A Survey on Image Steganography & its Techniques in Spatial & Frequency Domain

Kirti D. Nagpal
PG Student, Dept. of Electronics and Communication,
Agnihotri College of Engineering (ACE),
Wardha, India
e-mail: kirtinagpal.engr@gmail.com

Prof. D. S. Dabhade
Asst. Professor, Dept. of Electronics and Communication,
Agnihotri College of Engineering (ACE),
Wardha, India
e-mail: dabhaded29@yahoo.com

***Abstract*—**Steganography is an intelligent art of communicating in a way which hides the endurance of the communication. The image steganography technique takes the asset of confined power of visual system of human being. The art of hiding information such that it averts ferreting out of hidden messages is getting very popular nowadays, which is referred as Steganography. The word Steganography has been educed from the two Greek words - *Steganos*, which mean covered or secret and *Graphy* mean writing or drawing. There have been many techniques for hiding information or messages in images in such a manner that the modifications made to the image are perceptually undetected. This paper proposes the evaluation of a few techniques of the Image Steganography in spatial domain and frequency domain. The Image Steganography techniques in spatial domain that would be discussed are Least-Significant-Bit (LSB), LSB Replacement, LSB Matching, and Bit Plane Complexity Segmentation Steganography and frequency domain techniques to be conferred in this paper are Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Singular Valued Decomposition (SVD). Steganography technique is intended to be compared with the Watermarking Technique.

Keywords*-*Image Steganography, Spatial domain, Frequency domain, LSB, DWT, DCT, DFT, SVD

*****

I. INTRODUCTION

Due to advancement in multimedia processing technologies, it has been possible to exchange large amount of multimedia data over a wide variety of networks. The use of internet makes creation, edition, deletion and/or distribution of digital images, audio/video very easy and at low cost. However, the data transmitted through internet may not be safe. Various confidential data such as Government tenders, Military information, Banking information, commercial important documents and other secured data such as images taken in space or geographical images taken from satellite etc. are transmitted over the Internet. While communicating secret information, we need techniques that hide information more securely. This gives rise to the need of Steganography technique- an important tool to achieve security.

The steganography can be accomplished through various carrier file formats such as Image, Text, Audio, Video etc. but widely implemented with digital images because of their frequency on the internet. So in this paper, digital images would be used for the discussion for implementing Steganography techniques.

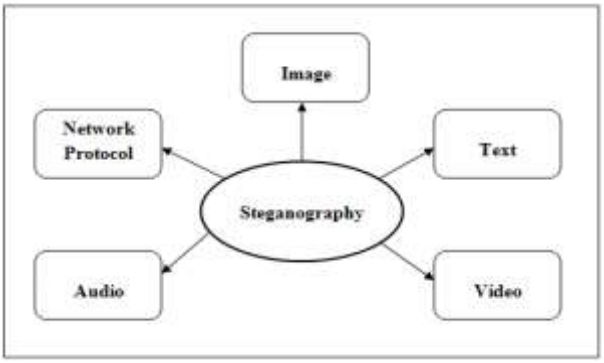

Fig.1: Various Digital Mediums to implement Steganography

A digital image is an accumulation of number of pixels with different intensity values, and each image is in the form of m*n, no of pixel (where m and n are number of Rows and Column respectively). During the image steganography process, some of the characteristics of the images are changed so as not to be identifiable by human eye. It is a process that hides the secret image behind the cover image in such a way that the presence of the secret image is undetectable and the cover image appears to be the same. Using this technology, the digital information can be embedded and transferred to the destination with minimum exposure to be recognized.

A large variety of steganography techniques exists for hiding secret information in images. This paper intends to give an overview of image steganography, its uses and few of its techniques. Over the past few years, numerous steganography techniques have been proposed that embed hidden messages in multimedia objects. Image Steganography hides information or messages in images in such a manner that amendment made to the image is perceptually obscured. Commonly approaches related to steganography are Spatial-domain and Frequency-domain approach. This paper presents the evaluation of Image Steganography techniques used in these domains.

Basically, image steganography includes two processes: Embedding and Extraction. Embedding process involves embedding the stego image into the cover image such that the embedded image should completely hide the stego image, where stego image refers to the undercover image to be concealed into the cover image. Cover image is the image which appears normal to the viewer. While extraction process removes the stego or secret image from the stego embedded image. To extract the secret image, same stego-key must be used as that of implied while embedding process. Due to this fact, only the intended receiver can suspect and remove the existence of the secret image providing high security. The model for image steganography for embedding and extracting the secret image is shown in the figure 2 and figure 3:

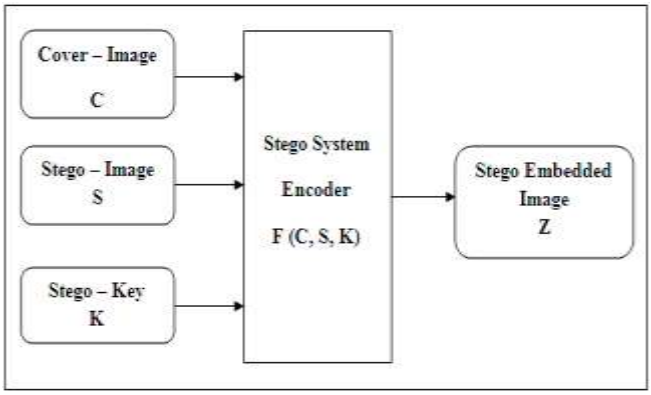

Fig. 2: Basic exemplary for Image Steganography-Embedding

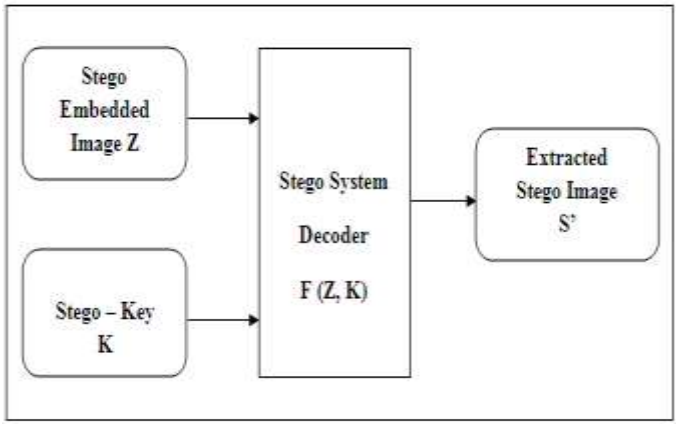

Fig. 3: Basic exemplary for Image Steganography-Extraction

Steganography technique is aimed to be correlated with the Watermarking Technique.

II. DIFFERENCE BETWEEN IMAGE WATERMARKING AND STEGANOGRAPHY

The two technologies those are firmly knit together to embedding the secret image into the cover image are-Watermarking and Steganography. These techniques are mainly related with the protection of subjective equities. But both the algorithms have different requirements [1]. Watermarking is based on the fact that the information buried inside the files may be enlightened to the public or it may even be visible. While, in steganography unrevealing of the information is momentous. The main goal of Steganography is to hide, some kind of data d, in some another data d', to obtain new data d'', practically indistinguishable from d', in such a way that an eavesdropper cannot detect the presence of d in d''; whereas, the main goal of Watermarking is to hide, a data d, in some data d', to obtain new data d'', such that a meddler cannot remove data d from d''.

III. BACKGROUND OF THE PROBLEM

In the present digital scenario, secure communication is the prime requirement. Communication of secret information is a critical factor in information technology that continues to create challenges with increasing levels of sophistication. In this modern era, internet offers great convenience in transmitting large amounts of data in different parts of the world. Yet, the safety and security of long distance communication remains an issue. Internet and web based systems are vulnerable to a variety of cyber-attacks, spoofing and many more. In order to solve this problem has led to the development of steganography schemes.

IV. HISTORY OF STEGANOGRAPHY

Throughout history Steganography has been used to secretly communicate information between people. It has been used in various forms for thousands of years.
Some case history of use of Steganography in past times is:

- During World War 2, invisible ink was used to write information on chunks of paper so that the paper appeared to the average person as just being blank pieces of paper. Solvents such as milk, vinegar and fruit juices were used for writing, because of the property of these substances such that when any of these is heated they darken and become visible to the human eye.
- In Ancient Greece, emperors used to select a person as a courier and shave their head to write a message on their head. Hair was allowed to grow back as the message had been written. After the hair grew back the messenger was sent to deliver the message, the legatee would shave off the messengers hair to see the secret message [1].

V. OBJECTIVE

This paper's focus is on the review of steganography in digital images. The objective of the paper is to study various Image Steganography techniques in frequency domain which focus on the fact that secret information being communicated is concealed and communication should take place in an inconspicuous manner. Image Steganography can be achieved by embedding a stego image into a digital image such that it should be practically indistinguishable from the cover image which can be applicable for the purpose of copy right protection, ownership verification, broadcast monitoring, authentication etc.

VI. CLASSIFICATION OF IMAGE STEGANOGRAPHY

Image steganography techniques can be classified into two types: Image steganography in the Image Domain and those in the Transform Domain. Image Domain techniques are also referred as spatial domain technique. In this technique, messages are directly embedded in the intensity of the pixels. Meanwhile transform domain methods also known as frequency domain techniques, transforms the images first and then embeds the secret message in the cover image [1].

A. Spatial Domain Methods: Steganography techniques that modify the cover image and the secret image in the spatial domain are known as spatial domain methods. These techniques implicates encoding at the level of least significant bits in the image. Spatial domain is based on physical location of pixels in an image**.** This technique changes some bits in the image pixel values in hiding data. Generally 8 bit gray level or color images can be used as a cover to hide data. Binary representations of these pixels are acknowledged to mask the secret information. Least Significant Bit (LSB) replacement, LSB matching, Plane Bit Substitution Method (PBSM), Matrix embedding and Pixel value differencing are some of the spatial domain techniques.

These techniques directly encode the message bits of pixel gray levels and their color values. Spatial domain based image steganography techniques makes embedding and extraction

quite simple. The major drawback of these methods is low Peak Signal to Noise Ratio because of high amount of noise added in the image scrambling the analytical features of the image. Moreover these embedding algorithms make loss of the message bits for lossy compression schemes like JPEG during the compression step. Hence are suitable to lossless image-compression schemes like TIFF images. [9]

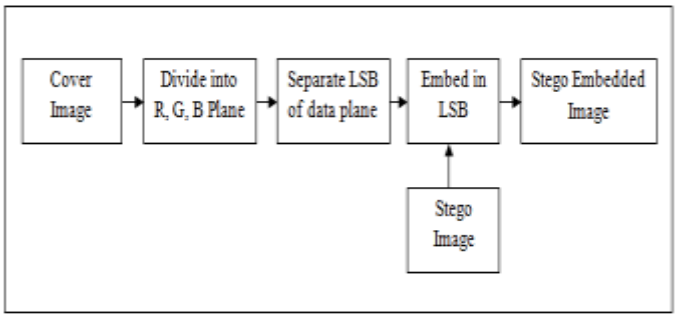

Fig. 4: Image Steganography in Spatial Domain

The least-significant-bit (LSB):

The least-significant-bit (LSB) based approach is a popular type of steganographic algorithms in the spatial domain. Least significant bit (LSB)-based steganography is one of the simplest techniques. The basic concept of Least Significant Bit technique includes the embedding of the secret data at the bits which having minimum weighting so that it will not affect the value of original pixel. It hides a secret message in the LSBs of pixel values without introducing many perceptible distortions since changes in the value of the LSB are imperceptible for human eyes. Inserting least significant bits (LSB) is a elementary approach to pierce information in an image file. The steganographic techniques based on least significant bit works on the principle of enclosing the secret message bits directly into least significant bit plane of the cover-image in a predetermined array. This technique takes an advantage of human perceptible system such that small changes in the amplitude does not make any difference in the human-perceptibility caused by inflecting the least significant bit [2,11].

The common LSB-based avenues includes LSB replacement, LSB Matching, and LSBMR which deals with each given pixel/pixel pair without considering the difference between the pixel and its neighbors [14].

LSB Replacement:

LSB replacement is a well-known technique for implementing steganography to an image. In this steganography technique, the least significant bit plane of the cover image is only overwritten with the secret bit stream according to a pseudorandom number generator (PRNG). Subsequently, some structural dissymmetry is introduced which results in never decreasing even pixels and increasing odd pixels when hiding the data, and thus existence of hidden message becomes more apparent even at a low embedding rate using some reported analytic algorithms related to image steganography, for instance Chi-squared attack, regular/singular groups (RS) analysis, sample pair analysis, and the general framework for structural steganalysis [6].

LSB Matching (LSBM):

LSB matching employs a minor modification to the LSB replacement technique. The working principle of this technique is that if the secret bit does not match the LSB of the cover image, then +1 or -1 is randomly added to the corresponding pixel value. The feasibility of increasing or decreasing for each modified pixel value is the same and so the accessible asymmetry rarity imported by LSB replacement technique can be easily refrained. Consequently, the typical advances used to detect LSB replacement are totally inadequate at detecting the LSBM [6].

Bit Plane Complexity Segmentation (BPCS]:

Kawaguchi introduced Bit Plane Complexity Segmentation (BPCS) Steganography technique. This technique uses the higher bit planes for embedding information. In Bit Plane Complexity Segmentation Steganography, each block is disintegrated into plane having number of bits. The LSB of each pixel in the image forms a binary image that is nothing but the LSB plane. Each segmented bit-plane is divided into two domains- 'informative domain' and 'noise-like domain' based on a verge value block by analyzing its complexity in each plane. The secret data is secluded in noise regions intending not to degrade the image quality. High stuff in sufficiency and fewest deterioration of the cover-image are the two key features of Bit Plane Complexity Segmentation Steganography technique [10].

B. Transform Domain Methods:

Transform domain based techniques encodes secret message bits in the transform domain coefficients of the cover image. The process of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain. The product of high quality embedded image is obtained by first transforming the original image into the frequency domain. With these techniques, the impressions are not enumerated to the intensities of the image but to the values of its transform coefficients. Then inverse transform is applied to the enumerated coefficients to generate the stego embedded image. Transform domain techniques have an asset over spatial domain techniques as they provide more secured information during hole up. Robust watermarking is the key aspect of the transform domain techniques to embed the data. By being embedded in the transform domain, the hidden data fits as fiddle in vigorous areas, radiates over the gross image, and provides better resistance against being detected by an eavesdropper. [9]

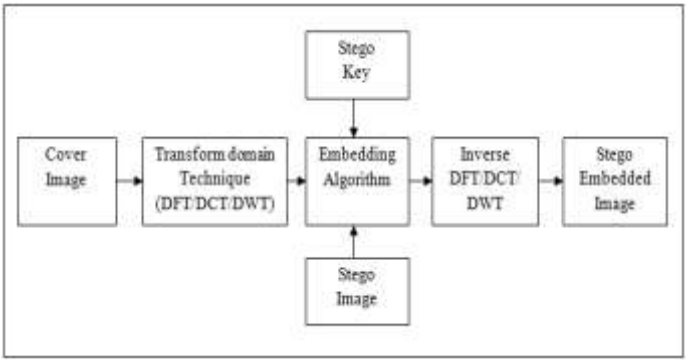

Fig. 5: Image Steganography in Frequency Domain

Transform domain techniques are customarily categorized into Discrete Cosine Transformation (DCT), Discrete Wavelet transformation (DWT), Discrete Fourier Transformation (DFT), Singular Value Decomposition (SVD) etc.

Discrete Cosine Transformation Technique (DCT):

The Discrete Cosine Transform allows an image to be broken up into different frequency bands, making it much apparent to embed secret information into the middle frequency bands of the cover image. The middle frequency bands are chosen such that they minimize the most visual important parts of the image i.e. low frequency components without over-exposing themselves to removal through compression and noise attacks. The transformed matrix consists of both AC and DC coefficients. If the DCT technique is applied on block of size NxN then it is called block DCT. In DCT transformed block the left top corner element is called as DC coefficient which is perceptually significant and the remaining coefficients are called AC coefficients which are perceptually insignificant. These coefficients are scanned in a zigzag manner to capture the frequency components of an image in the decreasing order [16].

Discrete Wavelet transformation technique (DWT):

The basic idea in the Discrete Wavelet Transform is like an image is split into two sections, customarily high frequencies and low frequencies parts. The elements at the edge of the image are predominantly to the high frequency part. The low frequency part is again breached into two parts of high and low frequencies. Depending on the application at hand, this process of dividing the low frequency components is continued an erratic number of times [4-5, 12].

Singular Value Decomposition (SVD):

SVD is an image steganography technique designed to inspect images in matrices form. While applying SVD to an image, a given matrix M is disintegrated into three matrices such that, $M=USV^T$ where U and V are matrices in orthogonal order. Also $U^TU=I$, $V^TV=I$, where I is an identity matrix. S matrix is called as singular equivalent of M which is a matrix in the diagonal position, the columns of U refers to left singular vectors of M and the columns of V are called the right singular vectors of M. This technique of decomposing an image is avowed as singular value decomposition (SVD) of a matrix M. Nesting a stego image in the S matrix offers more robustness against attacks as compared to other orthogonal matrices of SVD. Hence customarily, the stego image is ingrained in the singular matrix [8, 13].

Discrete Fourier Transform (DFT):

In this transform, the image is split into two matrices-one for amplitude and one for phase. The phase matrix contains most of the quality part of the image. Therefore to make the system more robust against various attacks, secret information is embedded in the phase matrix [17].

CONCLUSION

This paper presents a survey about Steganography, its mediums, Image Steganography, uses and various Image Steganography schemes available. Albeit only some of the image steganographic techniques in spatial and frequency domain were conferred in this paper, there exists a broad collection of advents to conceal information in images. Where one technique implies simple algorithm, the other provides improved robustness. So, a designer to decide on which steganographic algorithm to work on, one would have to decide on the type of application they want to use the algorithm for. In future papers we will provide more detailed survey about some of the frequency domain techniques for image steganography, progressively, our proposal algorithm.

REFERENCES

[1] T. Morkel, J.H.P. Eloff, M.S. Olivier, 'An Overview Of Image Steganography', Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria, 0002, Pretoria, South Africa

[2] Muhalim Mohamed Amin, Subariah Ibrahim, Mazleena Salleh, Mohd Rozi Katmin, 'Information Hiding Using Steganography', & Department of Computer System Communication, Universiti Teknologi Malaysia

[3] Mehdi Hussain and Mureed Hussain, 'A Survey of Image Steganography Techniques', International Journal of Advanced Science and Technology Vol. 54, May, 2013

[4] Vijay Kumar, Dinesh Kumar, 'Performance Evaluation of DWT Based Image Steganography', 978-1-4244-4791-6/10/$25.00_c 2010 IEEE

[5] Ali Al-Ataby and Fawzi Al-Naima, 'A Modified High Capacity Image Steganography Technique Based on Wavelet Transform', Department of Electrical Engineering and Electronics, University of Liverpool, UK Department of Computer Engineering, Nahrain University, Iraq

[6] Weiqi Luo, Member, IEEE, Fangjun Huang, Member, IEEE, and Jiwu Huang, Senior Member, IEEE, 'Edge Adaptive Image Steganography Based on LSB Matching Revisited', IEEE Transactions on Information Forensics And Security, Vol. 5, No. 2, June 2010

[7] Rosziati Ibrahim and Teoh Suk Kuan, 'Steganography Algorithm to Hide Secret Message inside an Image', Faculty of Computer Science and Information Technology, University Tun Hussein Onn Malaysia (UTHM), Batu Pahat 86400, Johor, Malaysia

[8] K Suresh Babu, K B Raja, Uma Maheshwar Rao K, Rashmi K A, Venugopal K R, L M Patnaik, 'Robust and High Capacity Image Steganography using SVD', IET-UK International Conference on Information and Communication Technology in Electrical Sciences

[9] Ms.G.S.Sravanthi, Mrs.B.Sunitha Devi, S.M.Riyazoddin, M.Janga Reddy, 'A Spatial Domain Image Steganography Technique Based on Plane Bit Substitution Method', Global Journal of Computer Science and Technology Graphics & Vision

[10] Babloo Saha and Shuchi Sharma, 'Steganographic Techniques of Data Hiding using Digital Images', Defence Science Journal, Vol. 62, No. 1, January 2012

[11] Gurmeet Kaur, Aarti Kochhar, 'A Steganography Implementation based on LSB & DCT', International Journal for Science and Emerging Technologies with Latest Trends, 2250-3641" 4(1): 35-41 (2012)

[12] H S Manjunatha Reddy, K B Raja, 'High Capacity And Security Steganography Using Discrete Wavelet Transform'

[13] V.Santhi Member, IACSIT, Prof. Arunkumar Thangavelu, 'DC Coefficients Based Watermarking Technique for color Images Using Singular Value Decomposition', International Journal of Computer and Electrical Engineering, Vol.3, No.1, February, 2011

[14] S. M. M. Karim, M. S. Rahman, and M.I. Hossain, 'A New Approach for LSB Based Image Steganography using Secret Key', 14th International Conference on Computer and Information Technology (ICCIT),pp.286-291,March2012,DOI:10.1109/ICCITechn.2011.6164800

[15] Gutta Sadhana, 'Strengthening the Security of Information using Steganography', International Journal of Computer Science and Information Technology, Research Vol. 2, Issue 1, pp: (27-35), Month: January-March 2014

[16] Blossom Kaur1, Amandeep Kaur2, Jasdeep Singh, 'Steganographic Approach For Hiding Image In DCT Domain', International Journal Of Advances In Engineering & Technology, July 2011

[17] Inderjit Singh, Sunil Khullar, Dr. S.C. Laroiya, 'DFT Based Image Enhancement and Steganography', International Journal of Computer Science and Communication Engineering, Volume 2 Issue 1