Color Image Steganography based on Wavelet Transform

Meenakshi Dhaundiyal
PG Student
Department of EXTC
YTIET, Bhivpuri Road
Mumbai University

Sangita Nikumbh
Professor
Department of EXTC
YTIET, Bhivpuri Road
Mumbai University

ABSTRACT
Steganography is a technique of hiding information in digital media. In contrast to cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists. In this paper comparative analysis of image compression is done by two transform method, which are Discrete Wavelet Transform (DWT) & Integer Wavelet Transform (IWT). Steganography can be applied on different file formats, such as audio, video, text, image etc. In image steganography, data in the form of image is hidden under some image by using transformations such as Discrete Cosine transformation (DCT), IWT, DWT etc and then sent to the destination. At the destination, the data is extracted from the cover image using the inverse transformation. This paper presents a new approach for image steganography using DWT & IWT. The cover image is divided into higher and lower frequency sub-bands and data is embedded into higher frequency sub-bands. The proposed approach is implemented in MATLAB 7.0 and evaluated on the basis of PSNR, capacity and correlation. In this method, we concentrated for perfecting the visual effect of the stego image and robustness against the various attacks by using different wavelet families.

General Terms
Steganography, Discrete Wavelet Transform.

Keywords
Discrete Cosine transformation, cover image, stego image, Capacity, PSNR.

1. INTRODUCTION
As more and more communication is conducted electronically, new needs, issues, and opportunities are born. At times when we communicate, we prefer that only the intended recipient have the ability to decipher the contents of the communication. We want to keep the message secret. A common solution to this problem is the use of encryption to obscure the information content of the message. Steganographic techniques can be used to hide or cover the existence of communication with other data, intuitively referred to as cover data. Consider a sender who wants to convey information to a recipient but does not want anyone else to know that the two parties are communicating. The sender could use steganography to hide information within innocuous information, for example, a weather map that covers the existence of the communication. The weather map would then be made available on an open channel for anyone to access, but only the intended recipient is aware of the hidden information, and has the ability to extract it. Steganography is not meant as a replacement to cryptography, but rather augmentation information can be encrypted and then covertly communicated via Steganographic means for added privacy. This can be achieved by using wavelet transform technique. Wavelets allow complex information such as music, speech, images and patterns to be decomposed into elementary forms at different positions and scales and subsequently reconstructed with high precision. Recently the JPEG committee has released its new image coding standard, JPG-2000, which has been based upon DWT. The stego image is obtained by applying various combinations of DWT and IWT on both images. In this method, we concentrated for perfecting the visual effect of the stego image and robustness against the various attacks by using different wavelet families. Finally performance evaluation is done on dual transform steganography using wavelet families and statistical methods.

Review of literature survey has been conducted on evaluating the performance of dual transform technique based steganography using wavelet families and statistical methods.

G.Prabakaran [1] has proposed an algorithm using the Discrete Wavelet Transform for hiding the secret message into the higher frequency coefficient of the wavelet transform while leaving the lower frequency coefficient sub band unaltered. In contrary, steganalysis is a process of detecting the secret communication, against Steganography.

Stuti Goel [2] This paper deals with hiding text in an image file using Least Significant Bit (LSB) based Steganography, Discrete Cosine Transform (DCT) based Steganography and Discrete Wavelet Transform (DWT) based steganography.

Ghasemi.E.[3] Integer wavelet transform avoids the floating point precision problems of the wavelet filter. The novel scheme embeds data in integer wavelet transform coefficients by using a mapping function based on Genetic Algorithm in an 8 × 8 block on the cover image.

Sabyasachi Pattnaik[4] presented a dual transform technique for robust steganography for secret and secure communication. This technique employed error detection and correction coding technique to increase robustness which has excellent PSNR with high levels of security.

H.S. Manjunatha Reddy [5] proposed wavelet based NON LSB steganography (WNLS) algorithm. The proposed algorithm is robust since the payload is embedded into the transform cover image indirectly with excellent PSNR values.

Ghosal N.,Mandal,J.K.[6] This transforms process done from beginning to end mask in row major order of the carrier image. Image authentication is done by hiding secrete message/image into the transformed frequency components of carrier image. Four secrete message/image bits are fabricated within the transformed real frequency component of each carrier image byte except the LSB of first frequency component of each mask. After embedding, a delicate re-adjust phase is incorporated in all the frequency component of each mask, to keep the quantum value positive and non fractional in spatial domain. Robustness is achieved by hiding

an authenticating or secretes message/image in the frequency component with positive and negatives both quantum values and invisibility is satisfied in spatial domain using delicate re-adjust phase.

Nilanjan Dey [7] propose new methodology to hide a color image within another color cover image using alpha-blending technique for the purpose of security. In this approach the imperceptibility and distortion of the Stego image is acceptable and it is resistant to several attacks.

Sarreshtedari, S., Ghaemmaghami, S.[8], proposed a method to achieve a higher quality of the stego image using BPCS (Bit Plane Complexity Segmentation) in the wavelet domain. The capacity of each DWT block is estimated using the BPCS.

The method proposed by Chen, R. J., Peng, Y. C., Lin, J. J., Lai, J. L., Horng, S. J [9], presents the novel multi-bit bitwise adaptive embedding algorithm for data hiding by evaluating the most similar value to replace the original one. This provides very good security.

Fawzi Al-Naima[10] proposed a modified high capacity image steganography technique that depends on wavelet transform with acceptable levels of imperceptibility and distortion on the cover image with high levels of overall security, a technique that depends on wavelet transform and Information-Hiding System.He used wavelet decomposition for hiding the data.

2. PROBLEM DEFINITION

Steganography is a camouflage technique used to hide secret data. Among all multimedia data on the Internet, images are the most popular; therefore, many researchers use digital images as the carrier medium. The original image in which we intend to hide the secret image is called the cover image, and the image after embedding is called the stegoimage. The stegoimage, which looks like a regular image, can avoid attracting undesired attention during transmission given that there is little distortion between the cover image and the stegoimage. To achieve better image quality on both the stegoimage and the extracted secret image without extra storage space, the DCT-based approach hides the most significant DCT coefficients of each DCT secret block into non-significant parts of each DCT cover block.

DWT comprises between compression ratio and quality of reconstructed image, it adds speckle noise to the image for improvement in the reconstructed image. Hence DWT technique is useful in medical applications. DCT gives less compression ratio but it is computationally efficient compared to other techniques. DWT gives better compression ratio without losing more information of image. Pitfall of DWT is, it requires more processing power. DCT overcomes this disadvantage since it needs less processing power, but it gives less compression ratio. DCT based standard JPEG uses blocks of image, but there are still correlation exits across blocks. Block boundaries are noticeable in some cases. Blocking artifacts can be seen at low bit rates. In wavelet, there is no need to block the image. It facilitates progressive transmission of the image (scalability). Hybrid transform gives higher compression ratio but for getting that clarity of the image is partially trade off. It is more suitable for regular applications as it is having a good compression ratio along with preserving most of the information.

In least significant bit (LSB), each pixel of an image transformed into the binary value and data is hidden into the least significant position of the binary value of the pixels of the image in such a manner that, it doesn't destroy the integrity of the cover image but this scheme is sensitive to a variety of image processing attacks like compression, cropping etc.

3. METHODOLOGY

This work proposes Steganographic technique for hiding multiple images in a color image based on DWT. The cover image is decomposed into three separate color planes namely R, G and B. Individual planes are decomposed into sub bands using DWT.DWT is applied in HH component of each plane. Secret data are dispersed among the selected DWT coefficients using a private key. PSNR, capacity and correlation are major aspects in steganography. More specifically PSNR is demanded high, but it depends application to application. PSNR is inversely proportional to capacity, and directly proportional to correlation and vice-versa. During the study we found a problem that is of a proper combination of PSNR, capacity and correlation is required so that data can be sent through unsecure channel without fear of third party access. The results in the steganography mainly depend on secrete data. The larger value of the secrete data; affect more to the quality of stego image rather than smaller value of secret data.

3.1 Algorithm

- Embedding Process both cover image & secret data by using DWT.

During the proposed embedding process, perform DWT on both the cover image and the secret data by using the fusion process we get fused image. Apply IDWT on fused image to get a stego image.

1) Algorithm for proposed embedding process:

Step 1: Read the cover image (i.e.Video) as C and segment the frame based on video file. Convert the pixel values Of cover image into a gray scale image as CG.

Step 2: Apply image pre-processing and correction process to get a gray scale cover image.

Step 3: Read the secret data(i.e. Text) as S. Apply image pre-processing and correction process to get a gray scale image as SG.

Step 4:Apply transforms domain technique into cover gray scale image and secret gray scale image.

Step 5: By applying 2D-DWT extract the approximation coefficients of matrix LL1 and detail Coefficients matrices LH1, HL1, HH1 of level 1 of the cover image as CG1.

Step 6: By applying DWT extract the approximation coefficients of matrix LA1 and detail coefficient matrices LH1,HL1, HH1 of level 1 of the secret image as SG1.

Step 7: Apply fusion operation on an image CG1 and SG1 and get merged image. Finally perform fused image with 2-DWT to form the stego image as ST.

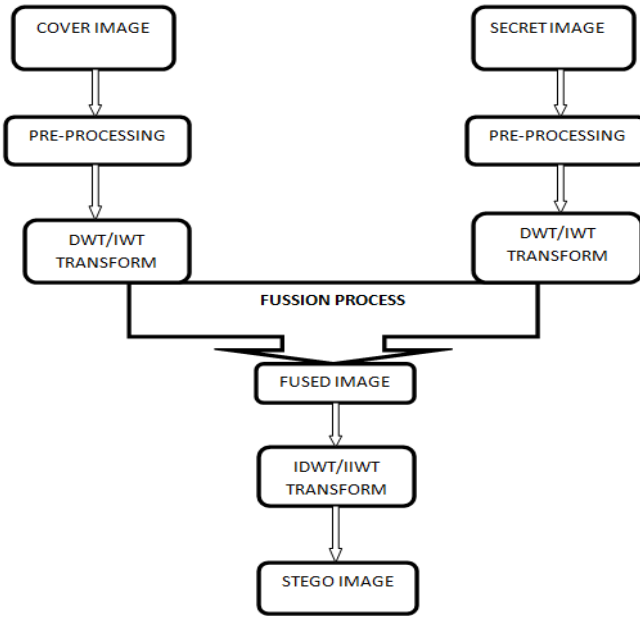

Figure1. Block Diagram of Embedding.

- Extraction of Secret Image

During the proposed extracting process, the recover stego image and known cover image were reconstructed with DWT transform domain and followed by the fusion process. Next, inverse transform IDWT was performed to rebuild the secret data. Finally the secret data is obtained, which is similar to the original secret image.

Step 1: Receive the stego image. Perform a 2-D DWT at the level of both stego image and known cover image.

Step 2: Apply fusion process on both stego image and cover image to get fused image.

Step 3: Separate the wavelet coefficients and take inverse IDWT of the fused image to reconstruct the secret image.

Step 4: Select the 4 bit privacy key to decrypt the secret information.

Step 5: Calculate the statistical parameters such as Mean square Error (MSE), Peak signal to noise ratio (PSNR),Capacity, Entropy Mean of the stego image**.**

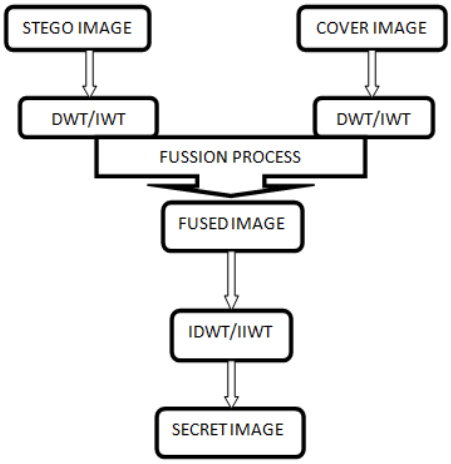

Figure 2. Block Diagram of Extraction.

3.2 Performance Parameter Evaluation

To retain the image quality and provide a stronger robustness and security of a image steganography scheme, the statistical parameters are further considered. The value of statistical parameters not only reduces the image perceptibility but also enhances the robustness to resist attacks. We used PSNR and MSE to measure the distortion between the original cover image and the stego image. The other Image statistical parameters are normalized cross correlation, average difference; structural content, maximum difference and normalized absolute error are taken into consideration.

3.2.1 Mean Square Error (MSE):

The distortion in the image can be measured using MSE and is calculated using Equation MSE can be defined as the measure of average of the squares of the difference between the intensities of the stego image and the cover image. It is popularly used because of the mathematical tractability it offers. It is represented as follows:

$$MSE = \frac{1}{MN}\sum_{j=1}^{M}\sum_{k=1}^{N}\left(X_{j.k} - X'_{j.k}\right)^2$$

Where $X_{j,k}$ is the original image and $X'_{j,k}$ is the stego image. A large value for MSE means that the image is of poor quality and vice-versa.

3.2.2 Peak Signal to Noise Ratio (PSNR):

It is the measure of the quality of the image by comparing the cover image with the stego image, i.e., it measures the statistical difference between the cover and Stego image. The PSNR depicts the measure of reconstruction of the transformed image. This metric is used for discriminating between the cover and stego image.

$$PSNR = 10\frac{\log_{10}(255)^2}{MSE}dB$$

3.2.3 Capacity:

It is the size of the data in a cover image that can be modified without deteriorating the integrity of the cover image. The steganography embedding operation needs to preserve the statistical properties of the cover image in addition to its perceptual quality. Therefore capacity depends on total number of bits per pixel & number of bits embedded in each pixel. Capacity is represented by bits per pixel (bpp) and the Maximum Hiding Capacity (MHC) in terms of percentage Capacity can be formulated as:

Capacity =No. of pixels of secret image that are hidden / No. of pixels of cover image that are used to hide data

4. EXPERIMENTATION AND RESULTS

To evaluate the performance of color image steganography based on DWT various statistical parameters were evaluated. The performance results of our transform domain technique based on DWT techniques were verified using MATLAB 7 version. The results showed that capacity and security of image had increased simultaneously. The proposed method pre adjusts the original cover image in order to guarantee that the reconstructed pixels from the embedded coefficients would not exceed its maximum value and hence the message will be correctly recovered. The method not only provides a better way for embedding large amounts of data into cover images with imperceptions, but also offers more robustness,

which can avoid various image attacks noise addition, compression. So, there is no chance that the intruder may detect the message after couple of attacks. DWT is a highly robust method in which the image is not destroyed on extracting the message hidden in it and provides maximum security.

Table 1.Shows The Performance Evaluation With Respect To Statistical Parameter Values.

PARAMETERS	VALUES
MSE	0.006042
PSNR	70.3187
PAYLOAD	4096
Mean	113.6965
Entropy	7.53
Space Left	4083

5. CONCLUSION

The proposed method embeds data i.e. text format in cover images using DWT method. The secret data is hidden in binary form into cover images due to which double protection has been provided to confidential data which can be any text, audio, video or image. The experimental results will show that the proposed scheme can be a good alternative for secure communication where two level of security is obtained in conjunction with high capacity and good imperceptibility. In this paper a secure color image steganography technique using DWT is proposed. In this technique the secret text is hidden using keys. The experimental results are expected to show that the technique produces good quality stego images with better PSNR values compared to similar other techniques.

The proposed approach is implemented in MATLAB 7 and video is used in implementation. Various images used for the experiment are described as under:

Cover Image: In implementation, is used as cover medium as video, of 31 frames. The image produced by the segmentation video is in .jpeg format.

Stego Image: After embedding the data (.txt) in cover image, stego image obtained. Cover and Stego images are shown below in Figure. 3.

Secrete Data: The data recovered is in .txt format.

Recovered Images: By applying extraction procedure, we recovered secret data from stego image. The secret data are shown in Figure. 4

a) Cover Image

b) Stego Image

Figure.3 Cover and Stego Images

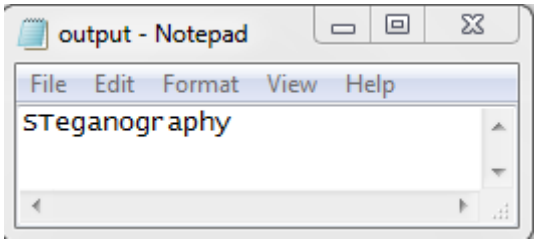

Figure. 4 Recovered Secret Data/Messages.

The work presented in this paper deals with the technique of image steganography using discrete wavelet transform DWT is applied on video. The proposed approach tries to overcome the demerits of previous similar image steganography approaches. In future the algorithm can be tested with some more transform domain techniques to improve the performance.

6. ACKOWLEDGEMENTS

I would like to thanks my guide Mrs. Sangita Nikumbh for her valuable guidance and suggestions while writing this paper.

7. REFERENCES

[1] G. Prabhakaran, Dr. R. Bhavaniand Kanimozhi, Dual Transform Based Steganography Using Wavelet families and statistical Methods.”Proceedings of 2013International Conference on Pattern recognition Informatics & Mobile Engineering(PRIME) Feb.21-22 IEEE 2013.

[2] Stuti Goel, Arun Rana and Manpreet Kaur, “A Review of Comparision Techniques of Image Steganography.” Global Journal of Computer Science & Technology, Vol. XIII Issue IV Version I Year 2013.

[3] Ghasemi. E. , Sci. & Res. Branch, Islamic Azad Univ., Tehran,Iran, Shanbehzadeh. J.,Zahir Azami. B. “A Steganographic Method Based On Integer Wavelet Transform And Genetic Algorithm.” International Conference On Communication And Signal Processing (ICCSP), 2011 IEEE Feb.2011 ISBN: 978-1-4244-97980.

[4] Sabyasachi Pattnaik, R.K. Chhotaray,K.B.Raja and K.B. Shiva Kumar,”Performance Comparision Of Robust Steganography Based On Multiples Transformation Techniques.”, International Jouranal On Computer Technology Applications, Vol 2(4), Pp.1035-1047, 2011.

[5] K. B. Raja And H.S. Manjunatha Reddy, “Wavelet Based Non Lsb Steganography,” International Journal Of Advanced Networking And Applications, Vol 03(3), Pp.1203-1209,2011.

[6] Ghosal.N.,Mandal J.K.,"A Steganographic Schemes For Colour Images Authtntication (SSCIA)", International Conference On Recent Trends In Information Technology (ICRTIT 2011). (Madras Institute Of Technology Chennai, India June 13-05,2011), IEEE Conference Publications, 826-831.

[7] Nilanjan Dey, Anamitra B. R, And Sayantan D. " A Novel Approach Of Color Image Hidind Using Rgb Color Planes And DWT, " International Jouranal Of Computer Applications, Volume 36-No. December 2011.

[8] Sarreshtedari.S.,Ghaemmaghami S."High Capacity Image Steganography In Wavelet Domain. In Proceedings Of 2010 7th IEEE Consumer Communications And Networking Conference (CCNC) (Las Vegas,Nevada, USA, 9-12 January 2010), IEEE Conference Publications,1-5.

[9] Chen, R. J., Peng, Y.C., Lin, J. J., Lai, J.L., Horng, S.J., " Novel Multi-Bit Bitwise Adaptive Embedding Algorithms With Minimum Error For Data Hiding" Fourth International Conference On Network And Systems Security (NSS 2010), (Melbourne, Australia 1-3 September 2010), IEEE Conference Publications, 306-311.

[10] Ali Al-Ataby And Fawzi Al-Naima, "A Modified High Capacity Based On Wavelet Transform," International Arab Journal Of Information Technology, Vol.7,Pp,1-7,2010.

[11] Weiqi Luo, Fangjun Huang And Jiwu Huang , "Edge Adaptive Image Steganography Based On LSB Matching Revisited" IEEE Transaction On Information Forensics And Security, Vol. 5, No. 2, June 2010.

[12] Xie, Qing, Xie, Jianquan, Xiao, Yunhua, "A High Capacity Information Hiding Algorithm In Color Images", 2nd International Conference On E-Business And Information System Security (EBIISS 2010).(Wuhan China, 22-23 May, 2010),IEEE Conference Publications, 1-4.

[13] Sacha Klonus And Manfred Ehlers , "Performance Of Evaluations Methods In Image Fusion ", 12th International Conference On Information Fusion Seattle, W.A. USA, Pp. 1409-1416,2009.

[14] R.O.EI Safy, H. H. Zayed, EI Dessouki Remote Sensing and Space Sciences, "An Adaptive Steganographic Technique Based on Integer Wavelet Transform",IEEE-2009.

[15] Sunil Lee ,Chang D. Yoo and Ton Kalker, "Reversible Image Watermarking Based on Integer-to-IntegerWavelet Transform" IEEE Transactions On Information Forensics And Security, Vol. 2, No. 3, September 2007.

[16] Guorong Xuan, Jiang Zhu, Jidong Chen, Yun Q. Shi, Zhicheng Ni and Wei Su, "Distortionless data hiding based on integer wavelet transform", IEEE Electronic letters, December 2002 Vol. 38 No. 25, pp. 1646-1648.