S. Liu, L.Wang, "Genetic algorithm based optimal block mapping method for LSB substitution," IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 215-218, 2006.
[10] C. C. Chang and H. W. Tseng, "Data hiding in images by hybrid LSB substitution," Third International Conference on multimedia and Ubiquitous Engineering, pp. 360-363, 2009.
[11] A. M. Al-Shatnawi, "A new method in image steganography with improved image quality," Applied Mathematical Sciences, vol. 6, 2012.
[12] C. C. Chang and H. W. Tseng, (2009), "*Data hiding in images by hybrid LSB substitution*," Third International Conference on multimedia and Ubiquitous Engineering, pp. 360-363.
[13] Pavninderpal Kaur, Harchet Singh, Dr. Anupama Gupta, Akshay Girdhar, "An improved steganographic approach to diminish data modification for enhancing image quality", IEEE, 2014.
[14] B.S.Patil, A.H.Karode, S.R.Suralkar, " Image Steganography Based on Entropy Thresholding Scheme" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-3, Issue-1, October 2013
[15] Jagdish Mali, Viraj Sonawane, Prof. R.N.Awale, "Image Steganography Using Block Level Entropy Thresholding Technique" International Journal of Engineering Research and ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 4, Jul-Aug 2013, pp. 412-415