Comparative Analysis of Different Transformation Techniques in Image Steganography

Sourav Kumar Kamila
(111CS0127)

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela - 769008, Odisha, India

Comparative Analysis of Different Transformation Techniques in Image Steganography

A thesis submitted in partial fulfilment of the requirement
for the degree of

Bachelor of Technology in

Computer Science and Engineering

by

Sourav Kumar Kamila

under the supervision of

Prof. Ramesh Kumar Mohapatra

Department of Computer Science and Engineering

National Institute of Technology Rourkela, Odisha - 769008

May 2015

List of Figures

List of Tables

Certificate

This is to certify that the work in the project entitled *Comparative Analysis of Different Transform Techniques In Image steganography* by *Sourav Kumar Kamila* is a record of his work carried out under my supervision and guidance in partial fulfillment of the requirements for the award of the degree of *Bachelor of Technology* in *Computer Science and Engineering*.

Date:
Place:

Prof. Ramesh Kumar Mohapatra
Dept. of Computer Science and Engineering
National Institute of Technology Rourkela - 769008

Acknowledgements

I express my profound gratitude and indebtedness to Prof. R. K. Mohapatra, Assistant Professor, Department of Computer Science and Engineering, NIT Rourkela for introducing the present topic and for his inspiring intellectual guidance, constructive criticism and valued suggestion throughout the project.

I am obliged to all the professor of the Department of Computer Science and Engineering, NIT Rourkela for instilling in me the basic knowledge about the field that greatly benefitted me while carrying out the project and achieving the goal.

Date:
Place:

Sourav Kumar Kamila
Dept. of Computer Science and Engineering
National Institute of Technology Rourkela - 769008

Abstract

Image steganography is a way of transferring confidential messages through a cover image which cant be observed by a third party. In this paper we have a comparative study among image steganography using LSB technique and Huffman encoding with DCT and DWT. In first case, the image is 8x8 block processed and 2D-DCT applied on it and Huffman encoding is applied on the text message. Then, the Huffman encoded binary string is inserted in the cover image. Then 2D-IDCT is applied on that inserted image. In second case, 2D-DWT is applied on the cover image and Huffman encoding is applied on the text message. Then, the Huffman encoded binary string is inserted in the cover image. Then, 2D-IDWT is applied on the inserted image. After applying IDCT and IDWT the images found are stego images. The PSNR value of these two stego images are compared and found that DWT stego image has better PSNR value.

Keywords: Steganography, DCT, IDCT, DWT,IDWT, Image, Secret message, Cover Image, Huffman Coding, Huffman Table, LSB embedding.

Contents

1 Introduction

In todays era Information is power. So, in this information age we have to transfer information very carefully. The way of transferring confidential information hiding inside a cover medium is called as Steganography.This word Steganography is a combination of two Greek words. The two sub-words are "Steganos" and "Graphia". In Greek "Graphia" means "writing" where as "Steganos" means "Covered".

This technique is not new for this world. It was practiced long before, since 440 BC. The war messages were transferred through different media such as writing message on wood then covering that by wax, writing with invisible inks which can be read in a particular light, writing inside the stomach of the rabbit [5]. They also used human as a secret medium to transfer data, first they used to shave the head, tattood the secret message on scalp, then wait until the hair grows. After the hair grows completely they send the person to the destination and the secret message extracted by shaving the head of that person again.

Now, internet is the main media of communication. After the invention of social media sites images, videos are transferred in enormous amount daily using internet. So, today steganography depends upon images and videos for covert media.

1.1 Steganography

Steganography is a Greek word which means concealed writing [5]. The word steganos means covered and graphia means writing . Thus, steganography is not only the art of hiding data but also hiding the fact of transmission of message. Thus, steganography is an art as well as science of transmission of secret message by embedding the message into cover body such that the existence of information is invisible. The cover body when carries the secret message is called as stego-medium. In ancient time, the data was protected by hiding it on the back of wax, stomach of rabbits, on the scalp of slaves. But today most of the data is transferred through text, images, audio and video over a network. So, for the transmission of any confidential data, the chosen stego-mediums are text, images, audio and video.

1.2 Cryptograpy

Cryptography is the art of communication between two parties in presence of a third party. Here, the secret message is encrypted first using any encryption

algorithm and encryption key then transferred. According to kerckhoffs principle there is no need for hiding the encryption algorithm, the only thing taken care of should be a large domain of encryption key [6].

1.3 Comparision

- **Steganography** send a secret message hiding inside a cover medium.
- **Steganalysis** process of breaking steganography.
- **Cryptography** send a secret message encrypting it using a key
- **Cryptanalysis** process of breaking cryptography.

1.4 Types of Stegangraphy

The various types of steganography [5] are given below;

- **Text Steganography**

  This is the oldest method of image steganography. Here, the secret data is hidden after the end of file character. But with rise of various file formats it is not suitable enough, because original files are very small in size. So, adding extra data can be visualized easily.

- **Image Steganography**

  It is the most common type of steganography. Here, the cover image is always an image file. The secret message is inserted into the image using various techniques and keys. After insertion of message, the image is sent to the recipient. The recipient extracts the secret message using the same technique and keys. The stego image is hardly observable of carrying any messages.

- **Audio Steganography**

  It is concerned with embedding secret message inside the innocuous cover speech so that it will make no difference in hearing. There are techniques to embed messages in MP3, WAV, etc. audio files.

- **Video Steganography**

  Here the stego medium is the video files such as MKV, AVL, etc. The secret message is embedded in such a manner that there will be minimized effect in video quality.

- **Protocol Steganography**

  Here the stego medium used is the header file of various network protocols such as TCP/IP, UDP. The secret message is hidden inside the reserve field or optional fields.

1.5 Objective

The objective of this project is to find a better method of image steganography using various transformation techniques. Among DCT and DWT transform methods which one is more suitable for image steganography using LSB technique and Huffman Encoding.

2 Literature Review

2.1 Before Digital Age

Origin of steganography can be tracked back to 440 BC. The term Steganography was coined in 15th century. But it has been used from several thousand years back.

2.2 During Digital Age

Now a days the majority ways of steganography are transmission of secret messages through image file, audio, video, network protocol headers, etc. as the cover medium. Because today social networking is a part of our day to day life and people normally communicates through mails, uploading image files, audio video files [1].

There are certain ingredients which are used to make a successful steganography communication. Such as

- Cover medium (image, audio, video, text, protocol)
- Secret message (text, image)
- Message embedding algorithm
- A stego key if necessary

2.3 Image Steganograph

2.3.1 What is an image?

An image is a picture that has been created or copied and stored in digital form. An image can be described in terms of vector or raster graphics. An image stored in raster form is sometimes called a bitmap. A pixel is the fundamental building block of any image. Gray images have pixels of 8 bits while colour images have pixels of 24 bits. So gray images can vary their pixel colours in 256 different shades of gray. Colour images have red, green, and blue as primary colours. Different percentage of this primary colour in this 24 bits constitute the coloured pixels which are also called as true colour pixels [1].

2.4 Steganography Techniques

2.4.1 Spatial Domain Steganography

Here, the original cover medium is directly modified to embed any kind of confidential message into it. One most popular method is the LSB insertion technique on image steganography. In this type of technique the least significant bit of cover image is modified to match with the secret messages binary bit string. The change of least significant bit from 0 to 1 or vice versa is not visible to human sight [5]. So, it is a simple but efficient method on early days of modern steganography.

2.4.2 Transform Domain Steganography

Here the cover image first transferred to the corresponding frequency domain of the image. Then any kind of insertion or modification isdone on the frequency domain coefficients. This is an effective process in image steganography. In fact all better steganographic methods today, are based on this techniques [2]. This technique is immune to image cropping, scaling, any kind of modification by a third party. Different types of transform domain steganography are as follows

(i) Discrete Fourier Transform Steganography(DFT)

(ii) Discrete Cosine Transform Steganography(DCT)

(iii) Discrete Wavelet Transform Steganography(DWT)

2.4.3 Steganography using Distortion Technique

In this method main idea is to modify the cover medium such a way that the difference between original cover image and modified cover image will give information. When the receiver gets the modified image he must have the original image. So comparing both the images he can find where are the changes. The changed pixels shall be taken as zero and unchanged shall be as one according to the modifier. Then after getting the string of zero and one the secret message can be retrieved. Here the disadvantage is the receiver must have original image and also any changes by a third party cant be recognized [5].

2.5 LSB Technique

This is the acronym used for least significant bit technique. Images consists of pixels. These pixels can be represented in binary format. These binary representation will have 0 or 1. So changing the least significant bit will either add 1 or subtract 1 to that pixel value. This change is so small that the result of change can not be recognized by human eyes. So taking images as cover medium for steganography we can use LSB technique to hide any secret image or secret text data inside the cover image. In colour images there are 24 bits in each pixel while in gray images there are 8 bits in each pixel [5]. In colour image each pixel consists of RGB components containing 8 bits each. So if we use colour image as cover image then we have 3 bits per pixel to hide data while 1 bit for gray images. The extraction of secret message from the cover image is done using the LSB extraction method which is just the reverse one of the insertion method.

We have cover image as C, stego image as S and binary encoded secret message M. Now, the LSB technique will be as follows,
If M == 1 and C(i,j) == 0 then S(i,j) = C(i,j)+1;
If M == 0 and C(i,j) == 1 then S(i,j) = C(i,j)-1;
If M == C(i,j) then S(i,j) = C(i,j);

2.5.1 Secret Message Embedding using LSB

Input: Cover image, Secret message
Output: Stego image
1. Convert the secret message into corresponding binary encoded bit string.
2. Measure the length of the binary string.
3. Take the pixel values from gray images.
4. Change the 8th bit of the pixel according to the binary string message.
5. Repeat step 3 and 4 binary string length times.
6. Put the terminating symbol.
7. Get the Stego image.

2.5.2 Secret Message Extraction using LSB

Input: Stego image
Output: Secret Message
1. Extract the pixels from stego image.
2. Find the 8th bit value and store it in binary bit string.
3. Repeat step 1 and 2 until terminating symbol found.
4. Convert the binary bit string into character string and find secret message.

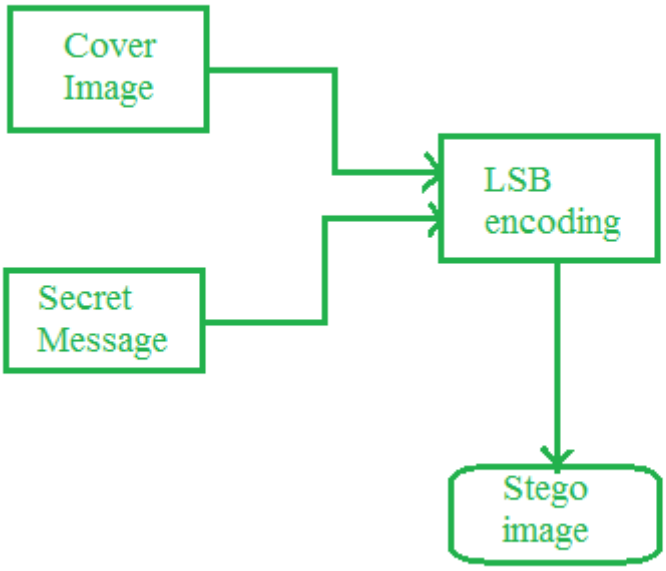

Figure 1: LSB Embedding Technique

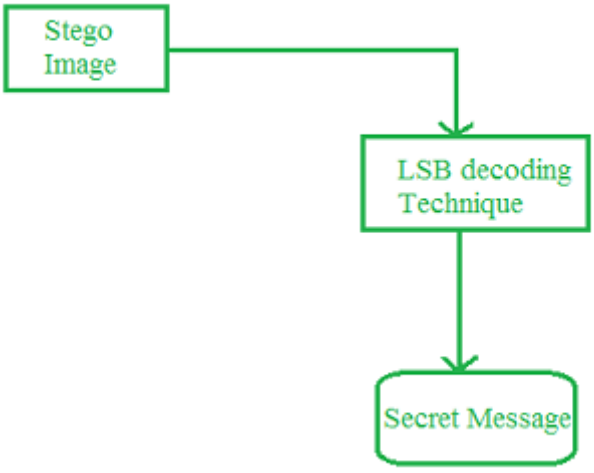

Figure 2: LSB Extracting Technique

2.6 DCT and IDCT

Here, in two dimensional DCT the gray image is first 8X8 block processed. Then DCT is applied on each non-overlapping block. After applying DCT each pixel modified to DCT coefficient in such a way that change in one pixel will be reflected in all 64 pixels [2]. It is a lossy compression method. It has only real components, no imaginary part due to absent of sine component.

In two dimensional IDCT the DCT coefficients are 8X8 block processed. Then Inverse Discrete Cosine Transformation is applied. It gives back the original image.

The two dimensional Discrete Cosine Transformation for NXN matrix is defined as:

$$F(u,v) = \frac{2}{N} C(u)C(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y) \cos \frac{(2x+1)u\pi}{2N} \cos \frac{(2y+1)v\pi}{2N}$$

Where

$$C(u), C(v) = \begin{cases} \frac{1}{\sqrt{2}} & \text{if } u, v = 0 \\ 1 & \text{else} \end{cases}$$

The Inverse Discrete Cosine Transformation is defined as below,

$$f(x,y) = \frac{2}{N} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} C(u)C(v)F(u,v) \cos \frac{(2x+1)u\pi}{2N} \cos \frac{(2y+1)v\pi}{2N}$$

2.7 DWT and IDWT

A wavelet is a wave form of effectively limited duration that has an average value of zero with varying frequency. Discrete wavelet transformation is used to analyse the frequency component of any signal as well as time component. DWT provides a multi resolution system.

So, DWT is the discrete wavelet transform which divides the image signal into four group of signals called LL or approximation band, HL or horizontal band, LH or vertical band and HH or diagonal band [4].

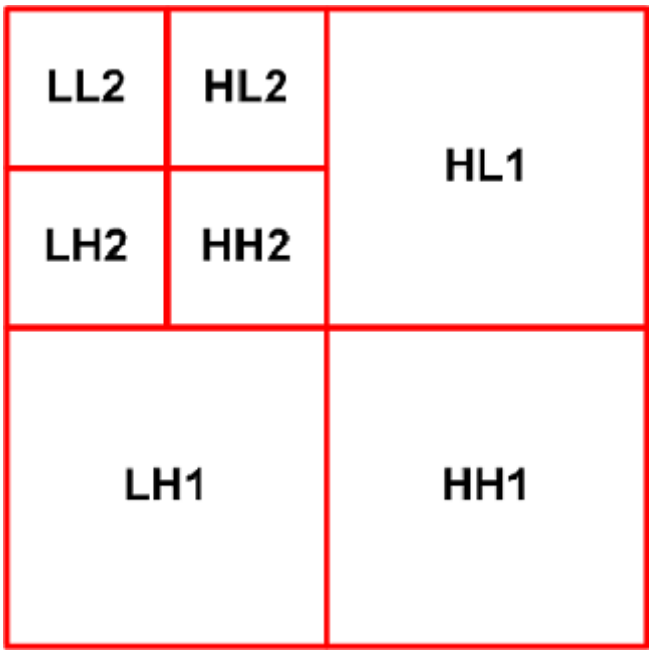

Figure 3: Two level of DWT

IDWT is inverse discrete wavelet transform. It takes the four band of image (LL, LH, HL, HH) as input and gives back the original image.

The most basic method in steganography using DWT is to apply the DWT on the cover image, the collect the high frequency band and insert the secret message there [3]. Then apply the IDWT using the four bands and get back the original image [3].

But if further DWT will be applied on the LL band of first DWT, then there will be some more bands available to insert the secret messages to it. Then, IDWT will be applied in the reverse order to the bands [4].

2.8 Huffman Coding

This is an algorithm used to compress the data size significantly. The concept here used is the alphabet with highest no of appearance will be given smaller no of bits and alphabet with lowest no of appearance will be given largest no of bits. So that unnecessary bit consumption can be checked. For retrieval a dictionary created in previous step is used [1].

From the above figure, we can see how the alphabets e, g, h, o, p, r, s, with frequencies 1, 3, 1, 3, 1, 1, 1, 2 respectively forms the Huffman tree. Then we have to put 0 on left child and 1 on right child from root to towards the leaves. Then traverse from root to leaf for the respective bit representation of symbol on leaf.

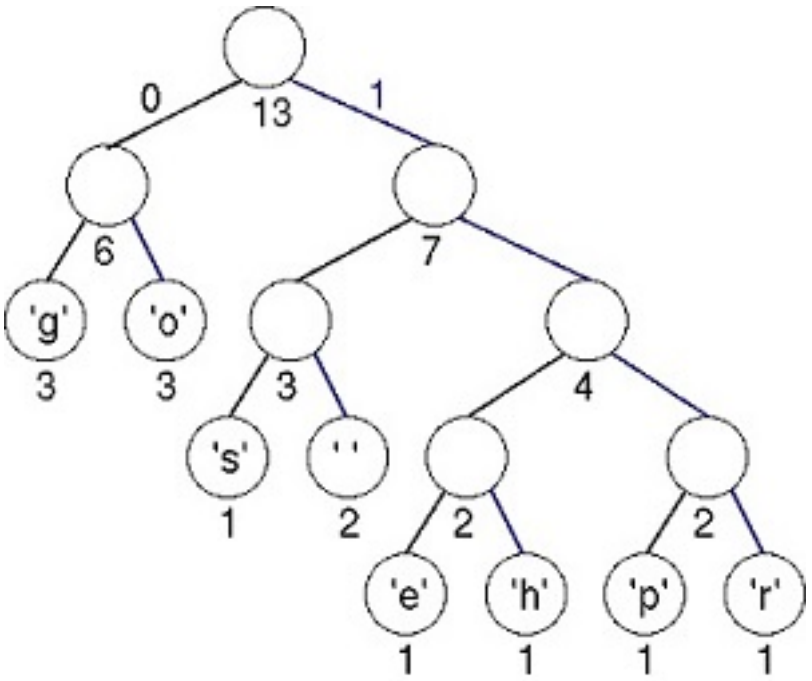

Figure 4: Huffman Tree

3 Proposed Work

Image steganography is mainly using spatial domain and transform domain. In spatial domain steganography the most commonly used method is LSB (least significant bit) insertion technique. But it can be easily attacked. But in case of transform domain steganography attack is not easy. In this paper our proposed work is based on both spatial and transform domain steganography.

We first converts the cover image into its frequency domain, then works on it using LSB technique. The secret message before inserted into cover image using LSB technique, is converted into its corresponding Huffman coded binary string. The insertion and extraction of secret message is shkown in these figures,

3.1 Embedding Algorithm for DCT Cover Image

I/P: One PXQ cover image and the secret text message.
O/P: One stego image.
Algorithm:
1. Prepare the cover image for block DCT of size 8x8 disjoint blocks.
2. Apply 2D-DCT on each block.
3. Prepare Huffman Table from the secret message.
4. Prepare Huffman encoded binary bit string of the secret message.
5. Measure the length of Huffman encoded binary bit string of secret message.
6. Insert the length into LSB of the DCT coefficient of the first block cover image.
7. Insert the bits of Huffman encoded binary bit string into the next coefficient of DCT cover image in LSB position.
8. Repeat step 7 length of Huffman encoded binary bit string times.
9. Insert the Huffman table after the Huffman encode binary bit string in LSB position.
10. Prepare 8x8 blocks of that image.
11. Apply 2D-IDCT on that image.
12. END.

3.2 Extraction Algorithm for DCT Stego Image

I/P: PXQ Stego image.
O/P: Secret message.
Algorithm:
1. Prepare the stego image for 8x8 block.

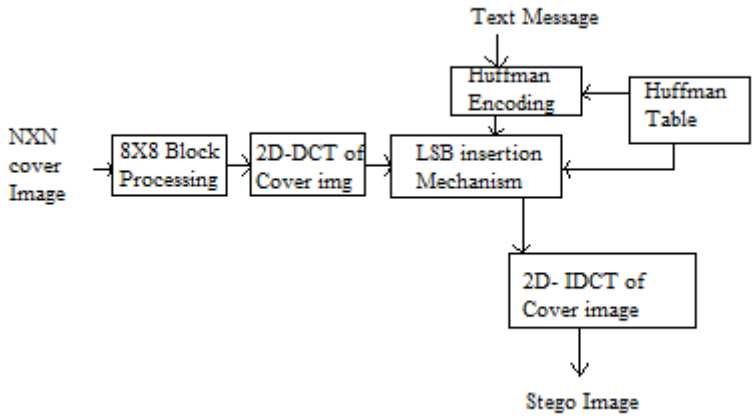

Figure 5: Embedding Algorithm using DCT

2. Apply 2D-DCT on the image.
3. Use LSB technique of extraction of length of the message by finding LSB of first 8 pixels.
4. Repeat step 5 length of message time.
5. Use LSB extraction method to get the Huffman encoded binary bit string.
6. Then extract the dictionary string from that image.
7. Apply Huffman Decoding method using Huffman encoded binary bit string and the dictionary.
8. Extract the secret message.
9. END.

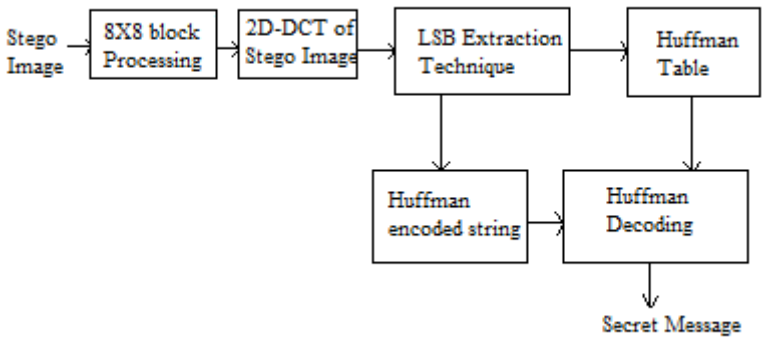

Figure 6: Extraction Algorithm using DCT

3.3 Embedding Algorithm for DWT Cover Image

I/P: One PXQ cover image and the secret text message.
O/P: One stego image.
Algorithm:
1. Apply 2D-DWT on the cover image.
2. Prepare Huffman Table from the secret message.
3. Prepare Huffman encoded binary bit string of the secret message.
4. Insert the bits of Huffman encoded binary bit string into the coefficient of DWT cover image in LSB position.
5. Insert the Huffman table after the Huffman encode binary bit string in LSB position.
6. Apply 2D-IDWT on that image.
7. END

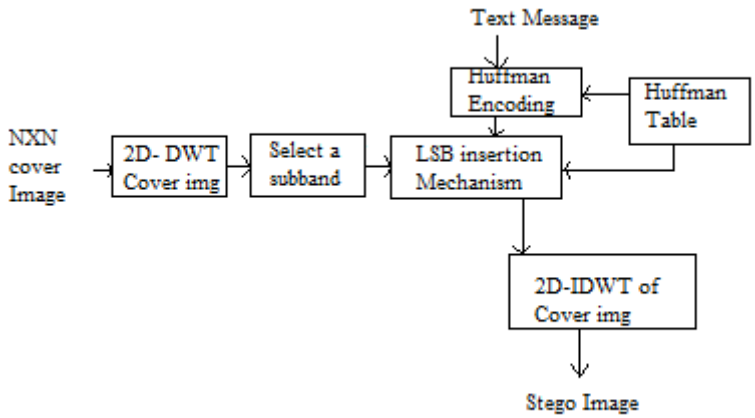

Figure 7: Embedding Algorithm using DWT

3.4 Extraction Algorithm for DWT Stego Image

I/P: PXQ Stego image.
O/P: Secret message.
Algorithm:
1. Apply 2D-DWT on the stego image.
2. Use LSB extraction method to get the Huffman encoded binary bit string.
3. Then extract the dictionary string from that image.
4. Apply Huffman Decoding method using Huffman encoded binary bit string and the dictionary.
5. Extract the secret message.
6. END

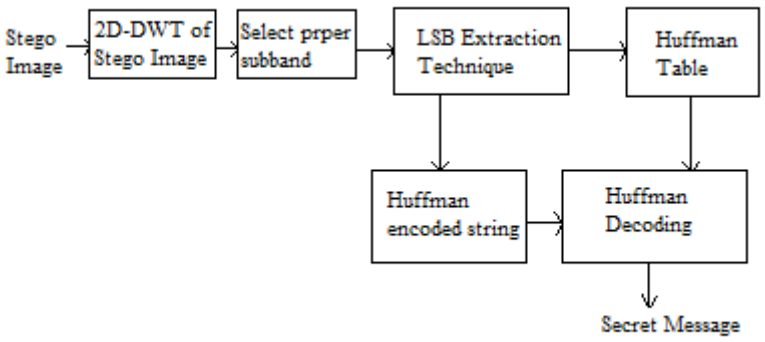

Figure 8: Extraction Algorithm using DWT

4 Simulation Results

Performance Measure

The performance of the proposed algorithm is observed by calculating most popular peek Signal to noise ratio (PSNR) value. This PSNR value will tell amount of distortion in the image due to the secret message. The formula is given by,

$$PSNR = \log_{10}\left(\frac{C_{max}}{\sqrt{MSE}}\right)$$

where C_{max}= Maximum pixel value, MSE= Mean Square Error

MSE is calculated as follows

$$MSE = \frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}[C(i,j) - S(i,j)]^2$$

where C is the cover image and S is the stego image. C(i,j) and S(i,j) are the pixel values of cover image and stego image respectively.

PSNR value is calculated in terms of dB. More the PSNR value better is the result , that means the cover image and stego image will look more similar. If PSNR value is less then the cover image and stego image will not look similar [1].

In this section we have some experimental results to prove the efficiency of the proposed algorithm. The experiment is carried out using MATLAB2012 in Windows 8, 64 bit Operating system. A set of 8bit gray scale images of size 512x512 are taken as cover image and stego image is created. The following figures are the cover images and we have taken some text lines as secret message. The result is shown in the Table 1 and 2.

The secret message used here is "Computer Science and Engineering NIT Rourkela".

Table 1: PSNR value using DCT and Huffman coding

No	IMAGE	Size(kb)	PSNR(dB)
1	Galaxy S6	53.4	29.8607
2	Fish	152.0	28.6935
3	BatMan	40.2	37.5976
4	CSE2015	100.0	29.3118
5	CircuitBoard	152.0	36.7474
6	Tiger	133.0	32.1469

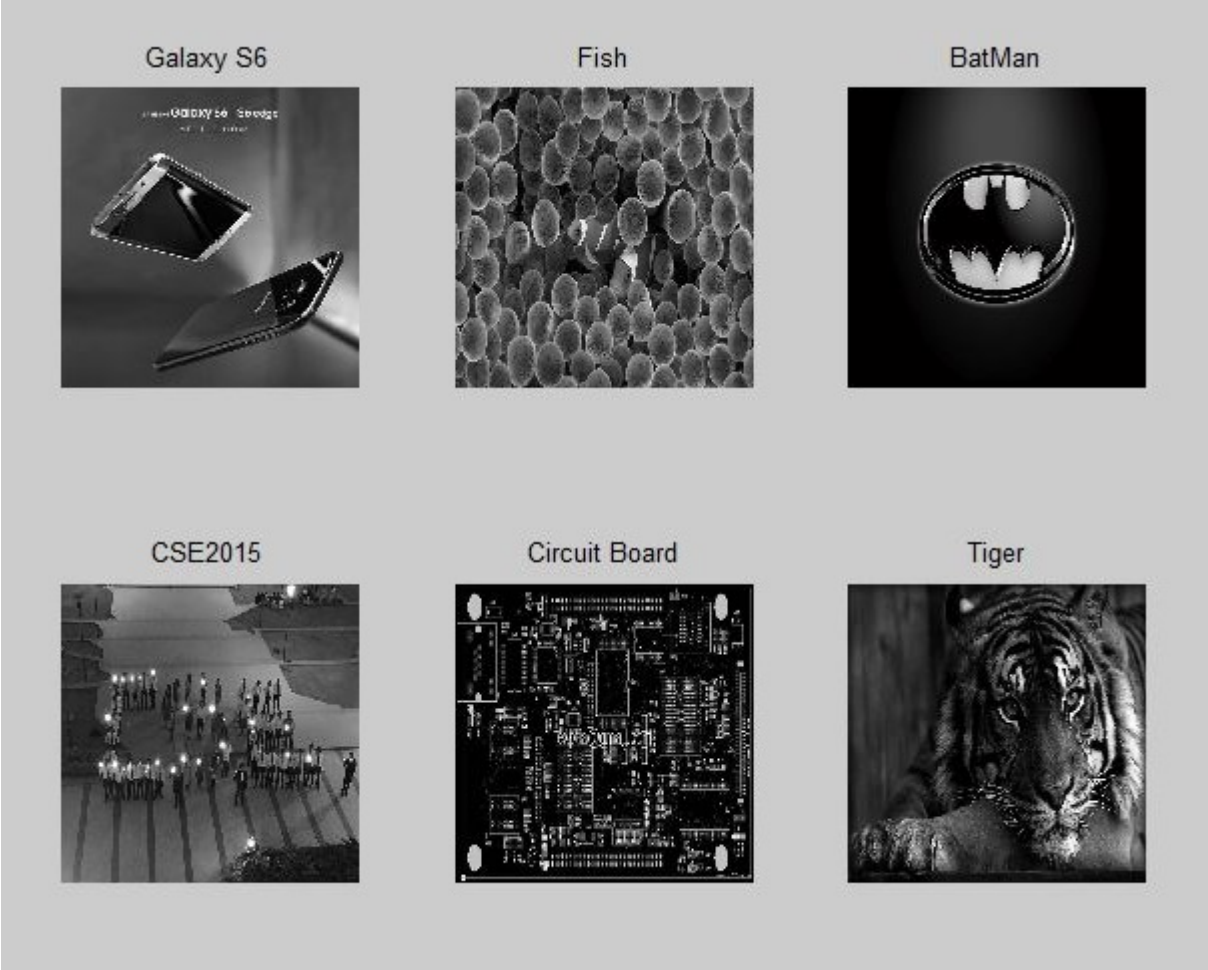

Figure 9: Gray Cover Images

Table 2: PSNR value using DWT and Huffman coding

No	IMAGE	Size(kb)	PSNR(dB)
1	Galaxy S6	53.4	39.4015
2	Fish	152.0	39.0908
3	BatMan	40.2	44.0167
4	CSE2015	100.0	39.7052
5	CircuitBoard	152.0	50.6943
6	Tiger	133.0	39.7392

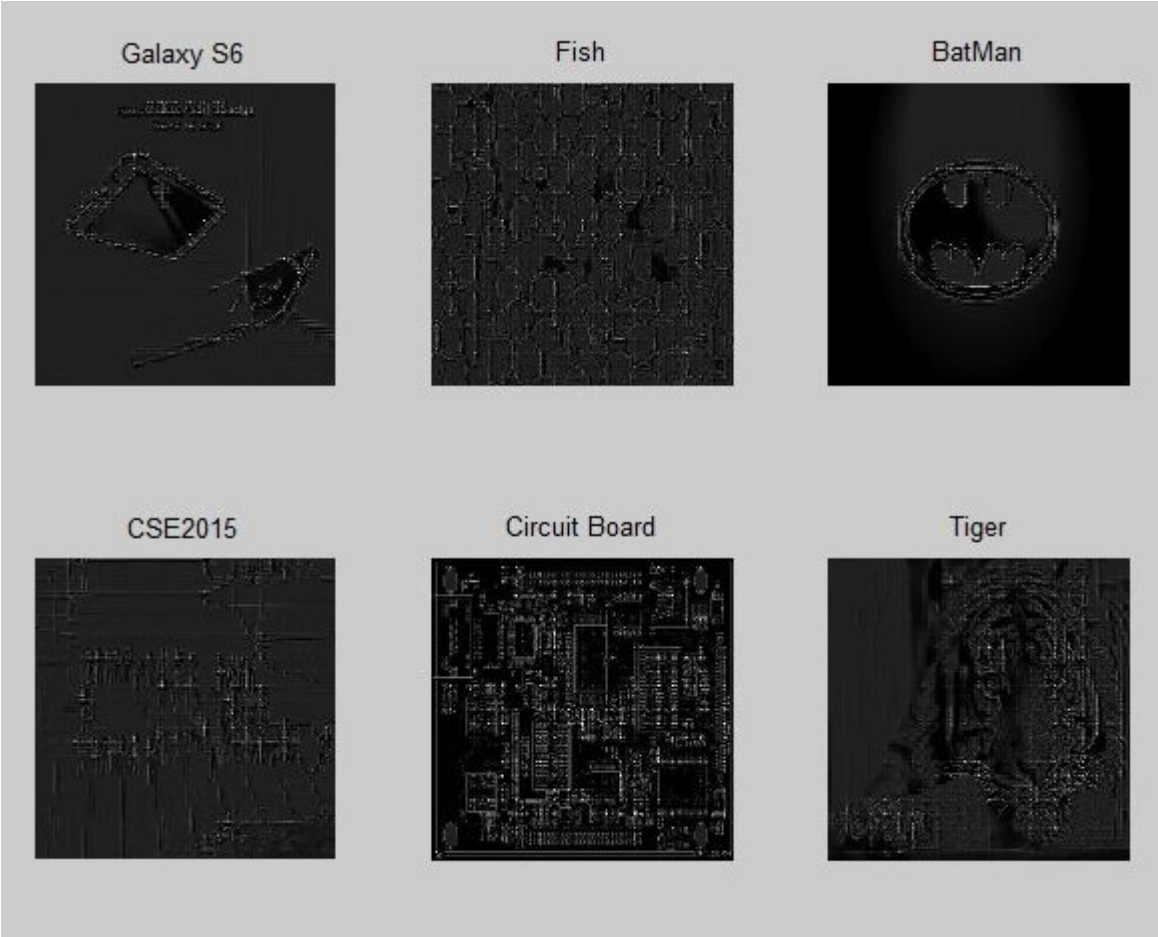

Figure 10: Stego Image using DCT

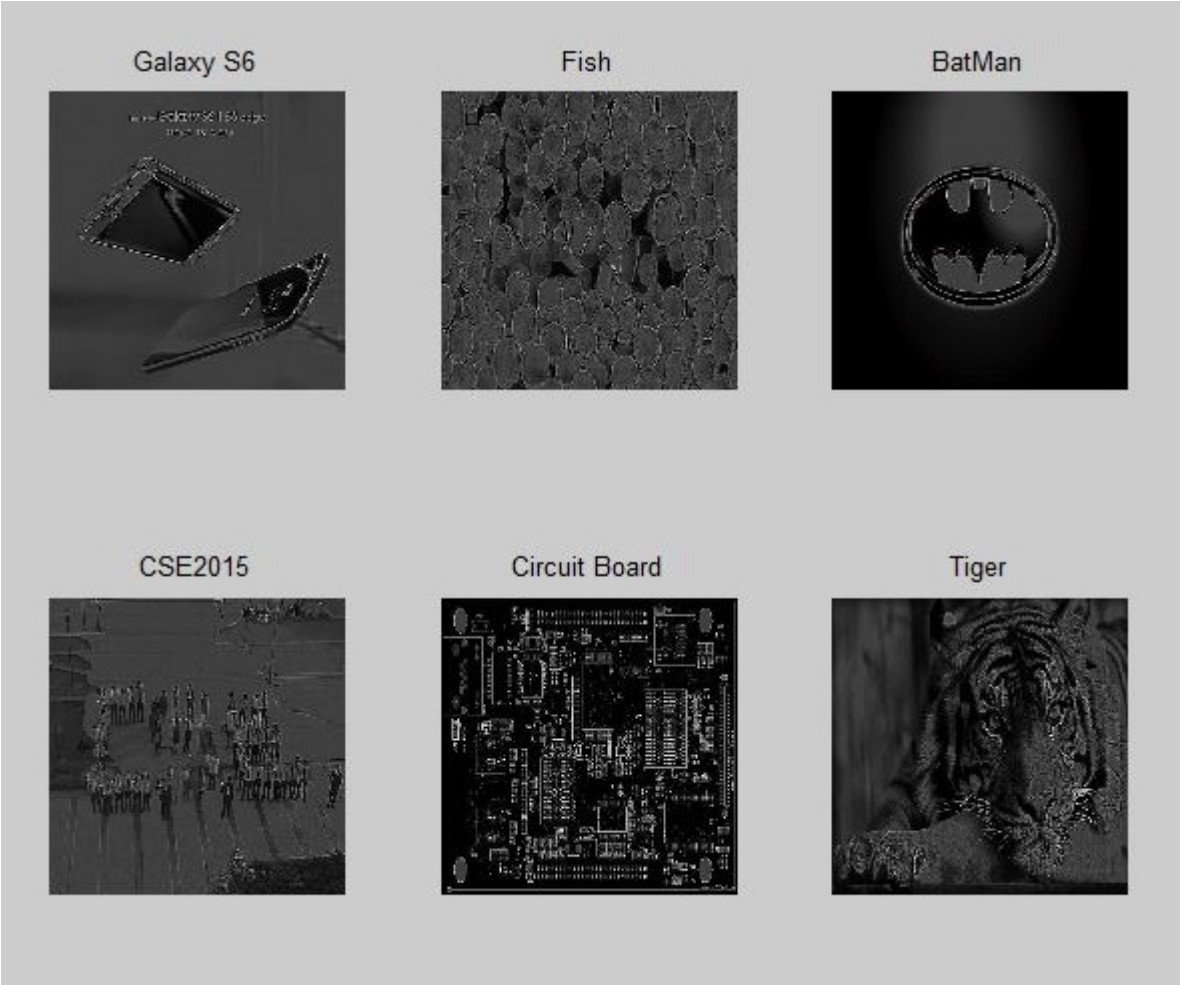

Figure 11: Stego Images using DWT

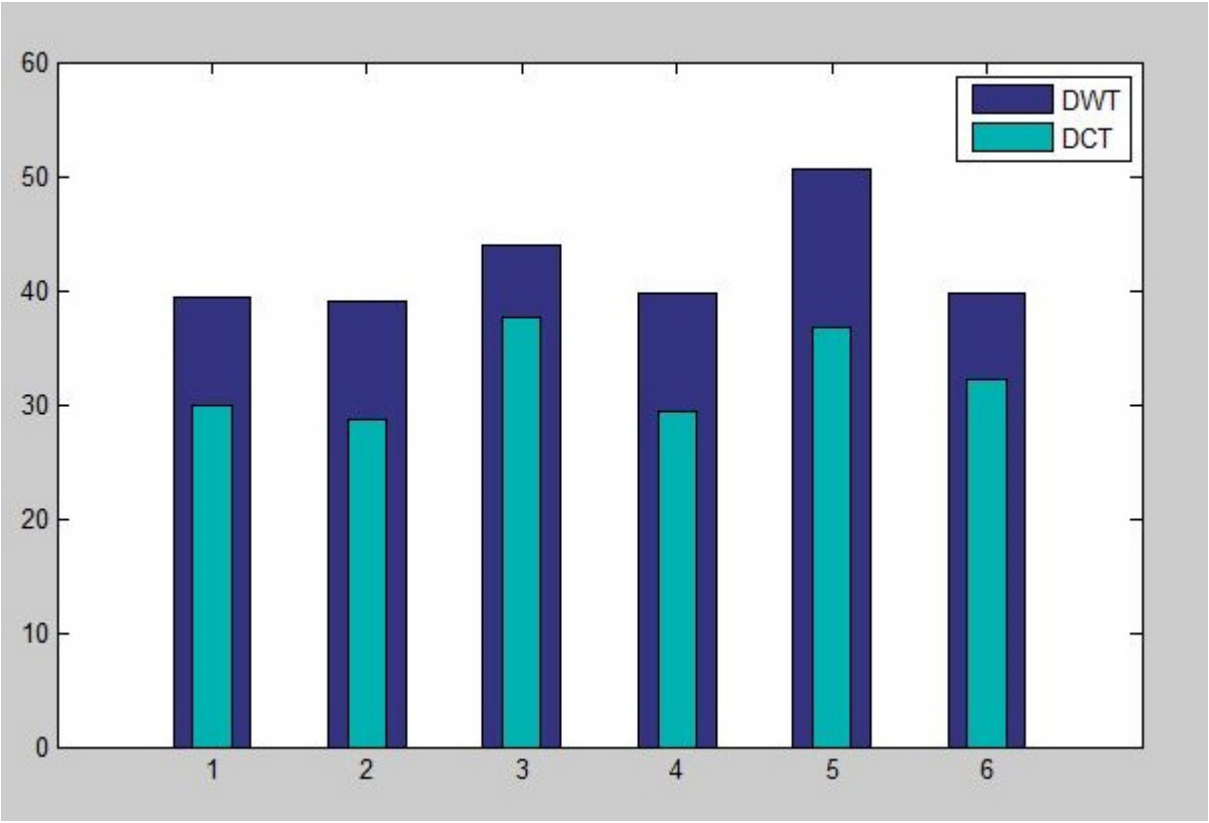

Figure 12: DCT and DWT stego Image PSNR values

5 Conclusion

Steganography is a very good method for sending confidential information through digital media. We have compared two methods of steganography using DCT, Huffman Encoding and LSB technique with DWT, Huffman Encoding and LSB Technique. It is found that for all the cover images used, have better corresponding stego image PSNR value in case of DWT, Huffman Encoding and LSB Technique. So, in place of DCT we can use DWT in steganography for better PSNR value of the stego image. This paper mainly focuses to increase PSNR and to reduce the distortion in the stego image.

References

[1] A. Nag, S. Biswas, D. Sarkar, and P. P. Sarkar *A novel technique for image steganography based on Block-DCT and Huffman Encoding*, International Journal of Computer Science and Information Technology, Volume 2, Number 3, June 2010.

[2] K. B. Raja, C. R. Chowdary, K. R. Venugopal, and L. M. Patnaik *A secure image steganography using LSB, DCT and compression techniques on raw images*, Intelligent Sensing and Information Processing, 2005. ICISIP 2005. Third International Conference on , 170-176, 2005, IEEE.

[3] A. Nag, S. Biswas, D. Sarkar, and P. P. Sarkar *A novel technique for image steganography based on DWT and Huffman encoding*, International Journal of Computer Science and Security , 2011.

[4] S. V. Joshi, A. A. Bokil, N. A. Jain, and D Koshti *Image steganography combination of spatial and frequency domain*, International Journal of Computer Applications , 53, 5, 2012, Citeseer.

[5] K. J. Devi and S. K. Jena *A Sesure Image Steganography Using LSB Technique and Pseudo Random Encoding Technique*, National Institute of Technology Rourkela , 2013.

[6] B. A. Forouzan *Cryptography And Network Security (Sie)*, McGraw-Hill Education (India) Pvt Limited , 2011.