A Review on Steganography

Ramandeep kaur Brar* and Ankit Sharma

Baba Farid College of Engineering and Technology
Bathinda, Punjab, India
*Email: brar.raman111@gmail.com

Abstract— **Steganography is the carry out of concealing the communication subsistence by thrashing the traveled message in cover media. This paper aims to study Discrete Cosine Transform (DCT) based steganography Using DC components for hiding secret bits serially in Least significant Bits (LSBs) (1-LSB & 2-LSB). The planned steganographic process can provide a high information hiding capacity and effectively increase the security.**

Keywords- ***Steganography, steganography techniques: spatial domain technique, frequency domain technique***

I. INTRODUCION

Steganography is the ability and science of thrashing the reality of the communication, i.e., it hides the covert message inside the other medium like images, audio, video, text, etc. Steganography word is consequent from Greek word steganos, which means covered and graphia means writing [1]. The Internet user's effect has upraised the possible of their information changed or lost by a moderator. Steganography is one of the solutions for securing data from any feasible risk [2] . There are two frequent techniques which are used for information hiding systems i.e., stegnography and watermarking (see fig1), steganography is useful in confidential communication, wherein watermarking a visible or an invisible spot that is fixed [2].

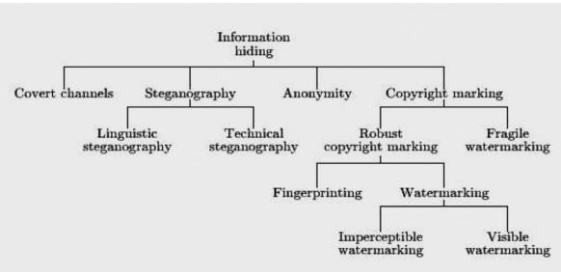

Fig.1. Disciplines of information hiding[2]

Cryptography was formed as a technique for securing the privacy of communication and many diverse methods have been developed to encrypt and decrypt data in order to maintain the message covert. Steganography differs from cryptography in the common sense that where cryptography focuses on charge the contents of a message secret, steganography focuses on keeping the subsistence of a message covert. Earlier used spatial domain methods of steganography are based on Least Significant Bit (LSB) substitution which giver better PSNR result but fail to prevent attacks and are easily detected so a need arises for alternative methods for steganography [3]. We choose an image as the media to screen the secret message in. This image is known as cover-image. With the secret message, the cover image is fixed in it is known as the stego-image. For an image, the image feature refers to the feature of the stegoimage, and the message capability concerns the question of how many secret messages can be fixed in the stego-image. If a stegoimage have excellent image quality, it can evade being supposed during transmission of hidden messages [4].

II. STEGANOGRAPHY TECHNIQUES

There are various steganography techniques:

a) Spatial domain techniques
b) Frequency or transformation domain technique

a) Spatial domain techniques

In spatial domain steganography techniques, some bits are changed directly for hiding the data in the image pixel values [5]. They offer a fine suppression while giving a big capability of the embedded data and simple inquiry. As a result, these techniques are greatly utilized in steganographic applications. They propose high aptitude, but do not afford robustness against easy modifications and are simple to identify. Least significant bit method are mostly used in this category [2-5].

Least Significant Bit (LSB)

LSB is a frequent and straightforward approach for embedding information in a cover file. Digital images used as cover file which are of two types i.e., 24-bit images and 8-bit images. By using 24-bit images, we can embed three bits of information in each pixel. By using 8-bit images, one bit of information can be secreted into images. After apply

the LSB algorithm the image obtained having secret message is called stego-image. LSB technique replaces the least significant bit of the pixel with the information to be hidden. Since LSB is replaced there is no outcome on cover image and hence unplanned user will not get the idea that some message is hidden behind the image. However a tiny change in level of concentration of original and modified pixel, but it cannot be detected visually [5].

Pixels: (00100111 11101011 11001010)
(00100111 11011000 10101001)
(11001000 00110111 11011001)
A: 010100111
Result: (00100110 11101011 11001010)
(00100111 11011000 10101000)
(11001001 00110111 11011001)

The main benefit of LSB method is straightforward to implement and high message payload and there is less chance of degradation of quality of original image. The demerits of LSB are that the information can be easily extracted or damaged by simple attacks and it is less robust, helpless to image manipulation.

Pixel Value Differencing (PVD)

In Pixel Value Differencing method, gray scale image is used as a cover image with a long bit-stream as the secret data. It was originally proposed to cover secret information into 256 gray valued images. The method is based on the piece of information that human eyes can easily examine small changes in the horizontal areas but they cannot observe moderately larger changes at the edge areas in the images. PVD uses the divergence between the pixel and its neighbor to conclude the number of fixed bits. The larger the difference amount is, the more secret bits can be fixed into the cover image. It scans the image in a zigzag manner which starting from the upper left corner. Then, it basically divides the cover image into the number of blocks where each block consists of two successive non-overlapping pixels. The data is fixed mostly in the edge areas because the changes of the pixel values are further easily noticed by human eyes.

Histogram Shifting Method

Histograms are basically used for graphical illustration of image. For each part of the image it plots the pixel. A histogram is very useful to identify pixel distribution, density of colors as well as tonal distribution. In histogram the highest value is known as maxima and the lowest value is known as minima. When the pixel value is customized for embedding process it should not cross the minima and maxima limit. Numerous histogram shifting techniques are improved by dividing the cover image into blocks to generate a respective peak for each block which provides more hiding capacity into the multiple blocks [5].

c)Frequency or transformation Domain Technique

Transformation domain methods hides message in the significant areas of the cover image which makes them more forceful against various image processing operations like compression, cropping and enhancement [2-5]. Transformation domain techniques are as follows:

III. DISCRETE COSINE TRANSFORM

Discrete Cosine Transform is the mostly common algorithm utilized in image steganography as a standard for JPEG image format and image compression (see Fig. 2) [2]. The DCT transforms the image from spatial to frequency domain and separates the image into spectral sub-bands with respect to visual quality of the image, which are low, middle and high frequency components as shown in fig.3. Here FL and FH is used to denote the lowest frequency components and higher frequency components respectively. FM is used as embedding region to provide additional resistance to lossy compression techniques, while avoiding significant modification of the cover image [5].

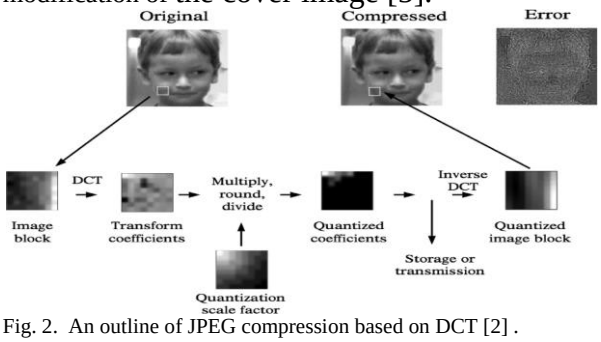

Fig. 2. An outline of JPEG compression based on DCT [2] .

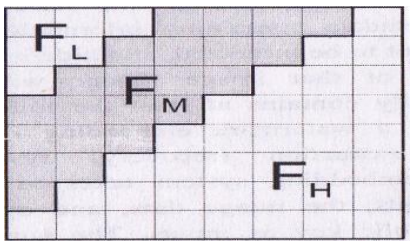

Fig. 3. DCT Regions[5]

In Discrete Cosine Transformation, the JPEG image format uses discrete cosine transform for each color component to transform successive 8 x 8 pixel blocks of the image into 64 DCT coefficients each.

IV. DISCRETE WAVELET TRANSFORM (DWT)

The Discrete Wavelet Transformation Technique is the very fresh thought in the applications of the wavelets [5]. It is utilized to transform the signals in time domain to the frequency domain. After transformation, it will construct coefficients set approved in a manner which allows the signal spectral analysis and the signal spectrum position in time. DWT is a tool of cutting edge in the image compression area. Wavelet algorithms provide essential

enhancements in the quality of images at a large ratio of compression. DWT is designed by consecutive low and high pass filters. Image signals decompose it into four sub-bands (see Fig. 4) [2].

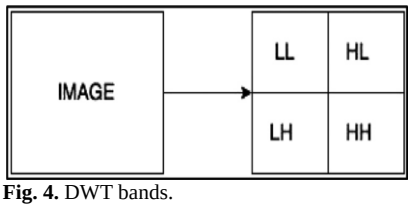

Fig. 4. DWT bands.

V. CONCLUSION

In this paper we focus our distress in image because of it's widely used in Internet and also in mobile system. Improved LSB algorithm can straightforwardly be implemented and do not visually disgrace the image to the point of being noticeable. It would appear that LSB is fine algorithm of steganography due to its security. Using enhanced LSB algorithm we can swap secret messages over public channel in a safe way.

REFERENCES

1. Deepika Bansal, Rita Chhikara,'An Improved DCT based Steganography Technique',International Journal of Computer Applications (0975 – 8887) Volume 102– No.14, September 2014.
2. Sahar A. El_Rahman a , b,'A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information',[m3Gsc; September 19, 2016;17:29] Computers and Electrical Engineering 0 0 0 (2016) 1–20.
3. Akanksha Kaushal, Vineeta Chaudhary, 'Secured Image Steganography using Different Transform Domain', International Journal of Computer Applications (0975 – 8887) Volume 77– No.2, September 2013.
4. Chin-Chen Chang a,*, Tung-Shou Chen b,1, Lou-Zo Chung a,'A steganographic method based upon JPE and quantization table modification', Information Sciences 141 (2002) 123–138.
5. Amritpal Singh1 , Satinder Jeet Singh2,'An Overview of Image Steganography Techniques', International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 7 July, 2014 Page No. 7341-7345.