A Discrete Wavelet Transform: A Steganographic Method for Transmitting Images

M.A. Wakure
Aurangabad University
TPCT'S COE, Osmanabad

Anilkumar N. Holambe, PhD
Aurangabad University
TPCT'S COE, Osmanabad

ABSTRACT

Steganography is the art of hiding private or sensitive information within a carrier that for all intents and purposes, appears safe. The main objectives of Steganography's are undetectability, robustness i.e resistance to various image processing methods and compression and capacity of the hidden data. Based on this factors steganography separates from related techniques such as watermarking and cryptography. In this paper a new Steganographic method for transmitting images based on discrete wavelet transform is proposed using technique 3-level wavelet decomposition. In this technique taking the single plane of cover image for embedding and processing the image as 4x4 blocks with swapping. The proposed method increasing the secret image capacity and security level of the data with maximum value of PSNR and minimum value of RMSE.

Keywords

Discrete Wavelet Transform, Peak Signal to Noise Ratio, Steganoanalysis and Steganography.

1. INTRODUCTION

Communication of secret information is critical factor in information technology that continues to create challenges with increasing levels of sophistication. Steganography can be used to protect intellectual property or trade secrets, thus maintaining the confidentiality of valuable information and protecting it from sabotage, theft or unauthorized viewing. Steganography is a technology concerned with ways of embedding of secret message in a cover message also known as cover object in such a way that he existence of embedded information is hidden [1]. A secret message can be plaintext, an image, an audio, video or anything that can be represented as bit stream. The embedding process is sometimes parameterized by a secret key, called stego key, and without knowledge of this key it is difficult for an unauthorized party to detect and extract the secret message. Once the cover object has information embedded in it, it is called a stego object.

Following figure 1 shows classification of data hiding techniques[13]

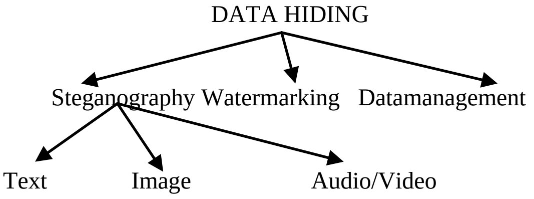

Fig 1: Classification of Data Hiding

The detection of steganographically encoded packages is called steganalysis. Steganalysis is the method of detecting stego tool usage by identifying suspected information streams and determining whether or not they have hidden messages encoded within them. With data hidden beyond the limits of human perception within cover images, detection is difficult. Such tools can recover the hidden information, and, if necessary destroy it along with the original message [2][4]. Steganalysis is achieved through applying different image processing techniques e.g., image filtering, rotating, cropping, translating, etc, or more deliberately by coding a program that examines the stego-image structure and measures its statistical properties [5]. Steganography is employed in various useful applications such as copyright control of materials, enhancing robustness of image search engines, smart IDs (identity cards) where individuals' details are embedded in their photographs, video-audio synchronization, safe circulation of secret data, TV broadcasting, TCP/IP packets and in medical imaging systems where a separation is considered necessary for confidentiality between patients image data or DNA sequences and their captions e.g., physician, patient's name, address and other particulars [3]. Digital Steganography provides privacy for intelligence and military personnel and for people who are subject to censorship. There are various domains of information hiding viz., spatial domain, transform domain and spread spectrum domain. In spatial domain methods a steganographer modifies the secret data and the cover medium in the spatial domain, which is the encoding at the level of the LSBs. LSB encoding, is extremely sensitive to any kind of filtering or manipulation of the stego-image. Scaling, rotation, cropping, addition of noise, or lossy compression to the stego-image is very likely to destroy the message. Furthermore an attacker can easily remove the message by removing (zeroing) the entire LSB plane with very little change in the perceptual quality of the modified stego-image [5]. The information hiding Steganography techniques are based on following transforms such as 1.Discrete Fourier Transform (DFT) 2. Discrete Cosine Transform (DCT). 3. Discrete Wavelet Transform (DWT). 4.Singular Value Decomposition (SVD) Transform and 5. Discrete Hadamard Transform (DHT). These techniques are independent of an image formats and hide data in more significant areas of the transformed image [6] [7].

This paper present a steganographic method based on discrete wavelet transform. This paper is organized as follows. Section 2 briefly discusses the basic idea of steganography model or system. Section 3 describes the frequency domain method such as Discrete Wavelet Transform (DWT) for transmitting images. Section 4 briefly explain the procedure of proposed technique i.e three level wavelet decomposition. Section 5 represents experimental results and statistical analysis of proposed method. Section 6 gives the conclusion and future scope. Finally in section 7 list of references that are useful for this work.

2. STEGANOGRAPHY MODEL

There are mainly four requirements of any information hiding technique, namely, Imperceptibility, Capacity, Security and Robustness. Imperceptibility means that human eyes cannot distinguish the difference between the stego-image and the original image. Capacity refers to the amount of data that can be embedded in the cover object. Security means that an eavesdropper cannot detect the hidden data, and Robustness requires that the hidden data can be recovered within certain acceptable errors even when the stego-image has endured some signal processing or noises.

The sender, who wants to send a secret message to the recipient, randomly chooses a harmless cover image. Afterwards, sender embeds the secret message in the cover and probably uses a stego key. As a result, sender gets a stego image which must be undistinguishable from the cover image neither by a human nor by a computer system. Therefore, the stego image represents the original (cover) image along with the secret message embedded inside this cover image. Then, sender transmits the stego image to receiver over a communication channel. The purpose of the system is to prevent a third party from observing or noticing the hidden message. On the other side, receiver extracts the embedded message since he knows the embedding method and the stego key used in the embedding process. Only the transmitter and the intended recipient should have the stego key. Therefore, most of steganographic systems prompt users to provide a stego key or password when they try to embed information in a cover image. Figure 2 shows the general principle of image-based steganographic model.

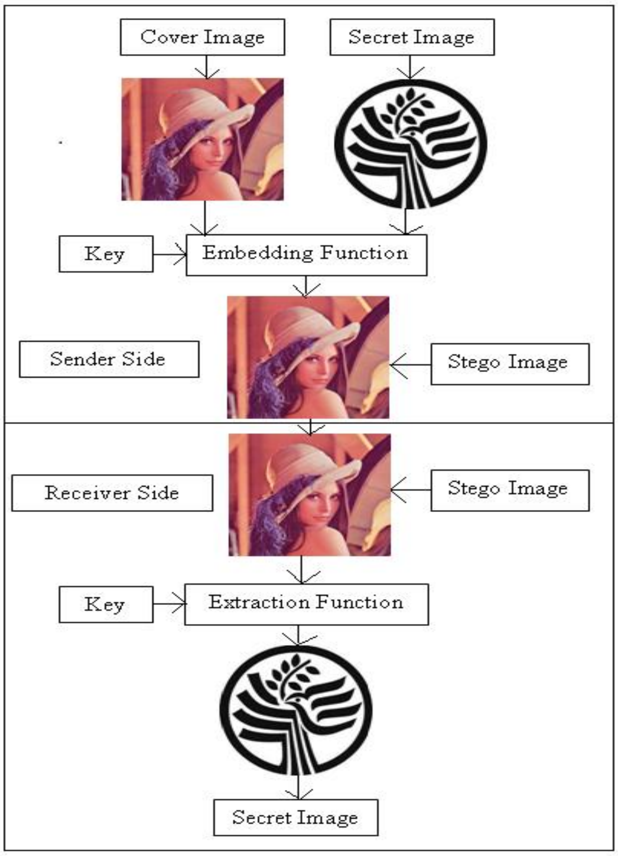

Fig 2: Steganography Model

3. DISCRETE WAVELET TRANSFORM

Image steganography techniques can be divided into two group's spatial domain and transform domain. Steganography in the transform domain involves the manipulation of algorithms and image transformation. These methods hide messages in more significant areas of the cover image, so making it more robust.

The text, images have been widely used as cover objects for the purpose of information hiding as their digital representation provide high degree of redundancy. The most widely used information/data hiding Steganography techniques are based on Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD) Transform and Discrete Hadamard Transform (DHT). These techniques are independent of an image formats and hide more data in significant areas of the transformed image. In this paper discrete wavelet transform is proposed for transmitting images because, DWT allows the use of long time intervals where we want more precise low-frequency information, and shorter regions where we want high-frequency information. The DWT consists in splitting the signal $x[n]$ in low and high frequencies using a lowpass and a highpass filter respectively. In DWT based steganography the information is stored in the wavelet coefficients of an image, instead of changing bits of the actual pixels. The idea is that storing in the least important coefficients of each 4 x 4 Haar transformed block will not perceptually degrade the image. In DWT based steganography method contains embedding and extraction process. Following figure 3 and figure 4 shows the block diagram of embedding process and extraction process respectively.

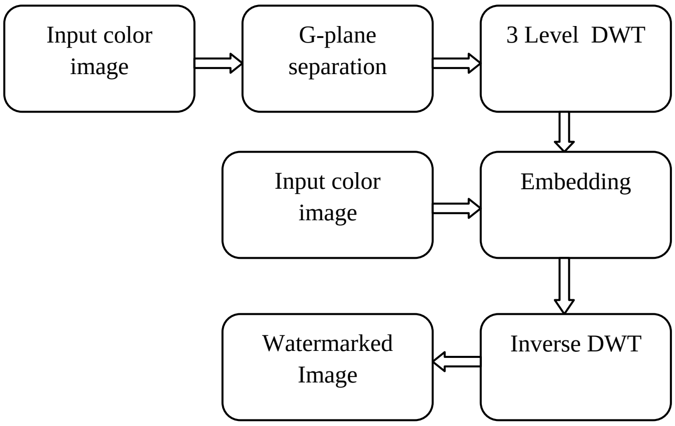

Fig 3: Embedding process using three level DWT

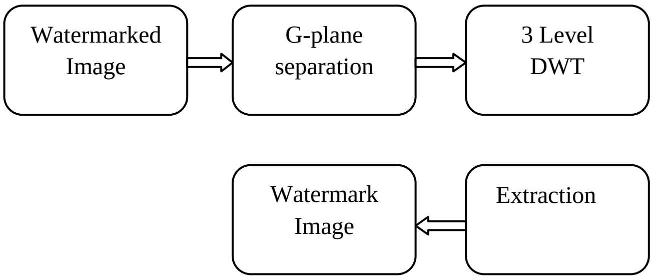

Fig 4: Extraction process using three level DWT

4. IMPLEMENTATION OF THE PROPOSED METHOD

This section describes the proposed method in frequency domain such as discrete wavelet transform (DWT).

4.1 Proposed Method : Three Level Wavelet Decomposition

l. Perform three level 2D-Haar DWT decomposition as follows:

a) Take the JPEG cover image (CI) (512 x512) and its green plane alone and perform first level 2D-DWT on the image to obtain approximation 1 coefficient (LL1), horizontal 1 coefficient (HL1) and vertical 1 coefficient (LH1), diagonal 1 coefficient (HH1) respectively.

b) Take the approximation 1 coefficient (LLl) and perform second level 2D-DWT on the image to obtain LL2, HL2, LH2 and HH2 respectively.

c) Take the approximation 2 coefficient (LL2) and perform third level 2D-DWT on the image to obtain LL3, HL3, LH3 and HH3 respectively.

2. Take the secret image (SI) and turn it into black and white.

3. Perform Embedding process as follows:

a) Assume an embedding coefficient of value of α= 0.05.

b) Process on LL3 block by block (4x4).

c) Process the secret image block by block (4X4).

d) To obtain the secret image block (4x4) following formula is used which is basically swapping,

SI block = {(1- α) * LL3 intensity value} +

{α * SI intensity value}

4. Perform three level 2D-Haar Inverse DWT (IDWT) for reconstruction to obtain the stego image.

5. Perform Extraction process as follows:

a) Perform three level 2D-Haar DWT decomposition on the stego image as well the cover image.

b) Process LL3 of the stego image and cover image block by block (4x4).

c) Assume an embedding coefficient of value of α= 0.05.

d) To get the image blocks of the secret image (4x4) following formula is used,

SI block = {LL3 intensity value of stego image – {(1- α) * LL3 intensity value of the CI}}/ α.

6. Calculate RMSE and PSNR values in order to check for the visual quality of the stego image.

5. EXPERIMENTAL RESULTS

For visual evaluation, consider natural appearance of secret image. This section present the experimental result of the proposed method. The quality of stego image produced by the proposed method has been tested exhaustively based on various image similarity metrics namely RMSE and PSNR.

5.1 Embedding and Extraction results using: Three Level 2D Haar DWT

Cover image is shown in figure 5 and secret image before embedding is shown in figure 6, after three level decomposition using 2D Haar DWT is shown in figure 7. Stego image with secret image embedded on cover image is shown in figure 8 and the extracted secret image is shown in figure 9.

Fig 5: Cover Image

Fig 6: Secret Image

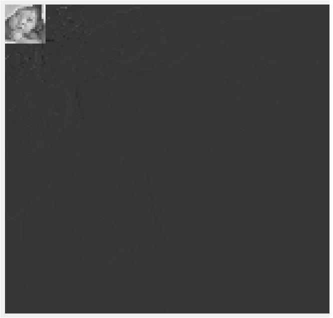

Fig.7: Cover image after three level decomposition using 2D Harr DWT

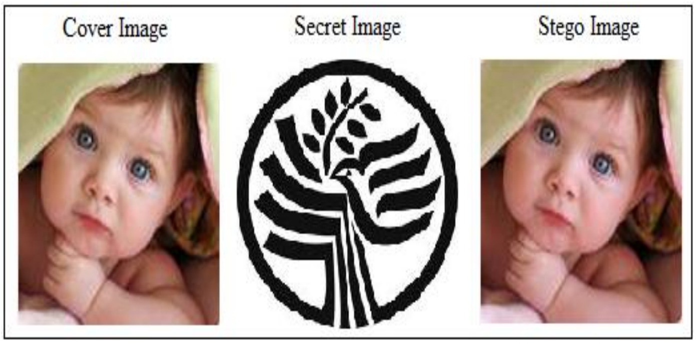

Fig. 8: Stego image with secret image embedded on cover image

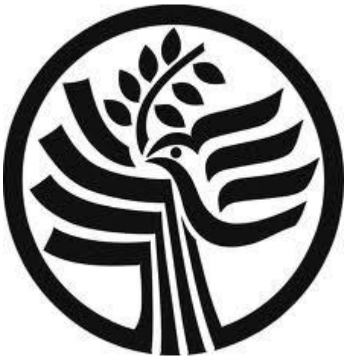

Fig 9: Extracted secret image

5.2 Stastical Analysis

In addition to the visual analysis, extended investigation to a quantitative analysis. The performance of tproposed technique can be measured by calculating the image quality parameter such as RMSE and PSNR of the secret image. The performance of proposed methods shown in table I.

5.2.1 RMSE (Root Mean Squared Error)

Calculate the root mean square error of the corresponding pixels in the reference image I and the extracted image F.

$$RMSE = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[I(i,j) - F(i,j)]^2}{M * N}$$

5.2.2 PSNR (Peak Signal to Noise Ratio)

The PSNR is the most commonly used as quality of reconstruction of extracted image. It is defined as,

$$PSNR = 10log_{10}\left(\frac{255^2}{RMSE}\right)$$

Where, 255 is the maximum pixel value of the image when the pixels are represented using 8-bit per samples.

The experimental results are analyzed based on the combination RMSE and PSNR.

Table I
Results Of Proposed Method

Parameters	Proposed Method
RMSE	6.56
PSNR	31.79

6. CONCLUSION AND FUTURE SCOPE

In this paper, image data hiding technique based on 2D Haar DWT has been proposed. The stego-image is looking perfectly intact and has high PSNR value low RMSE value. Hence, an unintended observer will not be aware of the very existence of the secret-image. The extracted secret image is perceptually similar to the original secret image. The file size of cover image and stego image will not be different too much. The advantage of steganography over the cryptography is it does not raise any suspicion and message can not be exchanged over the communication channel. Using this technique in transform domain the embedding capacity is better than other existing techniques. The relative analysis between the proposed method the other existing techniques has shown the pre-eminence of the proposed technique.

In future work, the steganography can also be used to enforce on a digital medium. For example, steganography can be used to hide information in a music/audio file or in a video file. When an unauthorized user plays the file, the information can be extracted and checked against the permission for that file.

7. REFERENCES

[1] S. T. Narasimmalou, Allen Joseph .R., “Discrete Wavelet Transform based Steganography for Transmitting Images”, IEEE-International Conference On Advances In Engineering, Science And Management (lCAESM - 2012) March 30, 31, 2012.

[2] Neil F. Jhonson, Sushil Jajodia, “Exploring Steganography- Seeing the Unseen”, IEEE 1998.

[3] Yuan-Hui Yu, Chin-Chen Chang, Iuon-Chang Lin, “A new steganographic method for color and grayscale image hiding” Computer Vision and Image Understanding 107 (2007), Elsevier.

[4] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt, “Digital Image Steganography: Survey and Analysis of Current Methods” , Elsevier.

[5] David Frith, “Steganography Approaches, Options and Implications”, Network Security , August 2007.

[6] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt , “Biometric Inspired Digital Image Steganography”, IEEE.

[7] S. K. Muttoo, Sushil Kumar, “Robust Source Coding Steganographic Technique Using Wavelet Transforms”, BIJIT - BVICAM’s International Journal of Information Technology, July – December, 2009; Vol. 1 No. 2; ISSN 0973 – 5658.

[8] Shikha Sarda, Sumit Budhiraja, “Image Steganography: A Review”, International Journal of Emerging Technology and Advanced Engineering, January 2013.

[9] 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.

[10] Souvik Bhattacharyya, Gautam Sanyal, “ A Robust Image Steganography using difference Modulation (DWTDM) ”, I. J. Computer Network and Information Security, 2012, 7, 27-40.

[11] Xiang- Yang Luo, Dao-Shun Wang, Ping Wang, Fen-Lin Liu, “A review on blind detection for image steganography”, Signal Processing, 2008, Elsevier.

[12] R.Amirtharajan, R. Akila, P. Deepika Chowdavarapu, “Comparative Analysis of Image Steganography”, International Journal of Computer Applications, olume 2 – No.3,May2010.

[13] S.K.Muttoo,Sushil Kumar, “A mulltilayred secure, robust and high capacity image steganographic algorithm”, 2011.