A Overview of various Steganographic Domains and its applications

Poonam Yadav [1], Maitreyee Dutta [2]
[1] ME Scholar, ECE Department, NITTTR, Punjab University, Chandigarh
[2] Professor, CSE Department, NITTTR, Punjab University, Chandigarh

Abstract – Due to increase in usage of internet, it has become important to keep the online communication secure and concealed. Many users are there all over the world who shares their views, thoughts and ideas through the use of international network. Many techniques have been developed so far for ensuring the secrecy of transfer of these thoughts and ideas. Few of them are stegnalysis, cryptanalysis and copyright protection more often known as digital watermarking. Sometimes the combination or hybrid of these techniques is used to attain confidential data such as in military, banks etc. One such technology named as crystography which is a hybrid of steganography and cryptography. This paper aims at discussing various steganography algorithms developed till now and their applications in real life that might help researchers in this field by giving guidelines for future scope and work.

Keywords – Steganography, transform domain, space domain, cover media, stego media, concealed information.

Layout of this paper is as follows: concept and brief of steganography is described in section I, various transform and space fields are covered under section II, evaluating parameters and its applications are discussed under section III, related work is described under section IV and section V concludes the paper.

I. INTRODUCTION

Digital image processing is one such field which makes the use of this concept of hiding i.e steganography as it can be applied to any type of cover object such as text, audio, video, images, network or protocol steganography. Most widely and commonly used cover media is image as it is less prone to imperceptibility [1]. The cover image can be gray scale image or colored image. An image is a collection of pixels which are arranged in rows and column format. Image steganography is a method of hiding a text in an image, an image in an image, or it can be some audio that can be hidden in an image. The message should be hidden in such a way that it is not easy to be detectable by the human visual system. The steganography is in use since historical time's long back in B.C. era. Steganography is study of concealing information over covert medium, so as to camouflage the data such that data imperceptibility can be attained. The Greek words 'Stegos' meaning 'cover' and 'graphia' meaning 'writing' form a word steganography which signifies 'cover writing' [2]. There are categories of steganography such as technical steganography, linguistic steganography, copyright enforcement and wisdom from cryptography [3]. A steganographic system can be counter played by an adversary observation that a file contains hidden information in it, while counter playing on a watermarking system signifies the removal of the trademark but not to trace that mark [4]. An example of image steganography is shown in figure 1. Here, text is hidden in the image having huge amount of redundant information. If the embedding capacity is to be increased then the message to be hidden can be compressed by various available compression algorithms. There are lossy as well as lossless compression techniques. Lossy includes JPEG compression whereas lossless includes Huffman coding, run length encoding, Lempel ziv Welch coding etc.

Fig. 1 Image Steganography

Steganographic mechanism can be understood well with the help of following block diagram shown in figure 2.

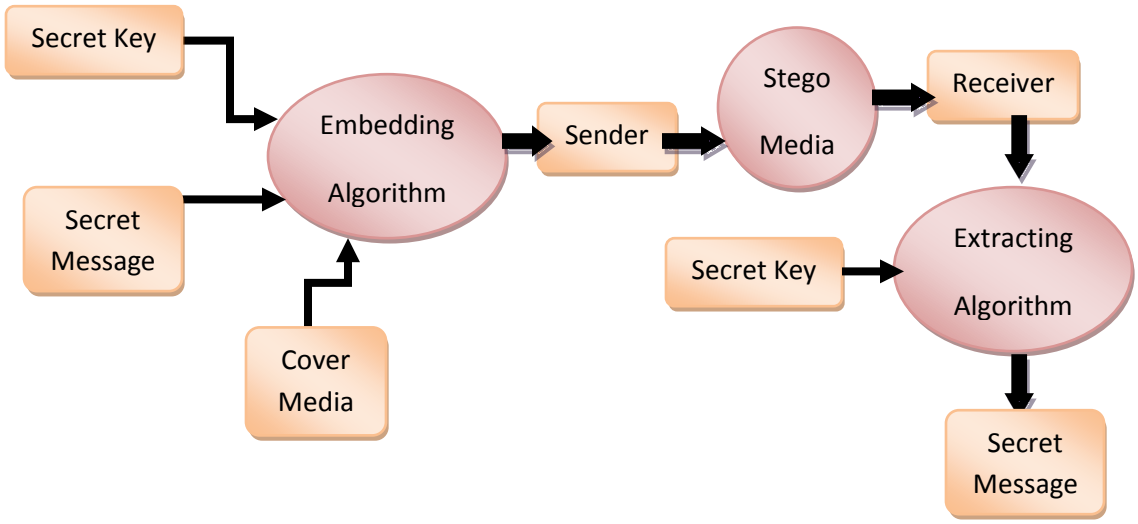

Fig. 2 Steganographic Mechanism

II. FIELDS OF STEGANOGRAPHY

Transform domain and space domains are the two broad categorization of steganography. In case of frequency or transform domain the image first undergoes transformation that might be discrete fourier, discrete cosine, discrete wavelet, and integer wavelet transformation. Once transformation takes place then the image is ready to hide the message into it. In case of DFT, the fourier analysis is done for transforming the image. DCT coefficients are generated by DCT blocks in case of discrete cosine transform. Wavelet frequency coefficients are formed namely called as baby wavelets which further get classified into detailed band and approximation band.

Space domain also known as spatial domain or image domain is called so because data is inserted directly into the intensities of pixels of an image. Various algorithms in space domain are LSB substitution in which the data is hidden into the least significant bits, pixel value differencing method where first the difference of two pixel values are calculated and then message is hidden into this difference value, Histograms based steganography is that in which data is hidden into the intensities generated in the histogram generation, Color palette steganography is the one in which indexed images are created in which colors of the image are stored in the palette which is called color look up table [5], and then is spread spectrum steganography in which direct sequence spread spectrum or frequency hopping spread spectrum method is used [6]. This method is highly secured above all the categories of steganography.

III. Evaluation parameters

The steganographic methods have some merits and demerits so it is essential to figure out the most suitable algorithm for a particular application on the basis of following parameters.

a) Imperceptibility: The basic evaluating parameter is the imperceptibility which is ability of the mechanism of being unnoticed by the human mind and senses. It can also be termed as invisibility. If one is able to find out the changes being made in the image then and there that algorithm fails [7]. Imperceptibility is the measure of PSNR and MSE which are also considered as distortion measure. Higher the PSNR better is the imperceptibility and the image quality at the receiver end. Value of PSNR should be maximum possible & is calculated by the following relation in equation (1)

$$PSNR=10 \log10 [Q2/MSE] \quad (1)$$

where Q is pixel values and for 8 bits per pixel Q=255. MSE should be minimum possible & is calculated from the equation (2):

$$MSE= (\frac{1}{N})2 \sum_{i=1}^{N} \sum_{j=1}^{N} (X[i,j] - \overline{\overline{X}}[i,j]) \quad (2)$$

where X is cover image and $\overline{\overline{X}}$ is stego image.

b) Embedding Capacity: Steganography requires large amount of hiding capacity because of covert communication between two parties which is not with the case of watermarking as it doesn't need high payload capacity for just embedding small amount of copyright protection mark [7]. Maximum hiding capacity and bit rate are the two measures of determining embedding capacity. As the name suggests maximum hiding capacity means the maximum amount of data that can be hidden in image and can be measured in bits, bytes or KB. Bit rate is the maximum number of bits that can be hidden in one pixel. It can be calculated as :

$$\text{Bit rate} = \frac{\text{Number of bits to be hidden}}{\text{Size of an image}} \text{bits per pixel} \quad (3)$$

For example, if 20,000 bits are to be hidden in an image of size 256*256, then bit rate will be (20,000/(256*256)) = 0.305bpp.[43]

c) Steganalysis: It means how robust an algorithm is to be secured against all kinds of attacks and the visual quality of cover media must not be degraded. It can also be termed as ability of being strong to withstand or overcome statistical attacks [7].

d) Image Manipulation: While communicating there may be a possibility that image undergoes some manipulation as an attempt to discard the hidden information. Also, image cropping or rotating can be done before reaching the destination. As a result, these changes may destruct the hidden information. Thus, it becomes a challenge for a steganographic algorithm to be robust against these manipulations [7].

e) Format of the files: There are many files available that are used for hiding the secret messages like images, audios and videos as discussed earlier. Each file type has its respective format. Image file formats such as BMP, JPEG, GIF, PNG and TIFF available over the internet. Few video file formats are AVI, MPEG and MP4. WAV, MPEG, MP3, Raw, Vorbis are some audio file formats [8]. If two parties are communicating in only one type of format then it becomes questionable and suspicious. Hence, a powerful steganographic algorithm should be designed which can support various types of file formats.

- Applications of Steganography

Steganographic techniques have obvious uses, some legitimate, some less so, and some are likely illegal. The illegal use varies from trivial to absonant. There might be a possibility that innocent files or images may have child pornography lurked inside [9].

The most common application of steganography is watermarking to be used as copyright protection. Photo collections, CDs and DVDs have hidden messages which can detect the unauthorized access. To keep the communication secret and to co-ordinate attacks terrorists makes use of steganography which seems facinorous. The most obvious usage of steganography is espionage which is the usage of spies to obtain military or political secrets in an organized manner. Steganography has found various uses in military, personal, diplomatic and intellectual property offenses applications [10].Many other applications of steganography are as follows:

- Infrared Communication in Military.
- Hiding confidential information of nuclear reactors (such as data related to munitions of wars, reports including reactions, unique chemical and physical features of specific materials etc).
- Medical Imaging
- Modern printers- used in color laser printers that adds minute dots of yellow color which is barely visible containing encoded printers serial number and date and time stamps.
- Online Challenge – Cicada 3301(puzzle mainly focusing on data security, cryptography and steganography).
- Cryptography based on RSA public key algorithm is used for digital signatures.
- ATM Transactions
- Criminal Communications
- Computer Security
- Paedophilia
- Sudoku Puzzle

IV. RELATED WORK

El_Rehman et. al. in [11] proposed a method of hiding secret bits sequentially in LSB by using frequencies in lower and middle range and performance analysis is done on the basis of PSNR and MSE. Here, image transformation into frequency domain is done with DCT where image coefficients of quantized DCT are fragmented into 8×8 blocks such that they are not overlapping each other. Then, data in LSB of DC components, lower and middle frequencies is embedded.

Subhedar & Mankar et. al. in [12] proposed a method combining Redundant Discrete Wavelet Transform and Quick Response decomposition to perform transform domain image steganography. For maximizing the embedding capacity with robustness to additive noise this redundancy in shift invariant RDWT is used. QR decomposition has an advantage of lower extrapolating complexity and avoiding false positive issues in Singular Value Decomposition. Performance analysis is done on the basis of PSNR, RMSE and SSIM.

Yash and Sudhanshu et. al. in [13] described steganography on grey as well as color images by aggregating DCT enhancement with RSA using LSB technique. RSA is performed to enhance the security. DCT is performed to enhance the stego image quality with smallest distortion. The performance analysis is on the basis of PSNR and entropy.

Gulve et. al. in [14] proposed spatial domain technique i.e. PVD for concealing message into frequency domain. Concealing of information is improved by modifying two wavelet coefficients difference when paired and then use this difference for hiding purpose. The performance analysis is evaluated on the basis of PSNR, MSE, Hiding Capacity and Security.

Huang et. al. in [15] proposed an effective structure of Reversible Data Hiding in ciphered form where sub-blocks of m × n size are generated by partitioning of pixels in an image. Afterwards pseudorandom key stream in combination to a plain text message is generated for getting a ciphered message, and the pixels in the same sub-block are encrypted with the same key. For all this procedure an encryption key is used. The performance analysis is done on the basis of PSNR and embedding capacity.

Gulve and Joshi et. al. in [16] has put forward a method in which five pixel pairs were formed by partitioning an image into 2×3 blocks of pixels after having gray code conversion of an image. Here, rather than hiding M bits, number of bits less than or equal to average number of bits, a pair of block can conceal using the difference value.

V. CONCLUSION

Since steganography has wide range of applications thus steganography has wide range of usability and it depends upon the types of application that what type of algorithm is used. The Steganographic mechanism should be so chosen so as keeping in mind all the evaluation parameters such as high imperceptibility, high PSNR, low MSE, low BER, higher embedding capacity and so on. More and more hiding mechanisms and optimization techniques are under work to increase the level of security

VI. REFERENCES

[1] Sumeet Kaur, Savina Bansal, R. K. Bansal, “Steganography and classification of image steganography techniques”, International Conference on Computing for Sustainable Global Development, pp. 870-875, 2014.

[2] T. Moerland, “Steganography and Steganalysis”, Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/privtech.pdf, pp. 1-8, 2001.

[3] Katzenbeisser, S., Petitcolas F. A.: “Information Hiding Techniques for Steganography and Digital Watermarking”, Artech House, London, 2000, pp. 64.

[4] R. J. Anderson & Petitcolas, “On the limits of steganography”, IEEE Journal of selected Areas in Communications, Vol. 16, pp. 474-481, 1998.

[5] Y. K. Lee & L. H. Chen, “High Capacity Image Steganographic Model”, IEE Proceedings- Vision, Image and Signal Processing, Vol. 147, pp. 288-294, 2000.

[6] L.M. Marvel, C.G. Boncelet, & C. Retter, “Spread Spectrum Steganography”, IEEE Transactions on image processing, Vol. 8, pp. 1075-1083, 1999.

[7] T. Morkel, J.H.P. Eloff & M.S. Olivier, “An Overview of Image Steganography”, Proceedings of Information and Computer Security Architecture (ICSA) Research Group, Pretoria, South Africa, pp. 1-12, 2005.

[8] Shivani Chauhan and Jyotsna, “Multiple Layer Text Security using Variable Block Size Cryptography and Image Steganography”, International Conference on Computational Intelligence and Communication Technology, IEEE, pp. 1-7, 2017.

[9] Brad H. Astrowsky, “Steganography: Hidden Images, A New Challenge in the Fight against Child Porn” URL http://www.antichildporn.org/steganog.html.

[10] James C. Judge, “Steganography: Past, Present, Future”, Information Security Reading Room, SANS, 2001.

[11] Sahar A. El_Rehman, “A Comparative Analysis of Image Steganography based on DCT Algorithm and Steganography Tool to Hide Nuclear Reactors Confidential Information”,

Journal of Computers and Electrical Engineering, Elsevier, pp. 1-20, 2016.

[12] Mansi S. Subhedar and Vijay H. Mankar, " Image Steganography using Redundant Discrete Wavelet Transform and QR Factorization ", Journal of Computer and Electrical Engineering, Elsevier, Vol. 54, pp. 406-422, 2016.

[13] Yash Kumar Singh and Sudhanshu sharma, "Image Steganography on gray and color image using DCT Enhancement and RSA with LSB method", International Conference on Inventive Computation Technologies, IEEE, Vol. 3, pp. 1-5, 2016.

[14] A. K. Gulve and M. S. Joshi, " An Image Steganography Method Hiding Secret Data into Coefficients of Integer Wavelet Transform Using Pixel Value Differencing Approach", Journal of Mathematical Problems in Engineering, Hindawi Publishing Corporation, Vol. 2015, pp. 1-11, 2015.

[15] Fangjun Huang, Jiwu Huang and Yun-Quing Shin, "New Framework for Reversible Data Hiding in Encrypted Domain", IEEE Transactions on Information Forensics and Security, Vol. 11, pp. 2777-2789, 2016.

[16] A. K. Gulve and M. S. Joshi, "An image steganography algorithm with five pair differencing and gray code conversion", International Journal Image, Graphics and Signal Processing, Vol. 6, no. 3, pp. 12-20, 2014.