Multilevel Information Security in multimedia environment using Frequency domain transformation

[1]Prasenjit Maji, [2]Dipsha Nandy, [3]Moumita Pal
[1]Assistant Professor, [2]Student, [3]Assistant Professor
[1]Bengal College Of Engineering & Technology,
[2]JIS College Of Engineering,
[3]JIS College Of Engineering

Abstract - **Due to rapid advancement in communication Security has become real concern. Thus to fulfill this requirement the information should be protected in such a way so that its presence should not be felt by anyone except the receiver. Steganography restricts the access to the unauthorized users. This method considers any text, image, voice, video as cover image. This paper approaches towards securing information exchange over the internet using image processing. In this proposed method the technique wavelet transformation is used along with cryptography and Steganography, where information contained text file is hidden inside a video frame or image without causing any distortion in the quality of that. The frames are transformed by discrete wavelet transform, where both the frame with and without noise exist. The message is carefully hidden into the noisy channels of image. Reconstruction of the stego image is done by inverse DWT. After receiving the stego video it need to be transformed by DWT again for segregation. Lastly the extraction of secured information contained text file is done by the receiver. Due to multilevel encryption, the hidden information remains highly secured compared to other methods.**

keywords **- DWT, Steganography, Stego image, security .**

I. INTRODUCTION

Steganography has comprised from two Greek words which are steganos and graphein. The combined meaning is depicted as secured writing. Using this technique communication can be done between two or more people silently with each other by covering any secret message on a media cover. Here secret message is embedded within a covering media using the appropriate algorithm and the encoded stego file is then transmitted to the receiver. After the message is received by the recipient its is decoded by the same key and successful secured transmission is fulfilled. Due to increase in requirement of high speed, secured communication, more the need of various steganography algorithm evolves. In this regard our main intention is to send the message in secured way so that, except the receiver none can make it out. Hence without letting others, phenomenon of secret transmission is conceptualized as cryptography. Various parameters can be involved in measuring the performance of different algorithms those are used for this encryption process. These parameters can be stated as peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE). In addition to this imperceptibility of cover and stego image, robustness of embedded data and rate of maximized data embedding capacity is also taken into consideration. Technically there are various methods of securing data but most recent trends of utilizing these are mostly in the field of implementation in image processing. This procedure is performed by various operations on an image, in order to get an high quality image or to extract some needful information from it. It is a type of signal dispensation in which image is an input, like frames of a video or photograph and output may be image or characteristics associated with that image. Image Processing generally treats images as two dimensional signals while applying various signal processing and transformation methods to be applied upon them. Image processing has to undergo through the below mentioned processes for successful transmission. These specific processes can be stated as –

1. Visualization - Observe the objects that are not visible.
2. Image sharpening and restoration - To create a better image.
3. Image retrieval - Seek for the image of interest.
4. Measurement of pattern- Measures various objects in an image.
5. Image Recognition-Distinguish the objects in an image.

In brief the various information hiding process is classified as per their application field as shown in fig 1.

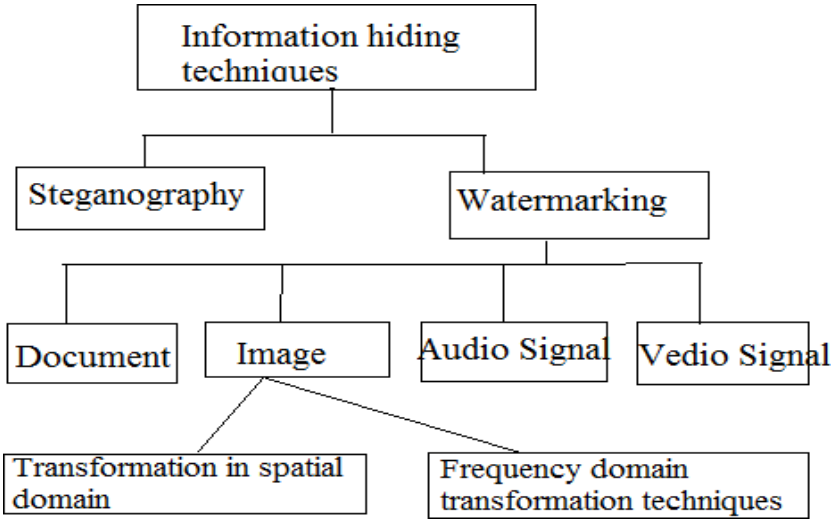


Figure.1: Classification of various information hiding techniques

Another rising research trends for nowadays is video Steganography, where hiding or embedding message in the video is like an art of hiding information. Hiding message in the video is another technique of hiding information that prevents the revealing of hiding messages. Video-based Steganography techniques are same like image based, its classified into spatial domain and frequency domain based methods .

Due to a pair of specific reasons video Steganography is used vastly. These can be expressed as: video consists of number of frames that carry information. Thus, to transfer large volume of information, video Steganography is utilized in large scale. In addition to this, as per the security concern, video Steganography is more secure as compared to Image Steganography

.

II. LITERATURE REVIEW

In spatial domain the unmodified secret image replaces the cover image. Involvement of LSB technique is mostly used in this transformation technique. In another way the gray cover image may be used for hiding the secret image. Here the cover image is divided into blocks of consecutive pixels and shows promising result compared to LSB technique. As a natural phenomenon, the further improvement in this regard has evolved a new approach of steganography in frequency domain. Due to transformation of image in frequency domain, data can be transmitted comparatively higher speed and more secured manner. Among various methods, shifting method by histogram analysis is truly accepted as extraction of existed frequency components from the cover image is quite possible in this case. Moreover, by reverse transformation process, frequency domain transformed image can again be transformed into spatial domain.

Po-Yueh Chen et al. [1] proposed a new steganography technique of embedding the secret image in frequency domain. Here segregation of the algorithm is done into two modes and 5 cases. Embedding of Secret messages are done by high frequency coefficients involving the transformation by Discrete Wavelet Transform. H S Manjunatha Reddy et al [2], proposed a high capacity and Secured Steganography using Discrete wavelet transform. The wavelet coefficients of both the cover and payload are fused into single image using embedding strength parameters alpha and beta. The cover image and payload are preprocessed to reduce the pixel range to ensure the payload is recovered accurately at the destination. This is observed that the capacity and security is increased with acceptable PSNR in the proposed algorithm.

Elham Ghasemi et al. [3] show the application of Wavelet Transform and Genetic Algorithm in a novel steganography scheme. They employ a genetic algorithm based mapping function to embed data in Discrete Wavelet Transform coefficients in 4x4 blocks on the cover image. The optimal pixel adjustment process is applied after embedding the message. Prabakaran Ganesan et al. [4]proposed a high secure steganography scheme hiding a 256×256 size gray secret image into a 512×512 size gray cover image with different combination of Discrete Wavelet Transform and Integer Wavelet Transform (IWT). Pixel Value Adjustment is first performed on cover image.

Hemalatha S. et al. [5] proposes a secure color image steganography technique to hide a secret image using the keys. The secret image is hidden by considering the three color components separately. The keys are generated using the corresponding color components and the keys are hidden in the respective color components of the cover image. Using the keys the secret image can also be extracted.

Preeti Chaturvedi and R. K. Bairwa. Et al. [6] have proposed a data hiding scheme that hides data into the integer wavelet coefficients of an image. Here a non blind watermarking scheme by taking 1D logistic chaos equation in DWT domain. Here, they have focused on the low frequency part to embed information.

III. METHODOLOGY

Discrete Wavelet Transform (DWT) is a mathematical tool for hierarchically decomposing an image. A discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled. As with other wavelet transforms, a key advantage it has over Fourier transforms is temporal resolution. It captures both frequency and location information [8]. It is useful for processing of non-stationary signals. Wavelet transform is based on small waves, called wavelets, of varying frequency and limited duration. Wavelet transform provides both frequency and spatial description of an image. Unlike

conventional Fourier transform, temporal information is retained in this transform process. Wavelets are created by translations and dilations of a fixed function called mother wavelet
Steganography and gives advantages of using DWT as against other transform. Wavelet transform is a time domain localized analysis method with the window's size fixed and forms convertible. There is quite good time differentiated rate in high frequency part of signals DWT transformed [9]. Also there is quite good frequency differentiated rate in its low frequency part. It can distil the information from signal effectively.

As shown in Fig.2, DWT is the most prominent information in the signal appears in high amplitudes and the less prominent information appears in very low amplitudes. Data compression can be achieved by discarding these low amplitudes. The wavelet transforms enables high compression ratios with good quality of reconstruction. The basic idea of discrete wavelet transform (DWT) in image process is to multi-differentiated decompose the image into sub-image of different spatial domain and independent frequency district [10]. After the original image has been DWT transformed, it is decomposed into 4 frequency districts which is one low-frequency district(LL) and three high-frequency districts(LH,HL,HH) Where, L represents low-pass filter, H represents high-pass filter.

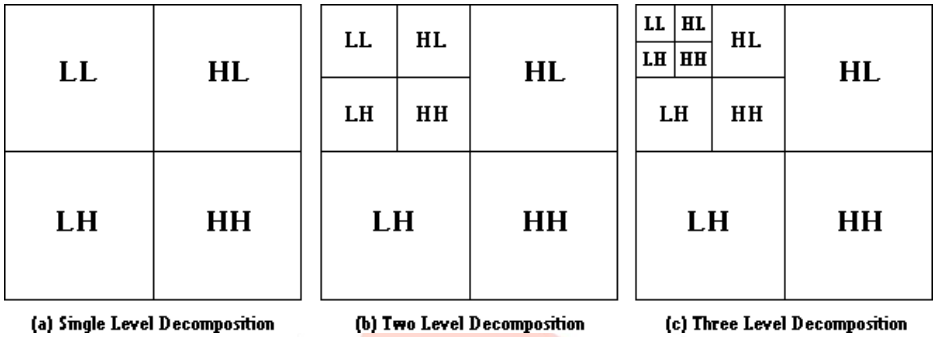
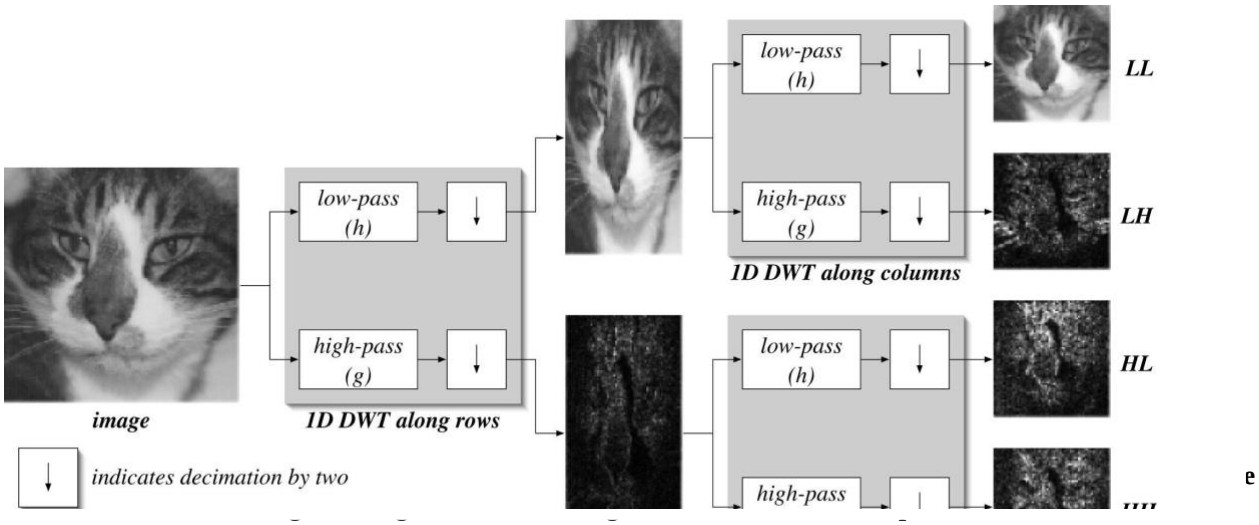


Figure.2: Decomposition of images/frames using DWT

A two-dimensional image after three-times DWT is decomposed. An original image can be decomposed of frequency districts of HL1, LH1, HH1. The low-frequency district information also can be decomposed into sub- level frequency district information of LL2, HL2, LH2 and HH2. By doing this the original image can be decomposed for n level wavelet transformation. The information of low frequency district is an image close to the original image. Most signal information of original image is in this frequency district. The frequency districts of LH, HL and HH respectively represents the level detail, the upright detail and the diagonal detail of the original image. According to the character of HVS, human eyes are sensitive to the change of smooth district of image, but not sensitive to the tiny change of edge, profile and streak. Therefore, it's hard to conscious that putting the watermarking signal into the big amplitude coefficient of high-frequency band of the image DWT transformed. Then it can carry more watermarking signal and has good concealing effect.



However, embedding in low frequency sub-bands could increase robustness. In contrast, the high frequency sub- bands represent the edges and textures of an image. Usually people do not notice slight changes in above, so high frequency sub bands is more suitable for embedding without being notice by the human eye. Peak Signal to Noise Ratio (PSNR) is used to measure the quality of reconstruction of loss and lossless compression (e.g., for image compression). Acceptable values for wireless transmission quality loss are considered to be about 20 dB to 25 dB [6][7]. The signal in this case is the original data, and the noise is the error introduced by compression. When comparing compression codes, PSNR is an approximation to human perception of reconstruction quality. PSNR is most easily defined via the mean squared error.

Parameters of Video Steganography The parameters which should be kept in mind for a better understanding of the quality and processing of video Steganography are as following [1,2,3]:

PSNR (Peak Signal to Noise Ratio): It is the ratio of the maximum possible power of a signal and the power of the corrupting noise that affects the fidelity of its representation. Use of PSNR value is to measure the quality of reconstruction of lossy compression. Higher PSNR generally indicates that the reconstruction is of higher quality.
P.S.N.R = 10.log10 (MaxI2/MSE)
Mean square error (MSE): It is calculated by comparing the stego image with cover image
MSE= ∑i=1 m ∑j=1 n [O (i, j)-S (i, j)]/m*n

Where M and n are the size of original video frame; Max =255; O is original frame; S is stego frame.

IV. PROPOSED ALGORITHM

Encryption Algorithm:-

Step 1: Read the cover video

Step 2: Separation of frames from the cover video

Step 3: Read the message data or secret data and converted to ASCII file.

Step 4: Open converted text file. (Normalized function is been used to convert to cipher text).

Step 5: Apply DWT on some selected frames to maintain the quality of the video.

Step 6: Hide message length in LH channel and normalized values in HH and HL channels.

Step 7: Apply Inverse DWT to the frames.

Step 8: Reassembling of frames.

Step 9: Stego video is generated.

Decryption Algorithm:-

Step 1: Read the stego video.

Step 2: Separation of frames from the stego video and select the target frames.

Step 3: Apply DWT

Step 4: Calculate the length of hidden text from LH channel from the frames.

Step 5: Generate hidden text and normalized it from HH and HL.

Step 6: Convert extracted text to message data and write it into a file.

Step 7: Secret message is recovered.

V. RESULT &DISCUSSION

In this proposed method we are using the concept of both i.e. transform domain and spatial domain to get the advantages of both the technique. The transform domain provide the high payload and least distortion in the cover medium where as the spatial domain is used for the data hiding purpose.

The basic idea of discrete wavelet transformation (DWT) in image processing is to multi-differentiated decompose the image into sub-image of different spatial domain and independent frequency district. Then transform the coefficient of sub-image. After the original image has been DWT transformed, it is decomposed into 4 frequency districts which is one low-frequency district(LL) and three high-frequency districts(LH,HL,HH). The HH district have maximum noisy part which is not much involve in the image quality or in image content so it will be always better to hide the information here as we are in the proposed method. For data hiding purpose we are using the basic idea of Pixel Value Differencing (PVD) with some extension on it. The hidden text is extracted from the cover video or stego video by the receiver. To recover the text, a Text extraction algorithm is used.

For extracting the text, at first the stego video is read and decomposes it into frames. Then apply the haar wavelet on the selected frames. This DWT function is used to decompose the wavelets. After applying DWT, a total number of four different channels are obtained and according to embedding technique we are able to extract. Next we will regenerate the hidden text data. Finally the extracted text will be written into the target file.

The quality of the algorithm can be measured by using performance parameters like Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) for the frames/images where the secret messages are to be embedded

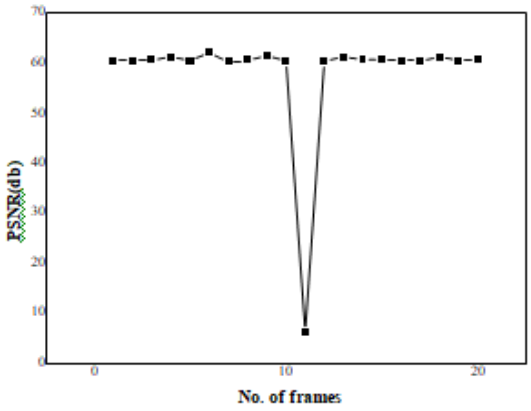


Figure 4: Variation of PSNR with respect to number of frames.

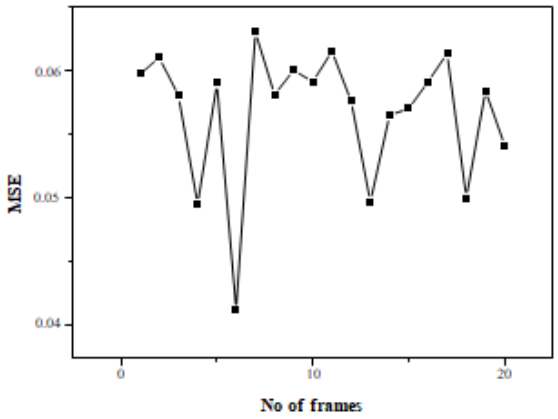


Figure 5. Variation of MSE with respect to number of frames

The PSNR and MSE is been calculated for those frames/images where the information are embedded with the proposed algorithm and show the same with the help of Fig4 and Fig5. The implementation is done with MATLAB.

VI. CONCLUSION

As per the algorithm it is completely a lossless method because we are not entertain a single bit data loss as the secret message is a information file. Due to high peak signal to noise ratio, the minimized distortion remain unseen by naked eyes of the unintended users. Consequently they also remain unaware about the existence of the hidden image. This leads to the intended receivers to achieve the exact information without any disruption or manipulation.

REFERENCES:

[1] Petitcolas, F.A.P., Anderson, R., Kuhn, M.G., "Information Hiding - A Survey", July1999
[2] Yeung, Daniel S., Wing WY Ng, Defeng Wang, Eric CC Tsang, and Xi-Zhao Wang. "Localized generalization error model and its application to architecture selection for radial basis function neural network." Neural Networks, IEEE Transactions on 18, no. 5 (2007): 1294-1305.
[3] Katzenbeisser, S., Petitcolas, F.A.P., Information Hiding Techniques for Steganography and Digital Watermarking, Norwood: Artech House, 2000, pg 56 - 92
[4] Johnson, N.F., Jajodia, S., "Steganalysis of images created using current steganographic tools", April 1998,
[5] Provos, N., Honeyman, P., "Detecting Steganographic Content on the Internet", August 2001,
[6] K. V. Kale, Najran N. H. Aldawla, M. M. Kazi, "Steganography Enhancement by combining text and image through Wavelet Technique ," in International Journal of computer & Applications (IJCA), Vol.51 No.21, pp. 0975 8887, August 2012.
[7] Souma Pal, Prof.Samir Kumar Bandyopadhyay, "Various Methods Of Video Steganography", International Journal of Information Research and Review, Vol.03, Issue, 06. Pp.2569-2573, June, 2016.
[8] K..Parvathi Divya, K. Mahesh, "Various Techniques in Video Steganography – A Review", International Journal of Computer & Organitazion Trends ,Volume 5, February 2014.
[9] L. Marvel, C. G. Boncelet, Jr, and C. T. Retter, "Spread spectrum image steganography", IEEE Trans. Image Process., Vol. 8, No. 8, pp. 1075–1083, Aug. 1999.
[10] Ying Wang, Pierre Moulin, "Perfectly Secure Steganography: Capacity, Error Exponents, and Code Constructions," IEEE Trans. On Information Theory, Vol. 54, No. 6, June 2008.