Analysis of Wavelet Based Digital Image Steganography using Hybrid Technique in Frequency Domain

Kirti D. Nagpal
Research Scholar, Dept. of Electronics and Communication,
Agnihotri College of Engineering (ACE),
Wardha, India
kirtinagpal.engr@gmail.com

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

***Abstract*—** Steganography intends to communicate securely in a completely indistinguishable manner and to avoid sneaking skepticism to the transmission of a hidden data. The steganography technique aspires not to keep others from distinguishing the hidden information, but it is to avert others from thinking that the information even exists. Steganography plays a vital role in the field of information hiding. It is used in wide range of applications such as internet security, substantiation, copyright protection and information assurance, etc. Numerous steganography techniques that embed hidden messages in multimedia objects have been proffered. There exist numerous techniques for hiding secret information or messages in images in such a way that the modifications implied to the image are perceptually indiscernible. This paper proposes the evaluation of few techniques of the image steganography in frequency domain. The implemented techniques are image steganography based on Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT) and Singular Valued Decomposition (SVD). The performance evaluation can be done in terms their ability to endure attacks, by the evaluation of Peak Signal to Noise Ratio (PSNR), Normalization Coefficient (NC), Mean Square Error (MSE).

***Keywords*-** *Image Steganography, Watermark, Hybrid, DWT, DCT, SVD*

*****

I. Introduction

Steganography word is originated from two Greek key words- *Stego* and *Graphy*. Stego pertain to concealed or covered and Graphy means writing. So Steganography essentially means concealed writing. Steganography deals with embedding information into the host data such that it remains totally transparent or imperceptible. The Steganography aims to hide information in a cover data in a manner that unintended person cannot detect the presence of hidden information. The major requirement of steganography is such that the secret information should be deep seated in such a way that this should neither be detectable nor removable even after many specious or innoxious attempts. The technique of steganography has its roots from ancient times. Nowadays, the steganography can be carried out through various carriers like Text, Audio, Video, Image etc. Because of high frequency use of digital images on the internet, it is widely accomplished with digital images. So in this paper, digital images are used as medium for implementing Steganography techniques in frequency domain. Steganography differs from Watermarking technique in a manner that watermarking aims to not removing the embedded information from the host data by the eavesdropper, while steganography focuses on making the embedded information totally undetectable from an meddler person [1] [2].

II. Applications of Image Steganography

Image Steganography can be beneficial for ample of areas essentially, for smart cards used for identification in numerous companies, institutes or even in government sectors, where some peculiar information is embedded in the Photostat for copyright purpose, securing fingerprint information, in defense systems for secure transmission of covert data in army and intelligence bureaus, to make mobile banking more secure. Image Steganography can also be implied in medical imaging, where patient's analytic information is encapsulated within image accommodating protection of information and abbreviating the cost and time required for the transmission. It is also helpful in networked balloting system to make the online election protected and robust against a variety of deceptive acts, in countries where cryptography is restricted for data hiding, in alter proofing to disclose or avert the illegitimate adaptations and other variety of applications [2][3].

III. Classification of Image Steganography

Depending on the technique employed for embedding stego image into the cover image, the image steganography can be classified into two domains: Image Domain and the Transform Domain [1]. Image domain also popular as spatial domain techniques embed messages directly in the intensity of the pixels, while for transform, also known as frequency domain, images are initially transformed and afterwards the message is embedded in the image. There are many steganography techniques which are broadly classified depending upon the domain used for embedding as spatial domain and Frequency domain.

A. Spatial Domain Methods:

The spatial domain [1] [2] [3] is a technique based on the normal image space, in which an alteration in position in Intensity (I) directly corresponds to a change in position in space. Distances in I (in pixels) correspond to real distances in space. This concept is used most often when discussing the frequency with which image values change, that is, over how many pixels does a cycle of periodically repeating intensity variations occur. One would refer to the number of pixels over which a pattern repeats (its periodicity) in the spatial domain. Mostly Least Significant bit (LSB) method is used that hides a secret message in the LSBs of pixel values without introducing many perceptible distortions. It takes advantage of the fact that changes in the LSB value are erratic to human eyes.

In Spatial domain, cover-image is first crumbled into bits planes and then secret data bits are substituted at the place of least significant bit (LSB) of the bits planes. Spatial domain techniques offers advantages such as indiscernibly of the concealed data, maximizing capacity of embedded data, ease of implementation and. The major drawback is its susceptibility to various simple statistical analysis methods.

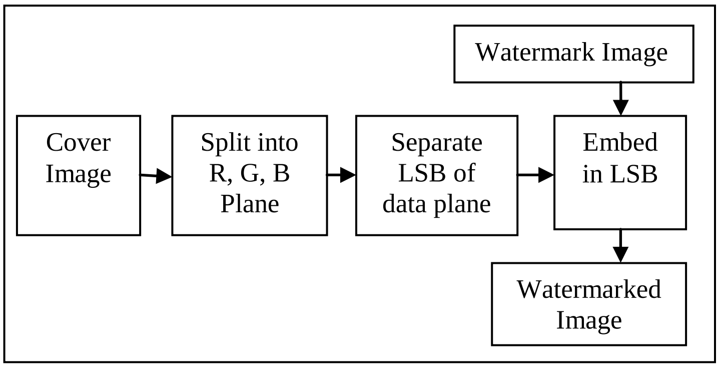

Figure I. Image Steganography in Spatial Domain

B. Transform Domain Methods:

The product of high quality watermarked image is obtained by first transforming the original image into the frequency domain by the use of different transforms such as Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) or Discrete Wavelet transforms (DWT) etc. With these techniques, the marks are not added to the intensities of the image as in the spatial domain based techniques but to the values of its transform coefficients. Then inverse transforming the marked coefficients forms the watermarked image. Transform domain techniques offers advantage of higher level of robustness against simple statistical analysis as compared to spatial domain based techniques. The use of frequency based transforms allows the direct understanding of the content of the image; therefore, characteristics of the human visual system (HVS) can be taken into account more easily when it is time to decide the intensity and position of the watermarks to be applied to a given image.

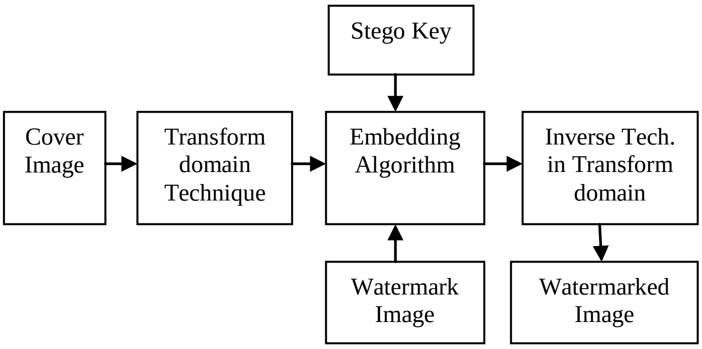

Figure 2. Image Steganography in Transform Domain

There exist numerous techniques to implement image steganography in transform domain. In this paper, the techniques that are discussed are:

1. Discrete Wavelet transformation technique (DWT)
2. Discrete cosine transformation technique (DCT)
3. Singular Value Decomposition (SVD)

1. Discrete Wavelet transformation technique (DWT):

A Discrete Wavelet Transform (DWT) [4] [5] is a transform in frequency domain in which discrete time signal is transformed to a discrete wavelet representation by sampling the wavelets discretely. Applying DWT on two-dimensional signal segregates the image in two levels of frequency components- High frequency and low frequency components. The key information about the original image is contained in the low frequency components which are approximate coefficients and the additional information about the image is covered by the high frequency components holding the detailed coefficients of the image. These detailed coefficients can be acclimated to embed secret image.

The 2-D discrete wavelet transform (DWT) transforms a discrete time signal to a discrete wavelet representation. While embedding the secret image into the cover image, the cover image is first converted into wavelet domain. After the conversion, high frequency components are manipulated to embed secret image. This secret image is further retrieved in extraction procedure to serve the purpose of steganography. Embedding procedure disintegrates an image into sub-images having detailed information and some alikeness. Two dimensional DWT (2D-DWT) partitions the image in four frequency bands. The first band referred as LL band is the low frequency band existing both in horizontal and vertical direction. The second band (LH) contains the low frequencies in horizontal direction and high frequencies in vertical direction. The third band (HL) contains the high frequencies in horizontal direction and low frequencies in vertical direction. The forth band (HH) contains the high frequencies both in horizontal and vertical direction. The LL band represents the approximation of the image and is the most significant band as it carries most of the image information. This process is continued an arbitrary number of times, which is usually determined by the application at hand. The decomposition of an image into these bands is depicted in figure 3.

LL	HL
LH	HH

Figure 3. Frequency Bands in One dimensional Discrete Wavelet Transform

The human visual system is less sensitive to the small changes in edges and textures of an image. In DWT Technique, the high frequency sub bands, (HH, HL, and LH) usually contain the edges and textures. Simultaneously, human eye is sensitive to the changes in the smooth parts of an image that are covered by the LL band. Therefore based on this fact stego image is usually embedded in any of the high-resolution detail bands. The technique of embedding stego image in these regions increases the robustness of the stego image.

2. Discrete cosine transformation technique (DCT)

The image is first divided into square blocks of size 8x8 for DCT [6] computation. Out of the 12 predetermined pairs, a pair of mid frequency coefficients is chosen for modification. The DCT breaks the image into different frequency bands, which makes it easier to embed watermarking information into the middle frequency bands of the image. The middle frequency bands are chosen such that they avoid the most visual important parts of the image (low frequencies) without over-exposing themselves to removal through compression and noise attacks.

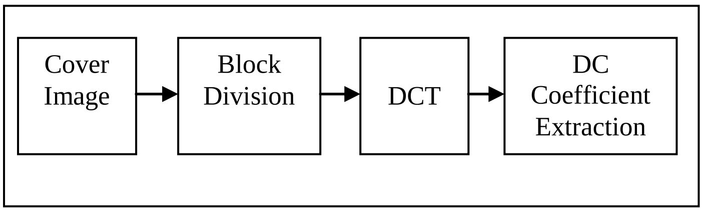

Figure 4. Discrete Cosine Transform

3. Singular Value Decomposition (SVD):

Singular Value Decomposition [7] [8] is used to decompose any rectangular real or complex matrix. The three main properties of SVD from the view point of image processing applications are:

1. The singular values of an image have very good stability, such that when an image is disrupted at a small level, its singular values do not alter greatly.
2. Each Singular value specifies the luminance of an image layer while the corresponding pair of singular vectors specifies the geometry of the image.
3. Singular values represent intrinsic algebraic properties.

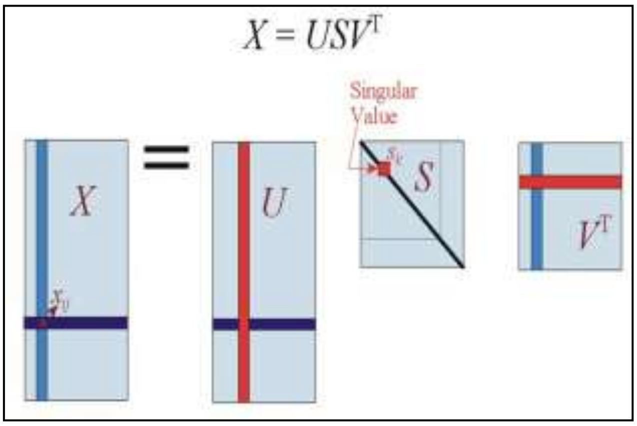

Figure 5. Singular Value Decomposition Transform

Advantages:

1) SVD is a stable and effective method to split the system into a set of linearly independent components, each of them is carrying own data (information) to contribute to systems. Thus, both rank of the problem and subspace orientation can be determined.

2) SVD can be well adapted to the statistical variation of the image since provides a good compression ratio.

IV. Performance Evaluation Characteristics

The performance of the above mentioned techniques can be evaluated on the basis of certain parameters such as Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Normalization Coefficient (NC) etc [5].

A) Peak Signal to Noise Ratio (PSNR):

The PSNR is most commonly used as a measure of quality of reconstruction of the embedded image. The signal in this case is nothing but the original data, and noise is the error introduced by compression. It is most easily defined via the Mean Squared Error (MSE) which for two m×n monochrome images *I* and *K* where one of the images is considered a noisy approximation of the other is given by:

$$\mathrm{MSE} = \frac{1}{\mathrm{m} * \mathrm{n}} \sum_{\mathrm{i}=0}^{\mathrm{m}-1} \sum_{\mathrm{j}=0}^{\mathrm{n}-1} [\mathrm{I}(\mathrm{i},\mathrm{j}) - \mathrm{K}(\mathrm{i},\mathrm{j})]^2$$

The PSNR is defined as the ratio of the maximum signal to noise in the stego embedded image. It is given by the expression:

$$\mathrm{PSNR} = 10 * \log_{10}\left(\frac{\mathrm{MAX}^2}{\mathrm{MSE}}\right) = 20.\log_{10}(\mathrm{MAX}) - 10.\log_{10}(\mathrm{MSE})$$

Here, MAX is the maximum possible pixel value of the image.

B) Normalized Correlation (NC):

Normalized Correlation is used to measure the robustness of the watermark. For numerous applications of image-processing, the images can be first normalized in cases where brightness of the image and template can vary due to exposure and lighting conditions,. This is normally done at every step by subtracting the mean and dividing by the standard deviation. That is, the normalized correlation of a template, w_1(i,j) with a sub image w_2(i,j) is

$$NC = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} w_1(i,j) * \, w_2(i,j)}{\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n} w_1^2(i,j)} \, \sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n} w_2^2(i,j)}}$$

Where m and n are the number of pixels in w_1(i,j) and w_2(i,j). In functional analysis terms, this can be thought of as the dot. Thus, if w_1 and w_2 are real matrices, their normalized cross-correlation equals the cosine of the angle between the two unit vectors, being thus 1 if and only if one vector equals second multiplied by a positive scalar.

V. Proposed Algorithm

The steganography techniques can be applied on individual basis or some of the techniques can be combined and a hybrid class of steganography technique can be built. DWT, DCT and SVD techniques can be combined to increase the robustness and capacity of the algorithm by selecting significant coefficients and number of color channels [9]. Proposed algorithm combines the properties of DWT, DCT and SVD techniques and forms a hybrid technique for implementing image steganography on color as well as black and white image. The procedure for embedding and extracting the watermark is given below.

A. *Watermark Embedding Algorithm:*

1. Read the cover image and decompose it into RGB color channels.
2. Apply DWT and separate into various frequency bands.
3. Select the frequency band and divide it into smaller blocks of size 4x4.
4. Apply DCT to each 4x4 block.
5. Extract the DC coefficients from each block, and form a new matrix C.
6. Apply SVD on matrix C, $C = U * S_{IMG} * V^T$
7. Read the watermark image (W) and decompose it using SVD technique.

$$U_W S_W V_W = SVD\ (W)$$

8. Modify the singular values of ‘C’ matrix (cover image) by using the singular values of watermark.

$$S1= S_{IMG} + \alpha * S_W$$

9. Combine the modified singular values with the orthogonal matrices of ‘C’,

$$S2 = U * S1 * V^T$$

10. Replace the original DC matrix coefficients with the modified new components.
11. Apply inverse DCT and then inverse DWT.
12. Recombine the RGB components and the watermarked image is formed.

B. *Watermark Extracting Algorithm:*

1. Convert the watermarked image into RGB color spaces.
2. Apply DWT to decompose the cover image in which watermark is hidden.
3. Divide middle frequency band into smaller 4x4 blocks and apply DCT to each block.
4. Extract the DC coefficients from every DCT transformed blocks and construct a new matrix C, which could be decomposed by SVD technique,

$$C = U* S* V^T$$

5. Extract the singular values from C matrix, and then compare the difference between the watermarked singular values and host image singular values.
6. Combine the obtained singular values with the orthogonal matrices of watermark. The watermark is extracted.

VI. RESULTS

The implementation and simulation of Image Steganography using above mentioned algorithm have been done using MATLAB environment and their responses have been studied. The Graphical User Interface (GUI) has been designed to view a better interface with the user as shown in the figure 6. The algorithm is tested for color cover image as well as black and white version of the same cover image with name “HK” as the watermark. Resulting images obtained after embedding and extracting the watermark image from the HL band are shown in the GUI snapshot. The analogy on the Image Steganography to be applied on different bands (namely LL, LH, HL and HH) has been carried out based on their PSNR and NC values. The PSNR value (in dB) and Normalized Correlation values for watermarked image and extracted watermark image respectively measured for both black and white cover image and color image are tabulated in Table 1 and Table 2 respectively. It is found that extraction of the watermark image is better in HL band than other bands in terms of addition of noise while extracting the watermark from watermarked image.

TABLE I
MEASURED VALUES OF PSNR AND NC FOR BLACK AND WHITE COVER IMAGE

Parameter	LL	LH	HL	HH
PSNR	78.9612	65.3198	63.4325	53.1618
NC	0.8275	0.791563	0.9925	0.80427

TABLE II
MEASURED VALUES OF PSNR AND NC FOR COLOR COVER IMAGE

Parameter	LL	LH	HL	HH
PSNR	78.4228	64.8362	64.8238	52.7264
NC	0.8355	0.7685	0.99128	0.7930

REFERENCES

[1] Kirti D. Nagpal, Prof. D. S. Dabhade, “A Survey on Image Steganography & its Techniques in Spatial & Frequency Domain”, International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 3 Issue: 2, February 2015

[2] Asha Pathak, Vrushali Bhuyar, “Image Steganography and Steganalysis: A Survey”, International Journal of scientific research and management, Volume2, Issue 12

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

[4] Barnali Gupta Banik, Prof. Samir K. Bandyopadhyay, “A DWT Method for Image Steganography”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, June 2013

[5] Aayushi Verma, Rajshree Nolkha, Aishwarya Singh and Garima Jaiswal, “Implementation of Image Steganography Using 2-Level DWT Technique”, International Journal of

Computer Science and Business Informatics, Vol. 1, No. 1. MAY 2013

[6] Prof. Priya Pise, Prof. R M Goudar, "Watermarking of Images in Discrete Cosine transform", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 5, May 2013

[7] Andrews, Harry C., Patterson, C., III, 'Singular Value Decomposition (SVD) Image Coding', IEEE Transactions on Communications, (Volume: 24 , Issue: 4)

[8] Klema, V, Laub, A.J., 'The singular value decomposition: Its computation and some applications', Automatic Control, IEEE Transactions on (Volume:25 , Issue: 2)

[9] Manjusha Tikariha, Amar Kumar Dey, "Comparative Study on Hybrid Watermarking Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 6, June 2014

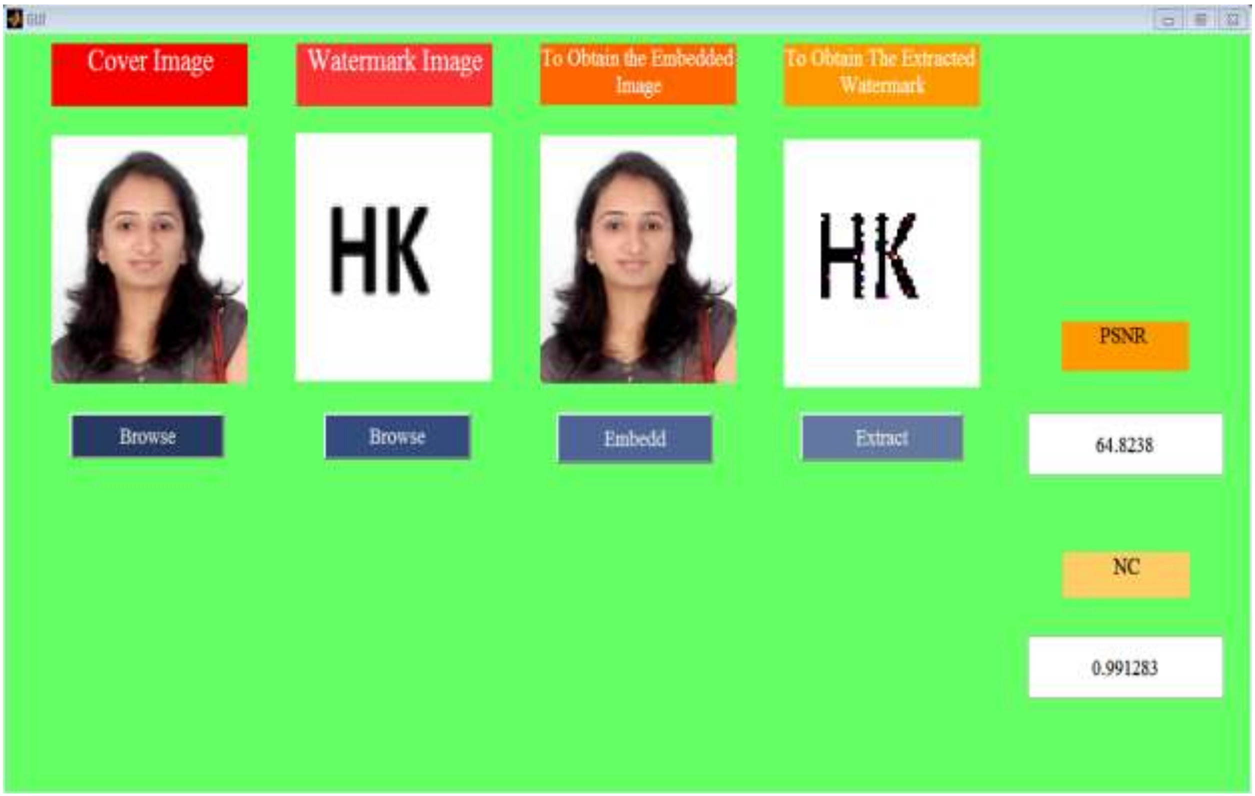

Figure 6. Graphical User Interface (GUI) showing the results of Image Steganography in HL Band for Color Cover Image