Analysis of Image Steganography Methods

[1]Rakhi, [2]Dr. Seema Malik, [3]Seema Jain

[1,2,3]Assistant Professor
Department of Electronics and Communication Engineering
HMRITM, GGSIPU, Delhi, India

***Abstract*: In the changing geopolitical scenario, Digital steganography becomes all the way more important, be it for citizens for expressing their dissent or for countries competing against each other in the world order. Steganography has become an important tool and is going to stay. Steganography is a technique of data hiding in which we hide the message content as well as its existence. Steganography uses different type of media i.e. audio, video, images as cover file to hide the data. In this paper, we discuss about different type of image steganography methods.**

Index Terms: **Steganography, LSB, PVD, DWT, DFT.**

I.INTRODUCTION

Present scenario has compelled us for digitizing every service. For this information security becomes the main concern. To resolve this problem, Steganography emerges as one of the pre-eminent data hiding techniques because of its unique features such as robustness, undetectability, invisibility and capacity. To keep the data confidential, cover file is the medium in which data is embedded and hides the presence of it. In this paper, we analyze different Image Steganography techniques in which digital images are used as cover files. Data hiding in skin tone region of the image provides an excellence in Image Steganography. This method is performed by using DWT. Data hiding is done in such a way that the difference of cover image and stego image becomes inconspicuous. We use PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error) to determine the quality of stego image.

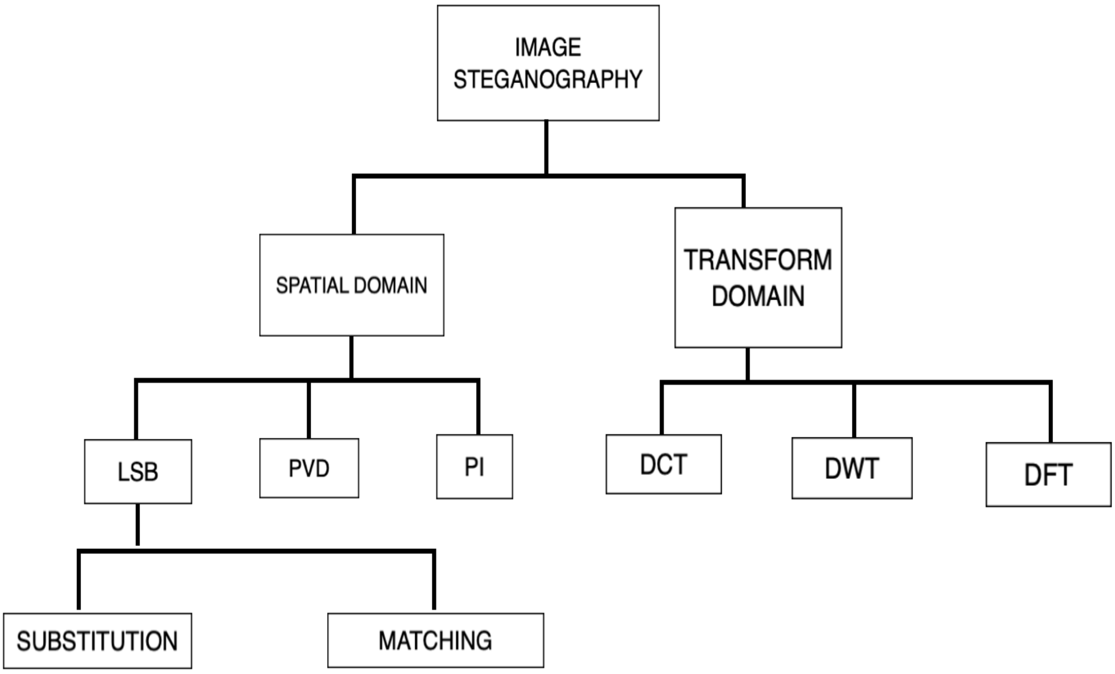

Fig.1. Flow Chart of Image Steganography Methods

II.IMAGE STEGANOGRAPHY METHODS

Spatial Domain Image Steganography

LSB Steganography- This steganography method is easy to implement and mostly used for data hiding. This method is of two types i.e., LSB Substitution and LSB Matching. In LSB Substitution, LSB of each selected pixel is substituted by a bit from confidential message.[1] In LSB Matching if the bit changes, ±1 is added to pixel value and has no effect on confidential message. Extraction of confidential message is same for both LSB Substitution and LSB Matching. Luon Ching Lin [2] proposed a scheme of data hiding in spatial domain with tolerance of distortion.

Pixel Indicator- In Pixel Indicator technique, RGB images are used as cover media. This technique chooses one channel from RGB which has sequential criteria i.e., RGB, RBG, GBR, GRB, BRG, BGR and embeds the confidential data into two least significant bits of this channel.[3]

Pixel Value Differencing- This is an efficient technique used for gray valued images. [4] In this method the size of confidential data bits can be calculated by the difference of two consecutive pixels in cover image. To embed the confidential data, cover image is partitioned into non-overlapping blocks of two consecutive pixels. In this method, there is no need to refer to the original cover image for extraction of confidential message.

Spread Spectrum- In this technique, the confidential message transmits below the noise level for any given frequency. Spread spectrum method uses cover image as noise or add pseudo noise to cover image. If cover image is used as noise, then single value is added to cover image and this value must be transmitted below noise level. In pseudo noise, the confidential data is spread throughout the cover image and it becomes difficult to detect. [5] Here two techniques are used, one is DSSS (Direct Sequence Spread Spectrum) and another is FHSS (Frequency Hopping Spread Spectrum). DSSS is used when subcover images are tiles and FHSS is used when subcover images consist of separate points distributed over the cover image.

Transform Domain Image Steganography

Due to consideration of robustness in data hiding techniques, frequency domain becomes more attractive. Here, sender transform the cover image into frequency domain coefficient before embedding confidential data into it [6]. In this technique, different frequency bands of cover are used to embed confidential data. The middle frequency band provides excellent location for data hiding. Transform domain is restricted with low embedding capacity.

Using DCT (Discrete Cosine Transform)- In this method, only JPEG images are used as most of the images are taken or stored with JPEG format. Here JPEG images are resized and their block boundaries are detected by applying 8x8 block DCT to input image pixels and analyze high frequency coefficient for them [7]. The boundaries of JPEG block and DCT block are different.

Using DWT (Discrete Wavelet Transform)- Wavelets are used because they separate the high frequency and low frequency information pixel on a pixel-by-pixel basis. This method consists of two operations, one in horizontal direction and another in vertical direction. As a result of this, the image is divided into four sub-parts i.e., LL, LH, HL, HH. Now select the sub-band to embed the confidential data [8]. The LL sub-band is low frequency part and very similar to original image. DWT gives better performance than DCT.

Using DFT (Discrete Fourier Transform)- In this technique, the length of confidential message is calculated and converted into ASCII format. Then the cover image is transformed from spatial domain to frequency domain using DFT. As we know, DFT has real and imaginary parts, so we hide confidential data into real part of Fourier Transform only.

Adaptive Steganography

This steganography method is a combination of Spatial Domain and Transform Domain. This technique is also known as Statistics-aware Embedding and Masking. Statistics decide the changes in the image. Image Statistical Characteristics are used to deal with its frequency transmitted coefficient. The main objective of this method is random adaptive selection of pixel. This method is mainly used for exploited images.

III.CONCLUSION

In this paper we approach towards the general idea about Image Steganography techniques that have the literature of last few years. All techniques satisfy the data hiding factors like robustness, undetectability and embedding capacity but still they have some limitations. Steganography as a technical advancement has bright prospect and we shall not be amazed to see it been used on wide scale in the times to come.

IV.ACKNOWLEDGEMENT

We are extremely grateful to previous works done in the sphere of steganography that acted as a precedent. Steganography is a powerful tool with wide ranging applications that hold the capacity to impact our life in big way. We believe our work would be of help and provide insight into new findings on the subject of steganography in coming times.

REFERENCES

[1] Xiao Yi Yu, Aiming Wang, “Revisit LSB Matching”, 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing 2010 IEEE DOI 10.1109/IIHMSP.2010.105

[2] L-C. Lin, “Hiding Data in Spatial Domain with Distortion Tolerance”, Computer Standard & Interfaces 31, pp. 458-464, (2009).

[3] Adnan Gutub,Mahmoud, Ankeer,Muhammad Abu- Ghalioun, Abdulrahman Shaheen, and Aleem Alvi,“Pixel indicator high capacity technique for RGB image based Steganography”, WoSPA 2008 – 5th IEEE International Workshop on Signal Processing and its Applications, University of Sharjah, Sharjah, U.A.E. 18 – 20 March.

[4] D. C. Wu and W. H. Tsai, “A steganographic method for images by pixel-value differencing”, Pattern Recognition Letters, vol. 24, no. 9- 10, pp. 1613-1626, 2003.

[5] L.M. Marvel, C.G. Boncelet Jr., C.T. Retter, “Spread Spectrum Image Steganography.” IEEE Trans. image processing 8(8), pp. 1075-1083. [Apr., 2011].

[6] Chang, C. C.,Chen, T.S and Chung, L. Z.,“A steganographic method based upon JPEG and quantization table modification”, Information Sciences, vol.[4], pp. 123-138(2002).

[7] Toshihiko Yamasaki,Tomoaki Matsunami and Kiyoharu Aizawa, “Detecting resized JPEG images by analyzing high frequency elements in DCT coefficients” 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing 2010 IEEE DOI 10.1109/IIHMSP.2010.144.

[8] Sunita Barve, Uma Nagaraj and Rohit Gulabani, “Efficient and Secure Biometric Image Stegnography using Discrete Wavelet Transform”, International Journal of Computer Science & Communication Networks, Vol 1(1), September-October 2011.

[9] Juned Ahmed Mazumder, K.Hemachandran, “Study of Image steganography using LSB, DFT and DWT”, International Journal of Computers & Technology Vol 11, No.5