



Tribhuvan University

Institute of Science and Technology

**Analysis of Frequency Domain Image Steganography using DCT,
DWT and DCT with DWT**

Thesis

Submitted to

Central Department of Computer Science and Technology

Kirtipur, Kathmandu, Nepal

In partial fulfillment of the requirements

for the Master's Degree in Computer Science and Information Technology

By

Sajina Maharjan

T.U. Registration No.: 5-2-22-1670-2007

T.U. Examination No.: 75/069

Date (April, 2019)

Supervisor

Mr. Jagdish Bhatta



Tribhuvan University

Institute of Science and Technology

Central Department of Computer Science and Information Technology

Student's Declaration

I hereby declare that I am the only author of this work and that no sources other than listed here have been used in this work.

Sajina Maharjan

Date: April, 2019



Tribhuvan University

Institute of Science and Technology

Central Department of Computer Science and Information Technology

Supervisor's Recommendation

I hereby recommend that this thesis prepared under my supervision by **Ms. Sajina Maharjan** titled “**Image Steganography Using DCT, DWT, DCT with DWT**” in partial fulfillment of the requirements for the degree of MSc in Computer Science and Information Technology be processed for the evaluation.

Asst. Prof. Jagdish Bhatta

Central Department of Computer Science and Information Technology,

Tribhuvan University,

Kathmandu, Nepal

(Supervisor)

Date: April, 2019



Tribhuvan University
Institute of Science and Technology
Central Department of Computer Science and Information Technology

LETTER OF APPROVAL

We certify that, we have read this thesis and in our opinion it is satisfactory in the scope and quality as a thesis in partial fulfillment for the requirement of Master's Degree in Computer Science and Information Technology.

Evaluation Committee

Asst. Prof. Jagdish Bhatta
Central Department of CSIT
Tribhuvan University
Kirtipur, Kathmandu, Nepal
(Supervisor)

Asst. Prof. Nawaraj Poudel
Central Department of CSIT
Tribhuvan University
Kirtipur, Kathmandu, Nepal
(Head of Department)

External Examiner

Internal Examiner

Acknowledgement

I offer my profound gratitude to my supervisor Asst. Prof. Jagdish Bhatta (Tribhuvan University) for his generous advice, inspiring guidance and encouragement throughout my research for this thesis. Without his kind and patient review of this work, it would have been impossible to complete this study.

I would like to extend my gratitude to Asst. Prof. Nawaraj Paudel (Head of Department, CDCSIT) and faculties for their guidance and help throughout my Masters Study and help for the completion of my thesis.

Last but not the least; I would like to express my gratitude to all my family members, friends and all other people who have helped me directly or indirectly in the completion of this thesis.

Abstract

Steganography is art and science of hiding communication. Image Steganography the process of hiding secret message in a cover image. Frequency domain hides the secret bits in the significant parts of the cover image. It tries to encode messages bits in the transform domain coefficients of the image. DCT and DWT come under frequency domain technique. This research evaluates the DCT, DWT and DCT with DWT algorithm using four measures: Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UCI) to measure the strength of the algorithms. The result shows that DCT with DWT is better than the two algorithms DCT and DWT. The PSNR value of the combined method has the highest value amount other two techniques. Using DCT with DWT, the original image and the stego image is similar without losing its image properties. The average PSNR value for DCT with DWT is 78.73, DWT is 76.62 and DCT is 73.56. The PSNR value of DCT with DWT method has higher value than other two techniques which verifies that the original image and stego image is similar without losing much of its image properties. But DCT and DWT has significantly has lower PSNR value, this value of PSNR results in a change of visual properties of the image. The average encoding value for DCT with DWT is 0.385045, DWT is 1.524587 and DCT is 1.09904 and decoding value for DCT with DWT is 0.173457, DWT is 0.117165 and DCT is 0.524236. The DCT with DWT has good differential analysis value which has average value 65.27% and 0.65 % for the NPCR and UACI respectively for different set of images used during analysis.

Keywords: *Steganography, cover image, stego image, DCT, DWT*

Table of Contents

CHAPTER 1	1
INTRODUCTION	1
1.1 Introduction	1
1.2 Problem Statement	2
1.3 Objective	3
1.4 Scope	3
1.5 Report Organization	4
CHAPTER 2	5
BACKGROUND STUDY AND LITERATURE REVIEW	5
2.1 Background Study	5
2.2 Basic Framework of Steganography	6
2.3 The Purpose of Steganography	7
2.4 Types of Steganography	7
2.5 Image Formats	8
2.6 Steganography Domains and Techniques	9
2.7 Literature Review	12
CHAPTER 3	16
METHODOLOGY	16
3.1 Framework	16
3.2 Discrete Cosine Transformation (DCT)	17
3.3 Discrete Wavelet Transformation (DWT)	22
3.3 DCT with DWT	25
3.4 Performance Evaluation Parameters	25
CHAPTER 4	28
IMPLEMENTATION AND ANALYSIS	28
4.1 Implementation	28
4.1.1. Programming Language and Framework	28
4.1.2. MATLAB R2016a overview	28
4.1.3. Image separation in RGB Plane	28

4.3 Encoding the secret message	29
4.4 Decoding the secret message	30
4.3. Result Analysis	31
4.3.1. Visual assessment analysis	31
5.2.2 Computational Speed Analysis	35
5.2.3 Differential Analysis	38
5.2.4 Statistical Analysis	40
5.3 Result	44
CHAPTER 6	45
CONCLUSION AND FUTURE RECOMMENDATION	45
6.1 Conclusion	45
6.2 Future Recommendation	45
References	46
Appendix	49

List of Tables

Table 5.1: PSNR in secondary data	32
Table 5.2: PSNR in secondary data (cont.).....	33
Table 5.3: PSNR in Primary Data.....	34
Table 5.4: Encoding and Decoding Time of Secondary Images	35
Table 5.5: Encoding and Decoding time of Primary Images.....	37
Table 5.6: NPCR and UACI of Secondary Images.....	38
Table 5.7 NPCR and UACI of Primary Image	40

List of Figures

Figure 2.1: General Steganography System.....	7
Figure 2.2: Types of Steganography	7
Figure 2.3: Components of 1-level 2-Dimensional Discrete Wavelet Transform	12
Figure 3.4: Message Embedding using DCT with DWT.....	16
Figure 3.5: Components of 1-level 2-Dimensional Discrete Wavelet Transform	23
Figure 3.6: Horizontal Operations	24
Figure 3.7: Vertical Operations.....	24

List of Abberrations

DCT	(Discrete Cosine Transformation)
DWT	(Discrete Wavelet Transformation)
PSNR	(Peak Signal to Noise Ratio)
MSE	(Mean Square Error)
LSB	(Least Significant Bit)
HVS	(Human Visual System)
NPCR	(Number of Pixel Changed Rate)
UACI	(Unified Average Changed Intensity)
JPEG	(Joint Photographic Experts Group)
BMP	(Bitmap)
GIF	(Graphics Interchange Format)
TIFF	(Tagged Image File Format)

CHAPTER 1

INTRODUCTION

1.1 Introduction

In this modern era, computers and internets are major communication media that connect different parts of the world as one global virtual world. As a result people can easily exchange information and distance is no longer barrier to the communication. However the safety and security of long- distance communication remains as issue. This is particularly important in the case of confidential data. The need to solve this problem has led to the development of the steganography techniques. . At times when we communicate, we prefer that only the intended recipient have the ability to decipher the content of the communication. We want to keep the message secret. A common solution to this problem is encryption. While encryption the meaning of the communication, instances exist where we would prefer that the entire communication process not be evident to any observer that is, even the fact that communication is taking place is secret. In this case, we want to keep communication hidden. Steganography can be used to hide or cover the existence of communication.

The performance of the steganographic system can be measured using several properties. The most important property is the statistical undetectability (imperceptibility) of the data, which shows how difficult it is to determine the existence of a hidden message. Other associate measures are the steganographic capacity, which is the maximum information that can safely embedded in a work without having statistically detectable objects [15] and robustness, which refers to how well the steganographic system resists the extraction of the hidden data.

The advantage of using image files in hiding information is the large amount of redundant space is created in storing the images and added security against the attack of hacker due to the relative complexity of the structure of image compare to text. A digital image is described using a 2-D matrix of the color intestines at each grid point (i.e. pixel). Typically gray images use 8 bits, whereas colored utilizes 24 bits to describe the color model, such as RGB model. The steganography system which uses an image as the cover, there are several techniques to conceal information inside cover-image. The spatial domain techniques manipulate the cover-image pixel bit values to embed the secret information. The secret bits are written directly to the cover image

pixel bytes. Consequently, the spatial domain techniques are simple and easy to implement. The Least Significant Bit (LSB) is one of the main techniques in spatial domain image steganography. Spatial domain techniques either operate on pixel wise or block wise bases. The advantage of the method is that the amount of data that can be embedded is more in LSB techniques.

A Steganography system consists of three elements: cover image (which hides the secret message), the secret message and the stego-image (which is the cover object with message embedded inside it).

Image steganography techniques can be divided into two groups: spatial domain and frequency domain. Spatial domain techniques embed message in the intensity of pixel directly. The commonly used spatial domain technique is Least Significant Bit insertion (LSB). In this method the encoder adds a sequence of changes to the cover image. So, information is described as being stored by signal distortion. Statistical techniques are vulnerable to rotating, cropping, scaling attacks and also all the watermarking attacks. These embedding techniques are applicable mainly to lossless image-compression schemes like TIFF images. For lossy compression schemes like JPEG, some of the message bits get lost during the compression step. Thus the frequency domain is processed to overcome the shortcoming of LSB i.e. weak resistance to attacks. In this method, pixel values are transformed and that transformed coefficients processing is applied. Frequency domain [2] hides the secret bits in the significant parts of the cover image. It tries to encode messages bits in the transform domain coefficients of the image. The frequency domain includes Discrete Cosine Transformation (DCT), Discrete Wavelet Transformation (DWT). This study aims at analyzing image steganography using DCT, DWT and DCT with DWT.

1.2 Problem Statement

The massive growth in the information technology and internet has made the distribution of digital content very easy and at low cost. But this progress has also led to many serious problems such as unauthorized access and malicious attacks to the digital information. Even though there are cryptographic mechanisms to maintain integrity and security of information, they deal by message encryption with a condition that the communication is visible and suspicious to

attackers. On the other hand, steganography deals with secret message hiding with the condition that the communication is not visible. Steganography technique hides the existence of the message so that intruders cannot detect what communication is going on, thus providing an advanced level of security.

The images are convincing for steganographic applications because they have a high degree of redundancy in the presentation and pervasive applications. This results a growing interest in research on image steganography. Number of approaches like spatial domain and frequency domain exist for image steganography. Even though there are computationally fast spatial domain approaches for image steganography but they are sensitive and weak to image processing attacks. Thus frequency domain approaches has been of great interest for researchers since they have an advantage of being more secure and noise tolerant. Since the frequency approach contains transforming the cover image into the frequency domain coefficients before embedding secret messages, thus determining the effect of embedding the secret messages into different bands of cover image is of utmost research. In this context, evaluating the performance of the frequency domain methods viz. DCT, DWT and DCT with DWT by the image quality and imperceptibility is the focused problem of this study.

1.3 Objective

The objectives of the research is to implement and analyze the image steganography system based on DCT and DWT techniques using different analysis parameters like Peak Signal to Noise Ratio (PSNR) , Mean Square Error (MSE), Number of Pixel Change Rate (NPCR) and Unified Average Change Intensity.

1.4 Scope

The scope of this research is

1. Hiding data in image steganography
2. Using DCT, DWT and DCT with DWT
3. Testing on cover image with 256 * 256, 512*512 and 1024*1024 resolution only.

4. JPEG image is chosen to be used in this thesis since it is most common image file format in internet as well.

1.5 Report Organization

The organization of this thesis is as follows:

Chapter 2 describes the reviews of the existing researches related to steganography techniques, different types of steganography and image formats.

Chapter 3 describes the framework to embed the secret message inside the steganography image and extracting the secret message hidden inside the image back from stego image.

Chapter 4 describes the implementation of the algorithms and the data set description together with the experimental result of different techniques and comparison using different measures.

Chapter 6 describes the conclusion and future work of the thesis

CHAPTER 2

BACKGROUND STUDY AND LITERATURE REVIEW

2.1 Background Study

Steganography is art and science of hiding communication. A steganographic system thus embeds hidden content in unremarkable cover media so as not to arouse an eaves-dropper's suspicion [16]. It is also define as hidden writing , whether it consist of invisible ink on paper copyright information hidden in an audio file, image file or video file. The word “**Steganography**” derived from the Greek word steganos which means covered or secret, and graphy (writing or drawing). Higher the quality of video, image or sound, more redundant bits are available for hiding. Application of Steganography varies from military, industrial application to copyright. Traditionally, Steganography was based on hiding secret information in image and audio files [18]. But modern work suggests that there has been growing interest among research fraternity in applying stenographic techniques to video files as well. Videos are the collection of frames and audio either in compressed domain or uncompressed domain.

2.1.1 History of Steganography

Steganography goes back to ancient times and used by different cultures such as: Greeks, Chinese, and medieval Europe. A famous which case dates back to 1586, when Mary Queen of Scots was conspiring to have Queen Elizabeth of England assassinated, with a view to taking over the English throne [22]. Also during the 1980's, Margaret Thatcher became so irritated at press leaks of cabinet documents that she had the word processors programmed to encode their identity in the word spacing, so that disloyal ministers could be traced [23]. Similar techniques are now undergoing trials in an electronic publishing project, with a view to hiding copyright messages and serial numbers in documents. In some applications, it is enough to hide the identity of either the sender or the recipient of the message, rather than its very existence [11]. Modern steganography entered the world in 1985 with the advent of the personal computer being applied to classical steganography problems. Also in modern Steganography practice the larger the cover message is relative to the hidden message, the easier it is to hide the latter [20].

2.2 Basic Framework of Steganography

An Example of steganography can be given in terms of communication between two people, Alice and Bob, where Alice and Bob are two inmates who wish to communicate in order to exchange some secret information. However, all communication between them is examined by the eavesdropper, Wendy, the third party who will try hardly to disclose, alter and/or destruct their secret message.

Specifically, in the general model for steganography, illustrated in Figure 2.1, Alice wishes to send a secret message m to Bob. In order to do so, she "embeds" m into a cover-object c , and obtains stego-objects. The stego-objects are then sent through the public channel. Thus we have the following definitions:

- i. **Cover-object:** is the object used as the carrier to embed messages into many different objects have been employed to embed messages into for example images, audio, and video as well as file structures, and html pages to name a few.
- ii. **Stego-key:** is the code that the sender of the secret message is going to use to embed the message into the cover-object. This same stego-key will be used by the recipient to extract the secret message.
- iii. **Stego-object:** is the combination of the cover object, the stego-key and the secret message.

In a pure steganography framework, the technique for embedding the message is unknown to Wendy and shared as a secret between Alice and Bob. However, it is generally considered that the algorithm in use is not secret but only the key used by the algorithm is kept as a secret between the two parties, this assumption is also known as Kerchoff's principle in the field of cryptography. The secret key, for example, can be a password used to seed a pseudo-random number generator to select pixel locations in an image cover-object for embedding the secret message (possibly encrypted). Hence, there is a need for a cover media, stego function, stego-key and the secret message to be hidden. The cover media can be a plaintext, still image, video and audio. Performing data hiding in Image was studied in a wide variety of literatures.

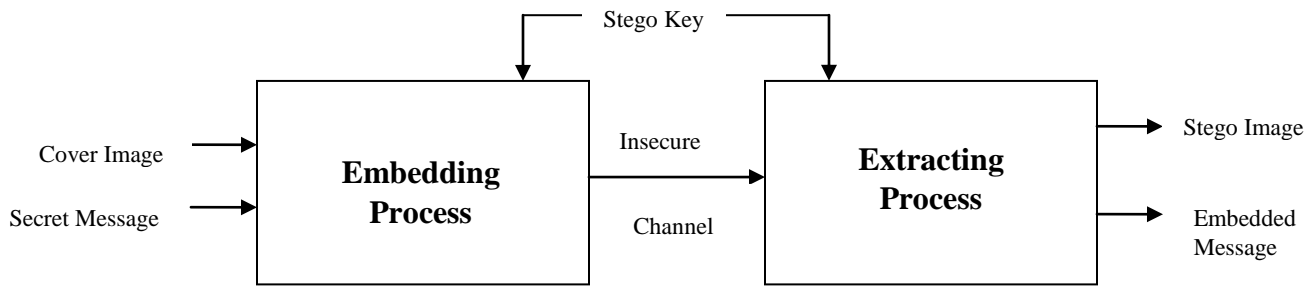


Figure 2.1: General Steganography System

2.3 The Purpose of Steganography

According to the major objective of steganography is to prevent some unintended observer from stealing or destroying the confidential information. There are some factors to be considered when designing a steganography system: [6]

- i. **Invisibility:** Invisibility is the ability to be unnoticed by the human.
- ii. **Security:** Even if an attacker realizes the existence of the information in the stego object it should be impossible for the attacker to detect the information. The closer the stego image to the cover image, the higher the security. It is measured in terms of Peak Signal to Noise Ratio (PSNR).

2.4 Types of Steganography

There are mainly four main types of steganography. They are steganography in text, steganography in image, steganography in audio and steganography in video.

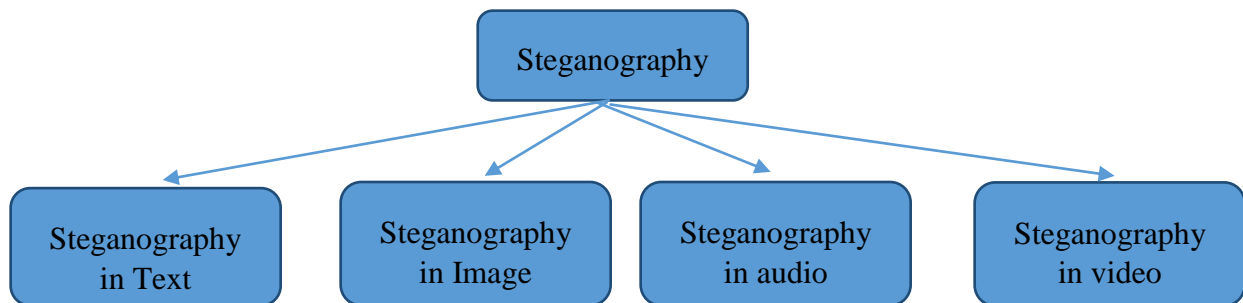


Figure 2.2: Types of Steganography

2.4.1 Steganography in Text

Text steganography can be achieved by altering the text formatting, or by altering certain characteristics of textual elements (e.g. characters). The goal in the design of coding methods is to develop alterations that are reliably decodable (even in the presence of noise) yet largely indiscernible to the reader. Text steganography using digital files is not used very often because the text files have a very small amount of redundant data.

2.4.2 Steganography in Audio

Audio steganography is masking, which exploits the properties of the human ear to hide information unnoticeably. An audible, sound becomes inaudible in the presence of another louder audible sound. This property allows the selection of the channel in which the information will be hidden. Although it is similar to images in steganographic potential, the larger size of meaningful audio files makes them less likely to use than images.

2.4.3 Steganography in Video

A video is combination of images and sound. So, huge amount of secret data can be encoded in video files. Video files such as MPEG, MP4, and AVI etc. can be used for hiding secret information.

2.4.4 Steganography in Image

Image is use as cover image in image steganography because images are most popular file format in steganography. They are known for constituting a non-causal medium, due to the possibility to access any pixel of the image at random. In addition, the hidden information could remain invisible to the eye. However, the image steganography techniques will exploit "holes" in the Human Visual System (HVS) [15].

2.5 Image Formats

There are different types of image format that is use in image steganography. They are as follows:

2.5.1 JPEG Format

Joint Photographic Experts Group (JPEG) format is one of the Transform Domain Techniques which has an advantage over LSB techniques because they hide information in areas of the image that are less exposed to compression, cropping, and image processing [15]. Also JPEG is most common image file format on the internet owing to the small size of resultant images obtained by using it, and it is efficient for appearing the stage image to something similar to the original image [17].

2.5.2 BMP Format

The letters “BMP” stand for “bitmap”, Bitmap images were introduced by Microsoft to be a standard image file format between users of their Windows operating system. The file format is now supported across multiple file systems and operating systems, but is being used less and less often. A key reason for this is the large file size, resulting from poor compression and verbose file format. This is, however, an advantage for hiding data without raising suspicion. To understand how bitmap images can be used to conceal data, the file format must first be explained. A bitmap file can be broken into two main blocks, the header and the data. The header, which consists of 54 bytes, can be broken into two sub-blocks. These are identified as the Bitmap Header, and the Bitmap Information. Images which are less than 16 bit have an additional sub-block within the header labeled the Color Palette [1].

2.5.3 GIF Format

Graphics Interchange Format is used for the purpose of storing multiple bitmap images in a single file for exchange between platforms and images. It is often used for storing multibit graphics and image data. GIF is not associated with a particular software application but was designed “to allow the easy interchange and viewing of image data stored on local or remote computer systems” [19].

2.6 Steganography Domains and Techniques

Image steganography techniques can be divided into two groups: spatial domain and frequency domain. Spatial domain techniques embed message in the intensity of pixel directly. While in the frequency-domain, it is necessary to transform the host-image first using a frequency-oriented mechanism, such as a discrete cosine transformation based (DCT-based), wavelet-based, etc.,

after which the secret is then combined with the relative coefficients in the frequency-form image. The least significant bit (LSB for short) secret embedding or LSB-like embedding is the most commonly used method in the spatial-domain approach [22].

2.6.1 Spatial Domain

These techniques use the pixel gray levels and their color values directly for encoding the message bits. These techniques are some of the simplest schemes in terms of embedding and extraction complexity. The major drawback of these methods is amount of additive noise that creeps in the image which directly affects the Peak Signal to Noise Ratio (PSNR) and the statistical properties of the image. These embedding techniques are mainly applicable to the lossless image compression scheme like TIFF images. LSB is the most common replacement algorithm.

2.6.1.1 Least Significant Bit Algorithm

In this method the encoder adds a sequence of changes to the cover image. So, information is described as being stored by signal distortion. Statistical techniques are vulnerable to rotating, cropping, scaling attacks and also all the watermarking attacks.

When using the least significant bit of the pixels' color data to store the hidden message, the image itself is seemed unaltered. A proper cover image is needed to hide a secret message. It is necessary to use a lossless compression format, because this method uses bits of each pixel in the image, otherwise the hidden information will get lost in the transformations of a lossy compression algorithm. When using a 24-bit color image, a bit of each of the red, green and blue color components can be used, so a total of 3 bits can be stored in each pixel. For example, the following grid can be considered as 3 pixels of a 24-bit color image, using 9 bytes of memory:

(00100111 11101001 11001000)

(00100111 11001000 11101001)

(11001000 00100111 11101001)

When the character A, which binary value equals 10000001, is inserted, the following grid results:

(00100111 11101000 11001000)

(00100110 11001000 11101000)

(11001000 00100111 11101001)

In this case, only three bits are needed to be changed to insert the character successfully. On average, only half of the bits in an image will be needed to be insider modified to hide a secret message using the maximal cover size. The result changes that are made to the least significant bit are too small to be recognized by the human visual system (HVS), so the message is effectively hidden [12].

2.6.2 Frequency Domain

Frequency domain [2] hides the secret bits in the significant parts of the cover image. It tries to encode messages bits in the transform domain coefficients of the image. These techniques are widely used for robust watermarking. This technique includes DCT (Discrete Cosine Transformation), DWT (Discrete Wavelet Transformation) and DFT (Discrete Fourier Transformation). By being embedded in the transform domain, the hidden data resides in more robust areas, spread across the entire image, and provides better resistance against signal processing. The hidden data resides in more robust area by embedding in the transformation domain and spread across entire image, provide better resistance against signal processing.

2.6.2.1 Discrete Cosine Transformation (DCT)

The DCT helps separate the image into parts of differing importance (with respect to the image's visual quality). DCT can be carried out by partitioning/sectioning the image into equally size 2D blocks i.e., $N \times N$ grids (e.g., 8×8 grid containing 64 pixels per grid). The DCT coefficients $F(u,v)$ of an 8×8 block of image pixels $f(x, y)$ are given by [2]

$$f(u, v) = \frac{1}{4} C(i) C(j) \sum_{x=0}^7 \sum_{y=0}^7 p(x, y) \cos\left[\frac{(2x+1)u\pi}{16}\right] \cos\left[\frac{(2x+1)v\pi}{16}\right] \dots \dots \text{Eq}(2.1)$$

Where,

$P(x,y)$ is the x, y^{th} element of the image represented by the matrix p .

N is the size of the block that the DCT is done.

The equation calculates one entry (i,j^{th}) of the transformed image from the pixel values of the original image matrix. For standard $8*8$ block, N equals 8 and x and y range from 0 to 7. Because

the DCT uses cosine function, the resulting matrix depends on the horizontal, diagonal, and vertical frequencies.

2.6.2.2 Discrete Wavelet Transformation

Wavelets are special functions which (in a form analogous to sines and cosines in Fourier analysis) are used as basal functions for representing signals. The discrete wavelet transform (DWT) we applied here is Haar-DWT, the simplest DWT. In Haar-DWT the low frequency wavelet coefficient are generated by averaging the two pixel values and high frequency coefficients are generated by taking half of the difference of the same two pixels.

For 2-D images, applying DWT (Discrete Wavelet Transform) separates the image into a lower resolution approximation image or band (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components.

LL ₀	HL ₀
HL ₁	HH ₁

Figure 2.3: Components of 1-level 2-Dimensional Discrete Wavelet Transform

With the DWT, the significant part(smooth parts) of the spatial domain image exist in the approximation band that consists of low frequency wavelet coefficients and the edge and texture details usually exist in high frequency sub bands, such as HH, HL, and LH.

2.7 Literature Review

Research in Steganography technique has been done back in the ancient Greek where during that time the ancient Greek practice of tattooing a secret message on the shaved head of the messenger, and letting his hair grow back before sending him through enemy territory where the latency of this communication system was measured in months [16]. The most famous method of traditional Steganography technique around 440 B.C. was marking the document with invisible secret ink, like the juice of a lemon to hide information. However, the majority of the

development and use of computerized steganography only occurred in year 2000. E. Cole[3] introduces different types of Steganography name as nut and bolts of Steganography: Original classification scheme and new classification scheme. Original classification scheme focus on how data is hiding whereas new classification scheme is based on both how and where the data is stored. According to classification scheme there are following three groups [3]:

- **Insertion-based:** Insertion-based steganography techniques work by inserting blocks of data into a host file. Using an insertion-based technique, data is inserted at the same point in every file. This type of technique works by finding places in a file that can be changed, without having any significant effect on the host file. Because data is always being inserted at the same point for each file, this can be categorized as an insertion steganography technique.
- **Algorithmic-based:** Algorithmic-based steganography techniques use some sort of computer algorithm to designate where in a file data should be hidden. Because this category of technique doesn't always insert data in the same spot in each file, it is possible that the process will degrade the quality of the file. If the original file has been compare to the one where data is hidden, that person might be able to see a change in the file.
- **Grammar-based:** Grammar-based steganography techniques require no host file in which to hide a message because it generates its own host file. This class of technique uses hidden data to generate an output file based on a predefined grammar. The output file produced looks just like the predefined grammar.

M.Ramaiya, N.Hemrajani and A.K. Saxena[13] proposed an AES based Steganography model to detect the security of the secret message in image. In this model they hide image inside an image. They use AES algorithm to encrypt the secret image then use LSB technique to hide it into cover image. The intensity value of each pixel of secret image was converted from decimal to binary. Then sixteen consecutive pixel values were taken from secret image one block of 128 bits and the block were input to AES encoding function. In their proposed model they concluded that the strength of s-box mapping and secret key for encryption secret image improves security and image quality.

S. Gupta, A.Goyal and B. Bhushan[26] proposed RSA and Diffie to encrypt the message before hiding in cover image. The impact of hiding single bit, two bit, three bit and four bit Steganography on image were tested. According to their result they concluded that during one LSB of image is replaced there is no visible change in the picture quality for pure as well as Diffie Hellman and RSA steganographic techniques. When two bit was replaced there is slight change in picture quality and replacing three bit and four bit the picture quality is distort more prominently.

E. Houssein, M. Ali and A. Hassanien[4] proposed An Image Steganography Algorithm using Haar Discrete Wavelet Transformation with Advanced Encryption System. In their paper an advance encryption data is proposed using AES and hiding the data using Haar DWT technique, carrying a less details of image in region and other three regions carrying a less details of the image then the cipher text is concealed at most two LSB positions.

M. Gunjal and J. Jha [9] suggested Image Steganography using Discrete Cosine Transformation and Blowfish Algorithm. They combine DCT and Blowfish algorithm to make the secret message more secure. The Blowfish algorithm first encrypts the message and then DCT steganography hides the message into image.

Image steganography using DWT and Blowfish algorithm was proposed by M. Vaidya et.al [14]. In this technique they use combination of steganography and cryptography. They used DWT to divide the image into low frequency and high frequency coefficient using Haar wavelet transformation and blowfish algorithm to encrypt the message before hiding.

K. Shah, S. Kaul and M. Dhande[8]proposed Image Steganography using DWT and Data Encryption Standard i.e. a system which use cryptography and steganography together. They use DES algorithm to encrypt the message so that concealing of message is hard. Before hiding the message the image is transformed from spatial domain to frequency domain using DWT.

Improved protection in video steganography using DCT and LSB was proposed by P. Bodhak and B. L. Gunjal [21]. They use DCT coefficient for JPEG compression which separates the image into parts of different importance and transforms a signal or image from the spatial domain to the frequency domain. They use AVI videos for analysis.

N.Saxena and G.Agrawal [18] suggested image steganography using DCT and DWT. In their research they had combined the two methods DCT and DWT. Then DCT is applied only into HH band. This method uses the method of hiding secret image in HH and HL band using DWT and makes a comparison on basis of PSNR. The method generally achieves the goal of hiding secret image and proves that HH band is good and gives better result than HL.

CHAPTER 3

METHODOLOGY

The research study includes the implementation and analysis of DCT, DWT and a combine method DCT with DWT. Each module is analyzed using primary and secondary image data. Primary data are the captured image from camera whereas secondary image data is of image data set and in the jpeg, bmp and gif format like sipi images dataset [29]. The analysis has been done to determine which technique is more secure by having high Peak Signal to Noise Ratio. As we know the goal of steganography is to secure communication from eaves- dropper, steganographic techniques strive to hide the very presence of the message itself from an observer. So in order to reach a high security and advance method DCT with DWT will be compared to the DCT and DWT algorithm and the performance of these techniques will be measured using PSNR (Peak Signal to Noise Ratio).

3.1 Framework

The data hiding using DCT with DWT will be compared to the DCT and DWT. The framework of the techniques is as show in figure 3.4.

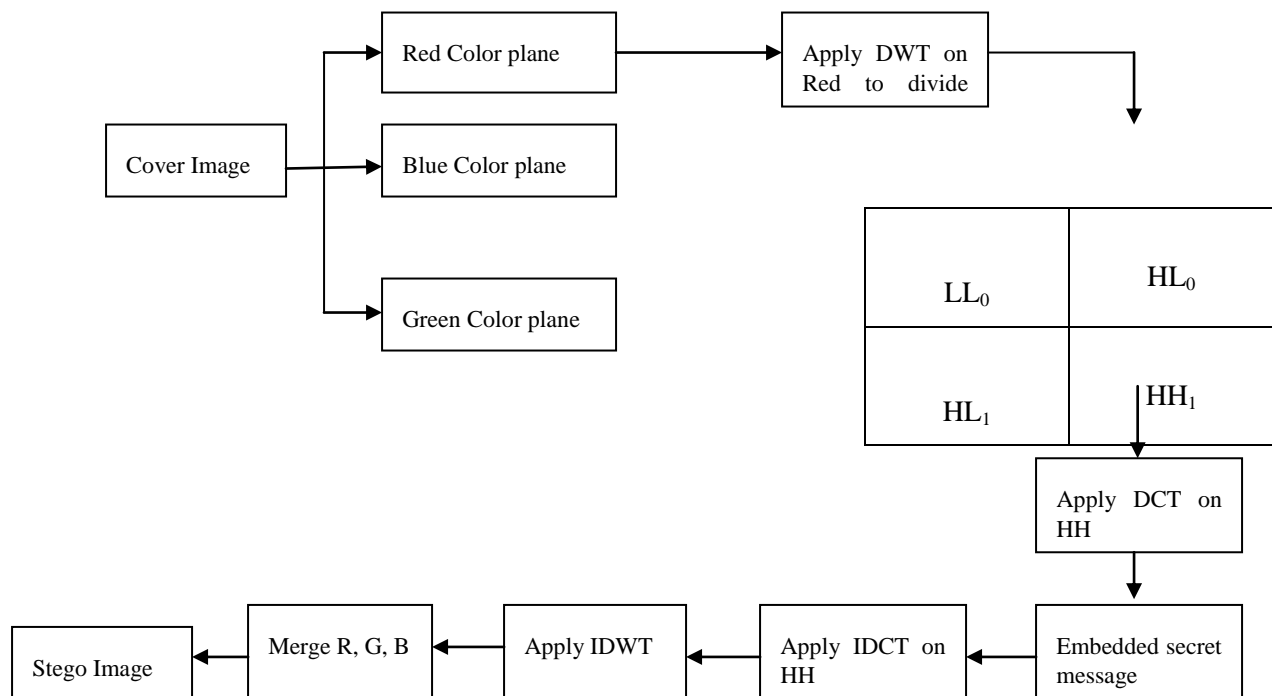


Figure 3.4: Message Embedding using DCT with DWT

As shown in Figure 3.4. In order to exchange the secret message in a secure way that prevent the eavesdropper from recognizing, hacking and/or altering the stego image and the secret message the sender and the Receiver will use DCT with DWT technique. The Sender wants to send a secret message to the Receiver where the Attacker is the third part or the eavesdropper who wants to attack the secret message in order to change according to his/her personal proposes. To prevent the Attacker from succeeding with his/her mission and even recognizing the stego image from the other images. First, the cover image is divided into four bands (LL₀, HL₀, HL₁, HH₁) by using DWT and DCT is applied to the HH band to embed the secret message. Then, the stego image is sent by the sender to the receiver where the receiver extracts the hiding data from the stego image by using DWT and DCT extracting algorithm. The stego images that produced from the two technique's embedding algorithms will be measured using Peak Signal to Noise Ratio (PSNR). Section 3.2 and section 3.3 will discuss the embedding and extracting algorithms in details.

3.2 Discrete Cosine Transformation (DCT)

In Discrete Cosine Transform, for each color component the JPEG image format uses a discrete cosine transform to transform successive 8 x 8 pixel blocks of the image into 64 DCT coefficients each. The DCT coefficients $F(u,v)$ of an 8 x 8 block of image pixels $f(x, y)$ are given by [2]

$$f(u, v) = \frac{1}{4} C(i) C(j) \sum_{x=0}^7 \sum_{y=0}^7 p(x, y) \cos\left[\frac{(2x+1)u\pi}{16}\right] \cos\left[\frac{(2y+1)v\pi}{16}\right] \dots \dots \text{Eq(3. 2)}$$

Where,

$P(x,y)$ is the x, y^{th} element of the image represented by the matrix p .

N is the size of the block that the DCT is done.

The equation calculates one entry (i, j^{th}) of the transformed image from the pixel values of the original image matrix. For standard 8*8 block, N equals 8 and x and y range from 0 to 7. Because the DCT uses cosine function, the resulting matrix depends on the horizontal, diagonal, and vertical frequencies.

The algorithm to embed the text message using DCT technique is as follows:

a. Breaking down image:

The cover image is read and the image is broken into 8 X 8 image block of pixels.

b. Apply DCT to each Block:

In this step, the image block is subtracted from 128 from each entry since DCT is designed to work on pixel values ranging from -128 to 127. Then on the resultant matrix the DCT is performed, which is accomplished by matrix multiplication.

$$D = TMT^T$$

Where, T is DCT matrix which is obtained from following equation

$$T_{i,j} = \begin{cases} 1/\sqrt{N} & \text{if } i=0 \\ \sqrt{\frac{1}{N}} \cos \left[\frac{(2j+1)i\pi}{2N} \right] & \text{if } i>0 \end{cases} \dots \dots \text{Eq(3.3)}$$

For an 8 X 8 block it result in this matrix: T=

$$\begin{pmatrix} .3536 & .3536 & .3536 & .3536 & .3536 & .3536 & .3536 & .3536 \\ .4904 & .4157 & .2778 & .0975 & -.0975 & -.2778 & -.4157 & -.4904 \\ .4619 & .1913 & -.1913 & -.4619 & -.4619 & -.1913 & -.1913 & .4619 \\ .4157 & -.0975 & -.4904 & -.2778 & -.2778 & .4904 & .0975 & -.4157 \\ .3536 & .3536 & .3536 & .3536 & .3536 & .3536 & .3536 & .3536 \\ .2778 & -.4904 & -.0975 & .4157 & -.4157 & -.0975 & .4904 & -.2778 \\ .1913 & -.4619 & .4619 & -.1913 & -.1913 & .4619 & -.4619 & .1913 \\ .0975 & -.2778 & .4157 & -.4904 & -.4904 & -.4157 & .2778 & -.0975 \end{pmatrix}$$

Suppose a block 8 X 8 of image pixel values is B=

$$\begin{pmatrix} 154 & 123 & 123 & 123 & 123 & 123 & 123 & 136 \\ 192 & 180 & 136 & 154 & 154 & 154 & 136 & 110 \\ 254 & 198 & 154 & 154 & 180 & 154 & 123 & 123 \\ 239 & 180 & 136 & 180 & 180 & 166 & 123 & 123 \\ 180 & 154 & 136 & 167 & 166 & 149 & 136 & 136 \\ 128 & 136 & 123 & 136 & 154 & 180 & 198 & 154 \\ 123 & 105 & 110 & 149 & 136 & 136 & 180 & 166 \\ 110 & 136 & 123 & 123 & 123 & 136 & 154 & 136 \end{pmatrix}$$

The resultant matrix after subtracting 128

M=

$$\begin{pmatrix} 26 & -5 & -5 & -5 & -5 & -5 & -5 & 8 \\ 64 & 52 & 8 & 26 & 26 & 26 & 8 & -18 \\ 126 & 70 & 26 & 26 & 52 & 26 & -5 & -5 \\ 111 & 52 & 8 & 52 & 52 & 38 & -5 & -5 \\ 52 & 26 & 8 & 39 & 38 & 21 & 8 & 8 \\ 0 & 8 & -5 & 8 & 26 & 52 & 70 & 26 \\ -5 & -23 & -18 & 21 & 8 & 8 & 52 & 38 \\ -18 & 8 & -5 & -5 & -5 & 8 & 26 & 8 \end{pmatrix}$$

The resultant D matrix is

$$\begin{pmatrix} 162.3 & 40.2 & 20.0 & 72.3 & 30.3 & 12.5 & -19.7 & -11.5 \\ 30.5 & 108.4 & 10.5 & 32.3 & 27.7 & -15.5 & 18.4 & -2.0 \\ -94.1 & -60.1 & 12.3 & -43.4 & -31.3 & 6.1 & -3.3 & 7.1 \\ -38.6 & -83.4 & -5.4 & -22.2 & -13.5 & 15.5 & -1.3 & 3.5 \\ -31.3 & 17.9 & -5.5 & -12.4 & 14.3 & -6.0 & 11.5 & -6.0 \\ -0.9 & -11.8 & 12.8 & 0.2 & 28.1 & 12.6 & 8.4 & 2.9 \\ 4.6 & -2.4 & 12.2 & 6.6 & -18.7 & -12.8 & 7.7 & 12.0 \\ -10.0 & 11.2 & 7.8 & -16.3 & 21.5 & 0.0 & 5.9 & 10.7 \end{pmatrix}$$

c. Quantization:

The 8 X 8 block of DCT coefficient is compressed by quantization. During quantization the less important frequencies are discarded. To obtain quantized DCT blocks by dividing each element in the transformed image matrix by corresponding element in the quantization matrix, then rounding to the nearest integer value. For this, standard quantization matrix Q is used.

$$Q = \begin{pmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{pmatrix}$$

The resultant matrix after quantization is

$$\begin{pmatrix} 10 & 4 & 2 & 5 & 1 & 0 & 0 & 0 \\ 3 & 9 & 1 & 2 & 1 & 0 & 0 & 0 \\ -7 & -5 & 1 & -2 & -1 & 0 & 0 & 0 \\ -3 & -5 & 0 & -1 & 0 & 0 & 0 & 0 \\ -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

d. LSB and Message Hiding

After obtaining quantized DCT blocks, the LSB of each DC coefficient is calculated and replace with each bit of the secret message. The zero element are discarded and only the non-zero element are taken to embed the message using LSB. Suppose if the secret message to hide is 'a', then first it converted to the binary value. The binary value of character 'a' is 01000001. The message hiding in DC coefficient is process as follows:

The binary value of DC coefficient of respective value

10 = 00001010, 4=00000100, 2=00000010, 5=00000101, 1=00000001, 3=00000011, 9=00001001, 1=00000001, 2=00000010

After hiding the message the binary value change as follows:

00001010=10, 00000101=5, 00000010=2, 00000100=4, 00000000=0, 00000010=2,
00001000=8, 00000000=0, 00000011=3

The resultant matrix after hiding message is as follows

$$\begin{pmatrix} 10 & 5 & 2 & 4 & 0 & 0 & 0 & 0 \\ 2 & 8 & 0 & 3 & 1 & 0 & 0 & 0 \\ -7 & -5 & 1 & -2 & -1 & 0 & 0 & 0 \\ -3 & -5 & 0 & -1 & 0 & 0 & 0 & 0 \\ -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

e. Dequantization

Dequantization is achieved by multiplying each element of the transformed matrix after secret message hiding by corresponding element in the quantization matrix. For this the same quantization matrix Q is used. The resultant matrix after Dequantization is

$$\begin{pmatrix} 160 & 55 & 20 & 64 & 0 & 0 & 0 & 0 \\ 24 & 192 & 0 & 57 & 26 & 0 & 0 & 0 \\ -98 & -65 & 16 & -48 & -40 & 0 & 0 & 0 \\ -42 & -85 & 0 & -29 & 0 & 0 & 0 & 0 \\ -36 & 22 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

f. Inverse DCT

The inverse DCT is next to applied to the matrix, which is rounded to the nearest integer. Finally 128 is added to each element of that result, giving us the JPEG version N of original 8 X 8 image block. The matrix after IDCT is

$$\begin{pmatrix} 164.42 & 147.92 & 128.24 & 117.70 & 106.77 & 113.15 & 99.00 & 95.87 \\ 214.72 & 183.78 & 150.01 & 137.21 & 117.15 & 132.05 & 120.15 & 80.57 \\ 258.65 & 215.76 & 171.34 & 159.13 & 132.86 & 157.19 & 114.31 & 75.12 \\ 224.86 & 207.53 & 170.97 & 165.52 & 146.10 & 172.94 & 136.25 & 98.63 \\ 218.44 & 189.61 & 162.57 & 161.51 & 149.39 & 174.44 & 147.28 & 118.16 \\ 116.08 & 118.23 & 123.64 & 132.91 & 143.70 & 156.12 & 163.06 & 168.92 \\ 124.34 & 124.16 & 127.22 & 136.00 & 145.44 & 159.33 & 163.93 & 167.45 \\ 88.51 & 94.13 & 106.15 & 110.07 & 122.08 & 125.25 & 139.81 & 161.78 \end{pmatrix}$$

g. Reconstruction of Image:

The 8 X 8 image blocks are merged to reconstruct the stego image.

3.3 Discrete Wavelet Transformation (DWT)

Wavelets are special functions which (in a form analogous to sins and cosines in Fourier analysis) are used as basal functions for representing signals. The discrete wavelet transform (DWT) we applied here is Haar-DWT, the simplest DWT. In Haar-DWT the low frequency wavelet coefficient are generated by averaging the two pixel values and high frequency coefficients are generated by taking half of the difference of the same two pixels.

For 2-D images, applying DWT (Discrete Wavelet Transform) separates the image into a lower resolution approximation image or band (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components.

LL ₀	HL ₀
HL ₁	HH ₁

Figure 3.5: Components of 1-level 2-Dimensional Discrete Wavelet Transform

With the DWT, the significant part(smooth parts) of the spatial domain image exist in the approximation band that consists of low frequency wavelet coefficients and the edge and texture details usually exist in high frequency sub bands, such as HH, HL, and LH.

The procedure to embed the secrete message using DWT is as follows:

1. The cover image is taking and decomposed into three color planes i.e. Red, Green, and Blue if the image is color image.
2. Then we take red plane and apply Haar DWT and divide them into four sub band.
 - a. To apply Haar DWT first we scan pixel from left to right in horizontal direction.
 - b. Perform the addition and subtraction operation on neighboring pixels.
 - c. Store the sum on the left and difference on the right as below

A	B	C	D



A+B	C+D	A-B	C-D
L		H	

Figure 3.6: Horizontal Operations

This step is repeated until all rows are processed. The pixel sum represent the low frequency part here it is denoted L while the pixel difference represent the high frequency part of the original image here denote as H.

- d. Again, scan the pixel from top to bottom in vertical direction. Perform the addition and subtraction operations on neighboring pixels and then store the sum on top and the difference on the bottom as below.

M		O	
N		P	
L		H	

M + N		O + P	
LL		HL	
M - N		O - P	
LH		HH	

Figure 3.7: Vertical Operations

This step is repeated until all the columns processed. At end, this mechanism gives four sub bands denoted as LL, HL, LH, and HH.

- 3. Then calculate LSB of the HH sub band.

4. After that the secret message is converted into binary format and bits of LSB of above selected sub band are modified with bits of secret message.
5. Apply IDWT after embedding bits of secret message and concatenate the plane to get stego image.

3.3 DCT with DWT

This is the combined method of the DCT and DWT. In this method the cover image is divided into three color planes and divides the red plane into four sub band using DWT. DWT splits the signal in low and high frequency parts. The high frequency part contains the information about the edge component so DCT is applied in HH band only. The High frequency components are usually used since the human eye is less sensitive to change in edges [28]. The algorithm is summarized as follows:

1. Cover image is taken and divided into three color planes.
2. Apply DWT in Red plane and divide them into four sub band.
3. Then apply DCT on HH band of Red pane.
4. Embedding secret message is converted into binary format and bits of DCT coefficients of above selected sub band are modified with bits of secret message using LSB.
6. Apply inverse Discrete Cosine Transform on HH sub band.
7. After embedding bits of secret message in red plane inverse wavelet transformation is applied to get back the plane.
8. Finally each plane is concatenated to get color stego image.

In N.Saxena and G.Agrawal's [18] paper they had used session based pseudo random 2D sequence to dispersed separately in to selected high frequency component but in this research LSB is used to embedded the secret message bit in DC coefficient of HH sub band.

3.4 Performance Evaluation Parameters

For performance evaluation of the above mentioned algorithms different images are considered. The steganographic techniques are evaluated on basis of payload and imperceptibility. The former describes the capacity of secret data embedded in the carrier media and the later gives the

measure of embedded data imperceptible to the observer (perceptual invisibility) and computer analysis (statistical invisibility).

There are two types of perceptibility measure: Fidelity and Quality. Fidelity means the perceptual similarity between signals before and after processing. Quality is an absolute measure of the goodness of a signal to avoid any suspension and therefore detection. The performance of the image steganography algorithms are evaluate in term of Peak Signal to Noise Ratio(PSNR) Mean Square Error (MSE), Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI) that are described in R.Vijayrajeswari et al [25].

3.4.1 PSNR (Peak Signal to Noise Ratio)

Peak Signal to Noise Ratio is used to measure the quality. Peak Signal to Noise Ratio is the standard measurement to measure the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation [5]. In Steganography technique, the signal is maximum possible pixel value and noise is the error or change in image pixel value after embedding secret message in it. It measure the quality of image between the cover image f and stego image g of size $M*N$. It is defined as follows [5]:

$$PSNR = 10 * \log_{10} \frac{MAX^2}{MSE} \dots\dots\dots \text{Eq(3. 4)}$$

Where MAX is the maximum possible pixel value of the image, when the pixels are represented using 8 bits per sample, it is 255.

3.4.2 MSE (Mean Square Error)

MSE measures the average of the square of “errors”, that is, the difference between the estimator and what is estimated. In Steganography MSE measure the average of square of error (i.e. noise or change in image introduce after embedding secret message in it) between cover image and stego image.

$$MSE = \frac{1}{MN} \sum_{X=0}^{M-1} \sum_{Y=0}^{N-1} ((F(X, Y) - G(X, Y))^2) \dots\dots\dots \text{Eq(3. 5)}$$

Where, $F(X,Y)$ represent cover image and $G(X,Y)$ represents the stego image. The height and width of the cover image is dented by X and Y respectively.

The PSNR and MSE are inversely proportional to each other. When there are low errors or changes between cover image and stego image, the PSNR value is higher and when there are high changes or errors between cover image and stego image, the PSNR value is lower. So higher the PSNR, lower is the difference between cover image and stego image and vice versa.

3.4.3 NPCR (Number of Pixel Change Rate)

NPCR measures the percentage of different pixel numbers between the two images such as cover image and stego image.

$$NPCR = \frac{1}{XY} \sum K(X, Y) \dots \dots \dots \text{Eq(3. 6)}$$

Let K1(i,j) be cover image and K2(i,j) be stego image.

$$K(i,j) = \begin{cases} 1, & \text{if } K1(i,j) \neq K2(i,j) \\ 0, & \text{else} \end{cases}$$

3.4.4 UACI (Unified Average Change Intensity)

It determines the average intensity of differences between the two images such as cover image and stego image. It is expressed as,

$$UACI = \frac{1}{XY} \sum |K1(X, Y) - K2(X, Y)| \dots \dots \dots \text{Eq(3.7)}$$

For a better system, the value of UACI should be low, and NPCR should be high

CHAPTER 4

IMPLEMENTATION AND ANALYSIS

4.1 Implementation

4.1.1. Programming Language and Framework

The entire algorithm has been implemented using MATLAB R2016a. The study is carried out in DELL Inspiron n4110 with 2.5 GHz Intel core i5 processor and 4GB (DDR3) RAM.

4.1.2. MATLAB R2016a overview

MATLAB (matrix laboratory) is a multi-paradigm numerical computing environment and proprietary programming language developed by MathWorks. MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages, including C, C++, C#, Java, Fortran and Python.

Although MATLAB is intended primarily for numerical computing, an optional toolbox uses the MuPAD symbolic engine, allowing access to symbolic computing abilities. An additional package, Simulink, adds graphical multi-domain simulation and model-based design for dynamic and embedded systems. MATLAB R 2016b is 9.2 versions which was release in September 2016 and has some extra features like define local functions in scripts; automatic expansion of dimensions.

4.1.3. Image separation in RGB Plane

The image separation in RGB plane in this section is intended to separate the image if the cover image is color image. So that the secret message for encoding (section 4.3) can be hide in any one of the plane. The image is separated into RGB using following function:

```
if strcmp(current_colourspace, 'Greyscale')
    use_greyscale = true;
else
    use_greyscale = false;

switch current_colourspace
case 'RGB [R]'
    channel = 1;
```

```

    case 'RGB [G]'
        channel = 2;
    case 'RGB [B]'
        channel = 3;
    otherwise
        error('Invalid colourspace: %s', current_colourspace);
    end
end
end

```

here current_colourspace is user define value.

4.3 Encoding the secret message

The encoding implemented in this section is intended to embed the secret message in the cover image. To encode the message in cover image, the DCT or DWT or DCT with DWT algorithm are used. Using DCT, first the image is quantized using quantization matrix. During quantization the less important frequencies are discarded. To obtained quantized DCT blocks by dividing each element in the transformed image matrix by corresponding element in the quantization matrix, then rounding to the nearest integer value. The function to encode the message is given below:

```

function [im, im_wavelet] = steg_wdct_encode(im, secret_msg_bin, mode,
frequency_coefficients, persistence)

```

```

[ll lh hl hh] = dwt2(im, mode);
hh = steg_dct_encode(secret_msg_bin, hh, frequency_coefficients, persistence);
im_wavelet = [ll, lh; hl, hh];
im = idwt2(ll, lh, hl, hh, mode);

```

```

end

```

```

function [imc_stego]=steg_dwt_encode(imc,msg_desired)
    wname='haar';
    data=[];
    for(i=1:length(msg_desired))
        d=msg_desired(i)+0;
        data=[data d];
    end
    imshow(imc);
    [cA1,cH1,cV1,cD1] = dwt2(imc,wname);
    dec1 = [cA1 cH1; cV1 cD1 ];
    figure;imshow(uint8(dec1));
    M=max(data);

```



```

data_norm=data/M;
n=length(data);
[x y]=size(cH1);
cH1(1,1)=-1*n/10;
cH1(1,2)=-1*M/10;
for(i=1:1:ceil(n/2))
cV1(i,y)=data_norm(i);
end
set(0,'userdata',y);
for(i=ceil(n/2)+1:1:n)
cD1(i,y)=data_norm(i);
end
imc_stego=idwt2(cA1,cH1,cV1,cD1,wname);
figure;imshow(uint8(imc_stego))
[x y]=size(cA1);
imshow(uint8(imc_stego))
ms=abs(imc_stego-double(imc));
ms=ms.*ms;
ms=mean(mean(ms))
ps= (255*255)/ms;
ps=10*log10(ps)
imwrite(uint8(imc_stego),'Stego.bmp','bmp');

return

```

4.4 Decoding the secret message

In this section, decoding is carried out to decode the secret message that is hidden inside the carrier image. The function to decode the message is as follows:

```

function [extracted_msg_bin]=stego_dwt_decode(imc_stego)
wname='haar';
[cA11,cH11,cV11,cD11] = dwt2(imc_stego,wname);
data=[]
data_norm=[];
n=ceil(abs(cH11(1,1)*10));
M=ceil(abs(cH11(1,2)*10));
y = get(0,'userdata');
for(i=1:1:ceil(n/2))
data_norm(i)=cV11(i,y);
end
for(i=ceil(n/2)+1:1:n)
data_norm(i)=cD11(i,y);
end

```

```
data=ceil(data_norm*M)-1;
extracted_msg_bin="";
for(i=1:length(data))
extracted_msg_bin=strcat(extracted_msg_bin,data(i));
end
extracted_msg_bin;
end
```

4.2. Data Set Description

The input data for the experiment are the different image formats. The input images types are of .bmp, .jpeg, jpg types. The image data are both primary and secondary. The secondary type are the standard images like Lena, Peppers, Baboon, Cameraman etc. of different dimension as 256×256 , 512×512 collected from sipi images dataset [29]. The primary image data are captured images from camera. The primary image are taken as the distribution in histogram is not evenly while in secondary the histogram distribution is evenly. So the primary images are also taken in this research.

4.3. Result Analysis

The algorithms implemented during this research are analyzed from various dimensions.

Computational analysis based on encryption and decryption time, visual assessment analysis based on Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) of input images and Stego images, differential analysis based on NPCR and UACI and statistical analysis based on histogram has been done.

4.3.1. Visual assessment analysis

Visual assessment analysis is done to measure the performance of the decoding procedure. For that the PSNR value and MSE of cover image and stego image will be calculated. It is the ratio of mean square difference of the component for the two images to the maximum mean square difference that can exist between any two images. The higher value of PSNR indicates higher image quality. The PSNR and MSE values for different set of images are measured and compared for visual assessment analysis.

PSNR and MSE for the sample test data image are as show in the table below:

Table 5.1: PSNR in secondary data

S.N	Image	Dimension	Method	MSE (dB)	PSNR (dB)
1	Baboon.jpg	256*256	DCT	14.749344	72.886153
			DCT with DWT	6.369904	80.178950
			DWT	0.023007	64.512242
2	Lena.jpg	512*512	DCT	16.182571	72.080657
			DCT with DWT	7.926361	78.280130
			DWT	0.002331	74.455644
3	Pepper.jpg	512*512	DCT	12.567455	74.276660
			DCT with DWT	12.516895	74.311675
			DWT	0.002442	74.253509
4	Cameraman.bmp	512*512	DCT	9.640030	76.580040
			DCT with DWT	11.109436	75.347767
			DWT	0.001167	77.458288

Table 5.2: PSNR in secondary data (cont.)

S.N	Image	Dimension	Method	MSE(dB)	PSNR(dB)
5.	man.bmp	256*256	DCT	6.530833	79.962235
			DCT with DWT	11.709124	74.891119
			DWT	0.002908	73.494962
6.	house.bmp	512*512	DCT	42.144482	63.766793
			DCT with DWT	33.723114	65.703054
			DWT	0.022897	64.533103
7.	Gems.bmp	512*512	DCT	15.098495	72.682934
			DCT with DWT	6.822784	79.582374
			DWT	0.000861	78.781007

The average value of MSE for secondary image using DCT is 16.70189, DCT with DWT is 12.88252 and DWT is 0.007945 and PSNR values are 73.1765, 75.47072 and 72.49839 respectively.

Table 5.3: PSNR in Primary Data

S.N	Image	Dimension	Method	MSE(dB)	PSNR(dB)
1.	Scene.jpg	1024*1024	DCT	11.383857	75.135819
			DCT with DWT	1.579077	92.293542
			DWT	0.000060	90.351171
2.	Flower.jpg	512*512	DCT	12.082359	74.618572
			DCT with DWT	3.863831	84.521246
			DWT	0.000231	84.485620
3.	Juice.jpg	512* 512	DCT	13.153252	73.880945
			DCT with DWT	5.047874	82.199436
			DWT	0.000263	83.926411

The average value of MSE for primary image using DCT is 12.20649, DCT with DWT is 3.496927 and DWT is 0.000185 and PSNR values are 74.54511, 86.33807 and 86.2544 respectively.

The PSNR value of the cover image with stego image is calculated and it is observed that the PSNR of DCT with DWT (combined technique) has high PSNR value compared to other two techniques which ensures that the algorithm has good visual assessment. The lesser the PSNR value, higher the degradation of image quality. The above result shows that the DCT and DWT has lesser PSNR and higher MSE value and the combined method has higher PSNR and lesser MSE, Thus Combined method is better than other two methods.

5.2.2 Computational Speed Analysis

Computation analysis is the measures of time consumed by the algorithms. We measure the value of encoding and decoding time for computational performance for different set of images in seconds to find which techniques has good results and it is observed from the given result analysis below that the DCT and DWT has relatively high encoding/decoding time. As the image sizes increases the time consumed by the algorithm to encode and decode get increased compare to other two techniques. Thus, from this analysis it can be conform that DCT with DWT is computationally efficient than that of other two techniques.

The Encryption and Decryption time of different methods are shown below:

Table 5.4: Encoding and Decoding Time of Secondary Images

S.N	Image	Dimension	Method	Encoding time (s)	Decoding time (s)
1.	baboon.jpg	256*256	DCT	0.202815	0.094626
			DCT with DWT	0.069036	0.031078
			DWT	1.478932	0.038033
2.	lena.jpg	512*512	DCT	0.874043	0.374802
			DCT with DWT	0.269972	0.120445
			DWT	0.889540	0.075235
3.	pepper.jpg	512* 512	DCT	0.789885	0.376081
			DCT with DWT	0.299634	0.143299

S.N	Image	Dimension	Method	Encoding Time (s)	Decoding Time (s)
4.	cameraman.tiff	256*256	DCT	0.198017	0.094247
			DCT with DWT	0.065465	0.028323
			DWT	1.344670	0.037176
5.	Man.bmp	512*512	DCT	3.159393	1.500172
			DCT with DWT	1.089029	0.501914
			DWT	1.844928	0.140491
6.	Gems.bmp	512* 512	DCT	0.202164	0.094198
			DCT with DWT	0.062825	0.028527
			DWT	1.346081	0.038597
7.	House.bmp	256*256	DCT	0.812129	0.384460
			DCT with DWT	0.289008	0.123216
			DWT	1.582466	0.111283

The average encoding time of secondary image using DCT is 0.891207, DCT with DWT is 0.306424 and DWT is 1.414436 and decoding time of DCT is 0.416941, DCT with DWT is 0.139543 and DWT is 0.073469 second.

Table 5.5: Encoding and Decoding time of Primary Images

S.N	Image	Dimension	Method	Encoding time (s)	Decoding time (s)
1	Scene.jpg	1024*1024	DCT	3.180095	1.543535
			DCT with DWT	1.111452s	0.492587
			DWT	2.581800	0.406389
2	Flower.jpg	512*512	DCT	0.784223	0.411227
			DCT with DWT	0.280570	0.126865
			DWT	1.612322	0.114015
3	Juice.jpg	512*512	DCT	0.787633	0.369014
			DCT with DWT	0.313461	0.138311
			DWT	1.006188	0.095597

The average encoding time of primary image using DCT is 1.583984, DCT with DWT is 0.297016 and DWT is 1.733437 and decoding time of DCT is 0.774592, DCT with DWT is 0.252588 and DWT is 0.205334 second.

5.2.3 Differential Analysis

Differential analysis is done for security measures. It is a technique which observes how difference in input affects differences on the output. NPCR (Number of pixel change) and UACI (Unified Average Change Intensity) are the two widely used security analyses in image steganography community for differential analysis. NPCR concentrates on the absolute number of pixels which changes value in differential attacks while the UACI focuses on the averaged difference between two paired images (original image and stego image). The different types of images are taken for experiments to predict which methods results the best results. The difference in NPCR and UACI of different algorithm is as follows:

Table 5.6: NPCR and UACI of Secondary Images

S.N	Image	Dimension	Method	NPCR (%)	UACI (%)
1.	baboon.jpg	256*256	DCT	90.895081	1.180091
			DCT with DWT	75.515747	0.645955
			DWT	90.237427	0.000160
2.	lena.jpg	512*512	DCT	92.101669	1.240979
			DCT with DWT	71.108627	0.681805
			DWT	92.863846	0.000050
3.	pepper.jpg	512* 512	DCT	91.300964	1.336271
			DCT with DWT	74.186325	0.825532
			DWT	91.600418	0.000069
4.	cameraman.tiff	256*256	DCT	91.621399	0.869338
			DCT with		

			DWT	56.866455	0.565604
			DWT	90.933228	0.000193
5.	Man.bmp	512*512	DCT	89.068317	0.763069
			DCT with DWT	77.169704	0.914090
			DWT	88.874245	0.000200
6.	Gems.bmp	512* 512	DCT	91.157532	1.182496
			DCT with DWT	56.002808	0.529426
			DWT	85.552979	0.000181
7.	House.bmp	256*256	DCT	92.039108	1.528516
			DCT with DWT	72.978210	1.024670
			DWT	90.598297	0.000484

The average NPCR of secondary image using DCT is 91.16915, DCT with DWT is 60.47848 and DWT is 78.83256 and UACI of DCT is 1.157251, DCT with DWT is 0.648385 and DWT is 0.000191.

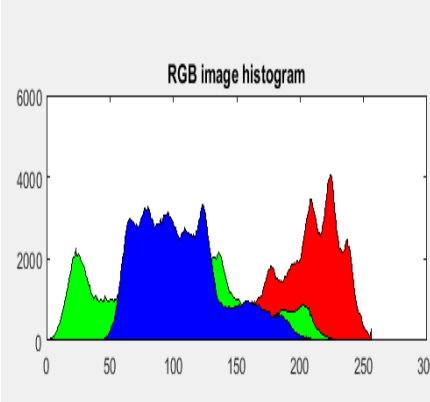
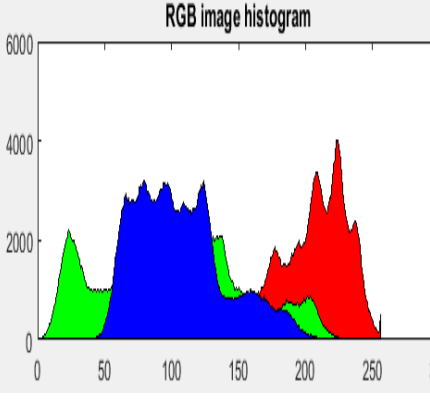
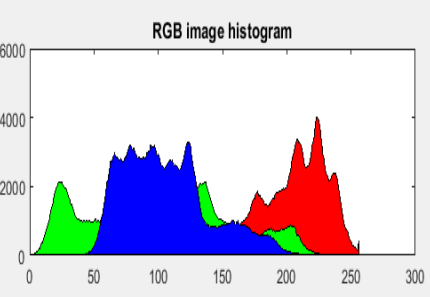
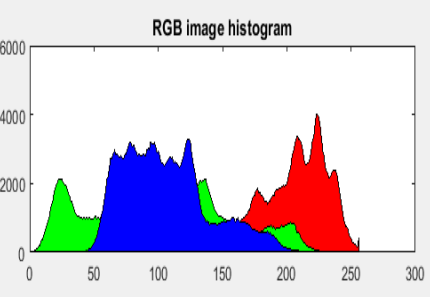
Table 5.7: NPCR and UACI of Primary Image

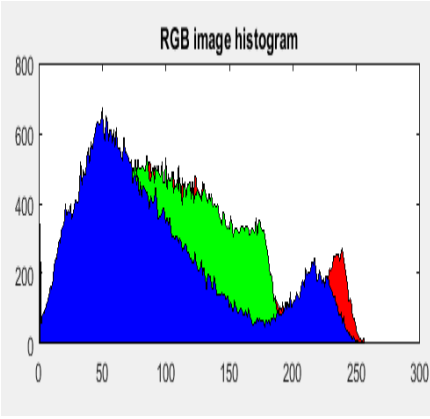
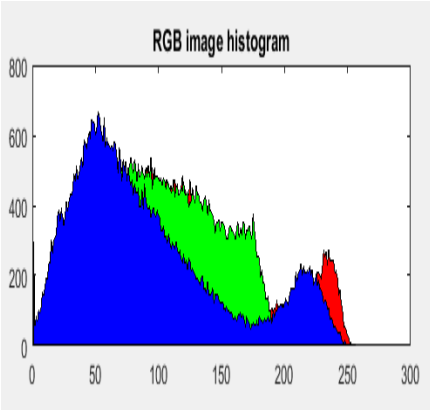
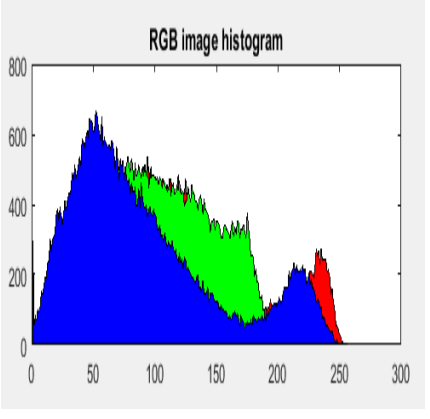
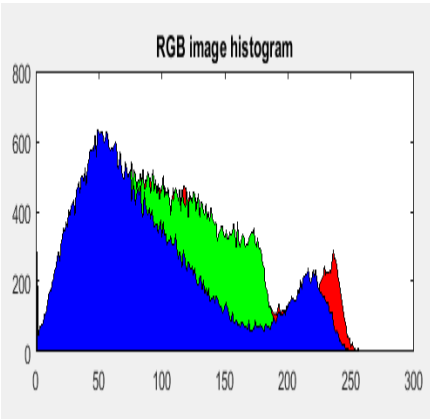
S.N	Image	Dimension	Method	NPCR (%)	UACI (%)
1	Scene.jpg	1024*1024	DCT	93.486977	1.124062
			DCT with DWT	47.319126	0.297875
			DWT	92.674065	0.000012
2	Flower.jpg	512*512	DCT	91.004181	1.109505
			DCT with DWT	56.517029	0.451570
			DWT	90.721512	0.000044
3	Juice.jpg	512*512	DCT	91.247177	1.133746
			DCT with DWT	65.110016	0.535760
			DWT	92.475510	0.000048

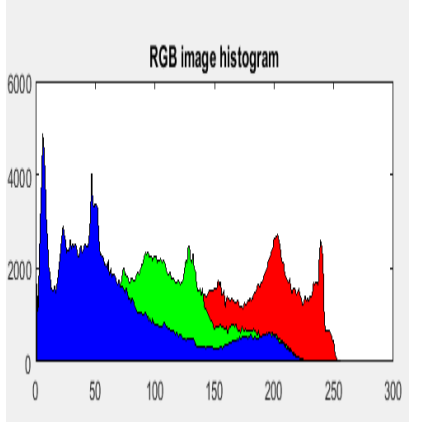
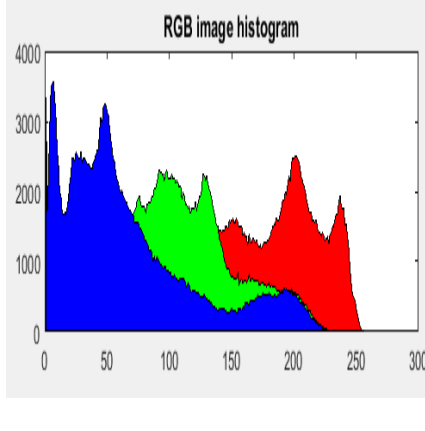
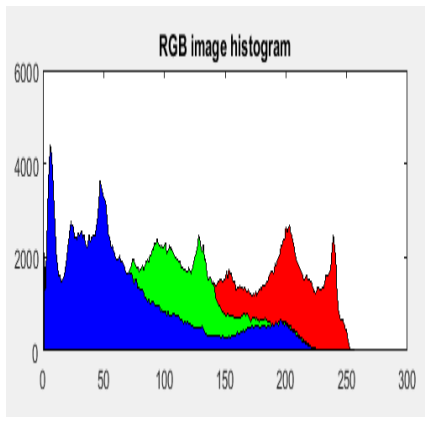
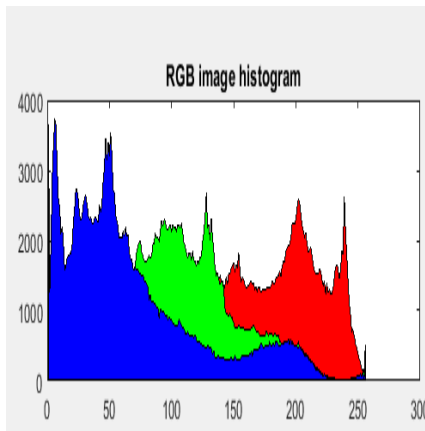
5.2.4 Statistical Analysis

Statistical analysis is has been carried out using histogram analysis. In an image processing context, histogram of an image normally refers to a histogram of the pixel intensity values. This histogram is a graph showing the number of pixels in an image at each different intensity value found in that image. For an 8-bit grayscale image there are 256 different possible intensities, and so the histogram will graphically display 256 numbers showing the distribution of pixels amongst those grayscale values. Histograms can also be taken of color images either individual histogram of red, green and blue channels can be taken, or a 3-D histogram can be produced, with the three axes representing the red, blue and green channels, and brightness at each point representing the pixel count. The histogram of different images is as follows:

Table 5.8 Histogram of Images

S. N	Image	Original Image histogram	Method	Stego Image Histogram
1	Lena. Jpg	 <p>RGB image histogram</p>	DCT	 <p>RGB image histogram</p>
			DCT With DWT	 <p>RGB image histogram</p>
			DWT	 <p>RGB image histogram</p>

2	Baboon.jpg	 <p>RGB image histogram</p> <p>This histogram shows the distribution of pixel intensities for the red, green, and blue channels of the Baboon.jpg image. The x-axis represents intensity from 0 to 300, and the y-axis represents frequency from 0 to 800. The red channel (leftmost area) has a peak around 240. The green channel (middle area) has a peak around 100. The blue channel (rightmost area) has a peak around 50.</p>	DCT	 <p>RGB image histogram</p> <p>This histogram is identical to the original image histogram, showing the distribution of pixel intensities for the red, green, and blue channels of the Baboon.jpg image after DCT transformation.</p>
			DCT With DWT	 <p>RGB image histogram</p> <p>This histogram is identical to the original image histogram, showing the distribution of pixel intensities for the red, green, and blue channels of the Baboon.jpg image after DCT and DWT transformation.</p>
			DWT	 <p>RGB image histogram</p> <p>This histogram is identical to the original image histogram, showing the distribution of pixel intensities for the red, green, and blue channels of the Baboon.jpg image after DWT transformation.</p>

3	Juice.jpg	 <p>RGB image histogram</p>	DCT	 <p>RGB image histogram</p>
			DCT With DWT	 <p>RGB image histogram</p>
			DWT	 <p>RGB image histogram</p>

From the above resultant histogram of cover image and stego image using all three techniques, it is observed that histograms are hardly distinguishable. The curves that are obtained from DCT, DWT and combine method are almost identical as the difference due to steganographic embedding is extremely small.

5.3 Result

The overall analysis shows that DCT with DWT method is computationally efficient method with other two approaches. With the increase in the image size DCT performance get degraded than that of DCT with DWT and DWT algorithm.

The analysis results also shows that DCT with DWT has maintain the image quality after encoding the secret message into cover image than other two approaches. This can be illustrated by the above results of PSNR value. The average PSNR value for DCT with DWT is 78.73, DWT is 76.62 and DCT is 73.56. The PSNR value of DCT with DWT method has higher value than other two techniques which verifies that the original image and stego image is similar without losing much of its image properties. But DCT and DWT has significantly has lower PSNR value, this value of PSNR results in a change of visual properties of the image. The average encoding value for DCT with DWT is 0.385045, DWT is 1.524587 and DCT is 1.09904 and decoding value for DCT with DWT is 0.173457, DWT is 0.117165 and DCT is 0.524236.

The DCT with DWT has good differential analysis value which has average value 65.27% and 0.65 % for the NPCR and UACI respectively for different set of images used during analysis. This value is able to protect the image from attackers as it hides the significant information of image data. DWT has significantly less impact on this categories but it is comparatively good than that of DCT as it can be shown in the above mentioned figures. Thus based on the above observation and result analysis DCT with DWT is better in resisting differential attack and computationally efficient. The overall analysis result show that DCT with DWT preserve the imperceptibility and maintaining quality of image; the property of image steganography as there is no significant difference in original (cover image) and stego image when we check the histogram of both cover image and stego image.

CHAPTER 6

CONCLUSION AND FUTURE RECOMMENDATION

6.1 Conclusion

Steganography is the need of today's digital world since there is no reliability over the medium through which the information is sent, in other words the medium is not secured. So, some methods are needed so that it becomes difficult for unintended user to extract the information from the message. Although a number of steganographic algorithm has been invented for secure secret message hiding. In this study, DCT with DWT algorithm has been implemented. The images of different types were used for testing the strength of the algorithms.

From overall analysis and result from above discussion concluded that DCT with DWT technique is more secure and powerful than other two approaches to hide the secret message before transferring to the communication channel. The algorithms are implemented and analyzed with different parameters to test the strength of algorithm and found that DCT with DWT is better than other two algorithms as it has higher PSNR value which also shows that it preserve the image quality after hiding secret message. DCT with DWT is found to be computationally efficient as it takes less encoding and decoding time than other two methods. DCT with DWT has high NPCR and UACI values which verifies that the strength of algorithm in the resisting differential attack and preserve the image steganography property of impeccability and security although DCT and DWT both method seem to preserve the less image properties than DCT with DWT.

6.2 Future Recommendation

Instead of using text as secret message image or audio or video can be carried out in near future. Digital watermarking can also be done using image as secret message. The steganalysis can also be performed in future to determine security threats and attacks threats. Instead of using Red plane, DWT can be applied to other two color channel i.e. Green and Blue also. While applying DCT in this research only HH band is used but other sub band like LL, HL and LH can also be used.

References

- [1] B. Grantham, "Bitmap Steganography: An Introduction", 2007.
- [2] D.Bansal and R.Chhikara, "An Improved DCT based Steganography Technique", *International Journal of Computer Application*, vol. 102, no. 14, 2014.
- [3] E. Cole, *Hiding in plain sight*. New York: Wiley, 2003.
- [4] E. Houssein, M. Ali and A. Hassanien, "An Image Steganography Algorithm using Haar Discreet Wavelet Transform with Advanced Encryption System", *Proceedings of the 2016 Federated Conference on Computer Science and Information Systems*, vol. 8, no. 2300-5963, pp. 641-644, 2016.
- [5] G.Chakrapani and V.L. Reddy, "Optimized Videotape Steganography using Genetic Algorithm", *Department of CSE, K.S.R.M. College of Engineering*, pp. 01-07, 2014
- [6] H. S, D. U, R. A and P. Kamath, "A Secure and High Capacity Image Steganography Technique", *Signal & Image Processing: An International Journal*, vol. 4, no. 1, pp. 83-89, 2013. Available: 10.5121/sipij.2013.4108.
- [7] H. Kaur and H. Aggarwal, "Review of Increasing Image Compression Rate Using (DWT+DCT) and Steganography", *International Journal of Recent Trends in Engineering and Research*, vol. 3, no. 6, pp. 67-72, 2017
- [8] K. Shah, S. Kaul and M. Dhande, "Image Steganography using DWT and Data Encryption Standerds", *International Journal of Science and Research(IJSR)*, vol. 3, no. 5, pp. 372-376, 2014.
- [9] M. Gunjal and J. Jha, "Image Steganography Using Discrete Cosine Transform (DCT) and Blowfish Algorithm", *International Journal of Computer Trends and Technology*, vol. 11, no. 4, pp. 144-150, 2014.
- [10] M. Jókay and T. Moravčík, "Image-based jpeg steganography", *Tatra Mountains Mathematical Publications*, vol. 45, no. 1, pp. 65-74, 2010. Available: 10.2478/v10127-010-0006-9.
- [11] M. M. Amin, M. Salleh, S. Ibrahim and M. R. Katmin, "Information hiding using steganography", *NCTT 2003 Proceedings. 4th National Conference*, vol. 71847, 2003.
- [12] M. Nosrati, R. Karimi and M. Hariri, "An introduction to steganography methods", *World Applied Programming*, vol. 1, no. 3, pp. 191-195, 2011.

- [13] M. Ramaiya, N. Hemrajani and A. Saxena, "Secured Steganography Approach using AES", *International Journal of Computer Science Engineering*, vol. 3, no. 2249-6832, pp. 185-192, 2013.
- [14] M. Vaidya et al., "Image Steganography using DWT and Blowfish Algorithms", *IOSR Journal of Computer Engineering*, vol. 8, no. 6, pp. 15-19, 2013.
- [15] N. Hamid, A. Yahya, R. Ahmad and O. Al-qershi, "Image Steganography Techniques: An Overview", *International Journal of Computer Science and Security (IJCSS)*, vol. 6, no. 3, pp. 168-187, 2012.
- [16] N. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen", *IEEE Computer*, vol. 31, no. 2, pp. 26-34, 1998.
- [17] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography", *IEEE Security & Privacy Magazine*, vol. 1, no. 3, pp. 32-44, 2003.
- [18] N. Saxena and G. Agrawal, "Image Steganography using DCT and DWT", *International Journal of Latest Trends in Engineering and Technology*, vol. 7, pp. 742-748, 2016.
- [19] N. Tiwari and D. Shandilya, "Evaluation of Various LSB based Methods of Image Steganography on GIF File Format", *International Journal of Computer Applications*, vol. 6, no. 2, pp. 1-4, 2010. Available: 10.5120/1057-1378.
- [20] P. Saraswat1 and R. Gupta, "A Review of Digital Image Steganography", *Journal of Pure and Applied Science & Technology*, vol. 2, no. 1, pp. 98-106, 2012.
- [21] P.V. Bodhak and B.L. Gunjal, "Improved Protection in Video Steganography Using DCT and LSB", *International Journal of Engineering and Innovative Technology*, vol. 1, no. 4, pp. 31-37, 2012.
- [22] R. Anderson, "Stretching the limits of steganography. In Information Hiding", *Springer Berlin Heidelberg.*, pp. 39-48, 1996.
- [23] R. Anderson and F. Petitcolas, "On the limits of steganography", *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 474-481, 1998. Available: 10.1109/49.668971.
- [24] R. Kaur and B. Singh, "Survey and Analysis of Various Steganographic Techniques", *International Journal of Engineering Science and Advance Technology*, vol. 2, no. 3, pp. 561-566, 2012.

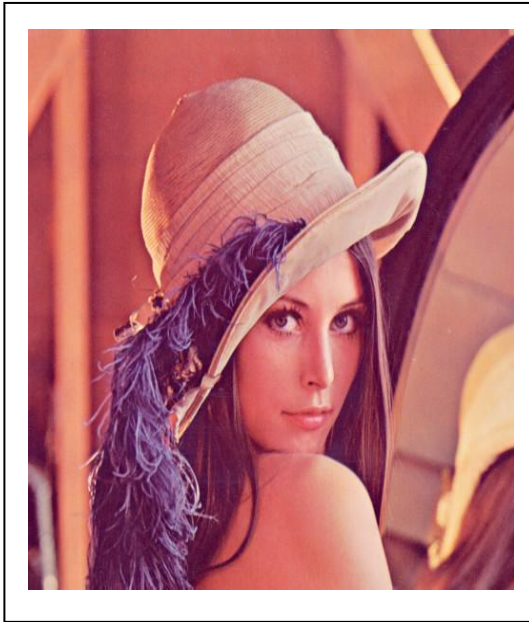
- [25] R. Vijayrajeswari, A. Rajikannan and J. Santhosh, "A Simple Steganography Algorithm Based on Lossless Compression Technique in WSN", *Circuits and System*, vol. 7, pp. 1341-1351, 2016.
- [26] S. Gupta, Ankur Goyal and B. Bhushan, "Information Hiding Using Least Significant Bit Steganography and Cryptography", *International Journal of Modern Education and Computer Science*, vol. 4, no. 6, pp. 27-34, 2012.
- [27] S. Wang, "Steganography of capacity required using modulo operator for embedding secret image", *Applied Mathematics and Computation*, vol. 164, no. 1, pp. 99-116, 2005. Available: 10.1016/j.amc.2004.04.059.
- [28] T. Narasimmalou and J. Allen, "Optimized discrete wavelet transform based steganography", 2012 IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), pp.88-91,2012.
- [29] "SIPI Image Database", *Sipi.usc.edu*, 2019. [Online]. Available: <http://sipi.usc.edu/database/>.

Appendix

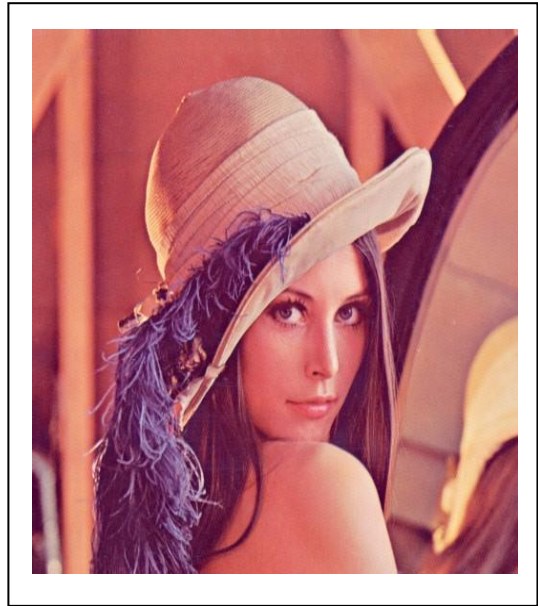
1. Input Image: Lena.jpg Original Image size: 512*512

Secret Message Embedded: The quick brown fox jumped from wall.

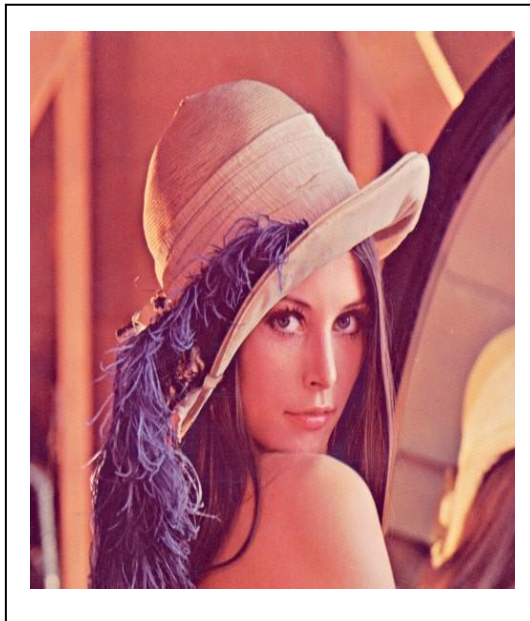
Original Image



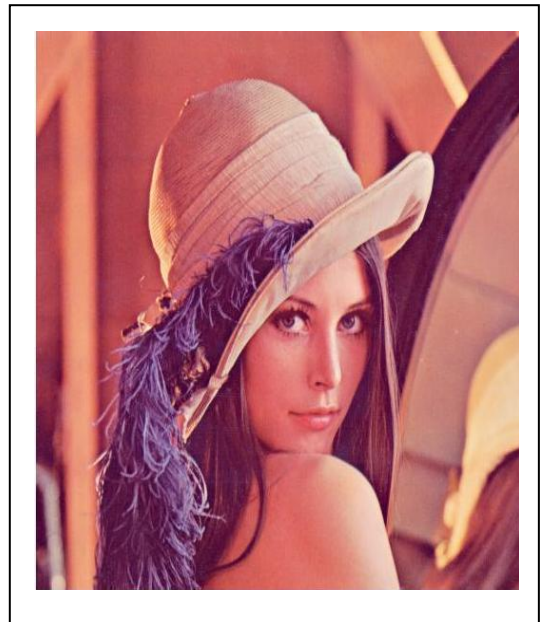
Stego image using DCT



Stego image using DCT with DWT



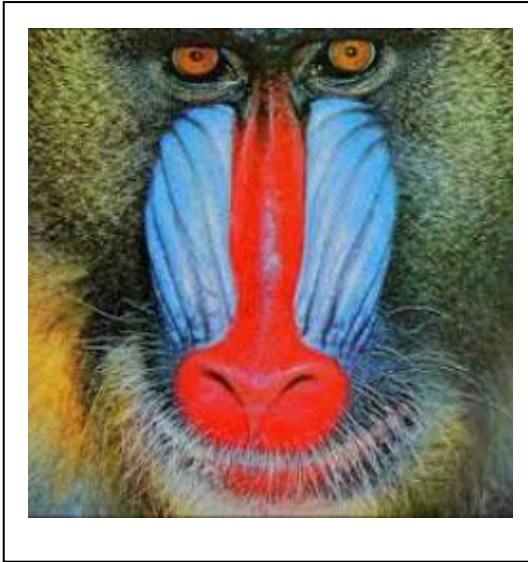
Stego Image using DWT



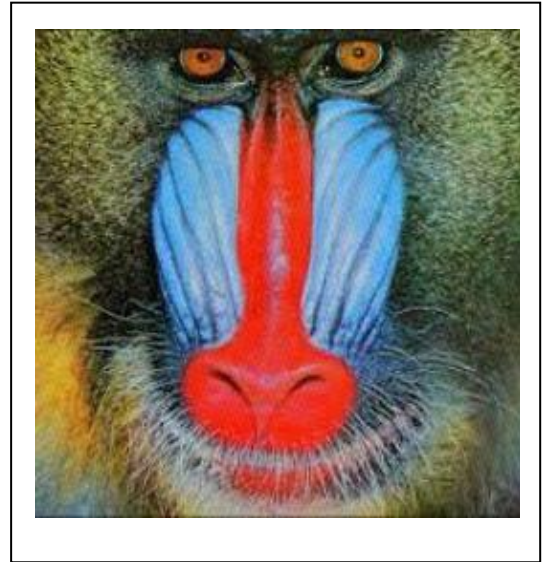
2. Input Image : Baboon.jpg size: 256*256

Secret Message Embedded: The quick brown fox jumped from wall.

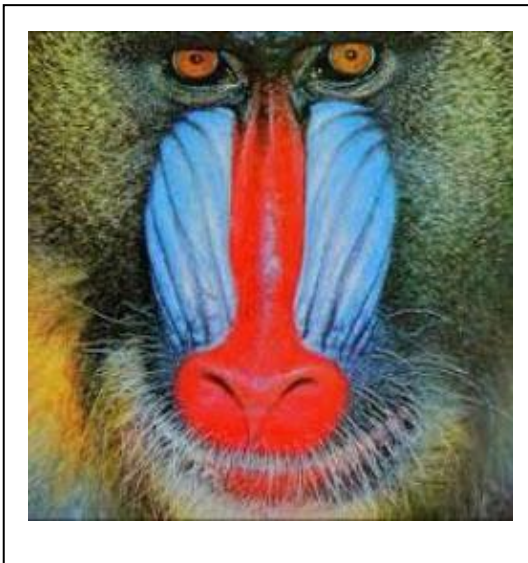
Original Image



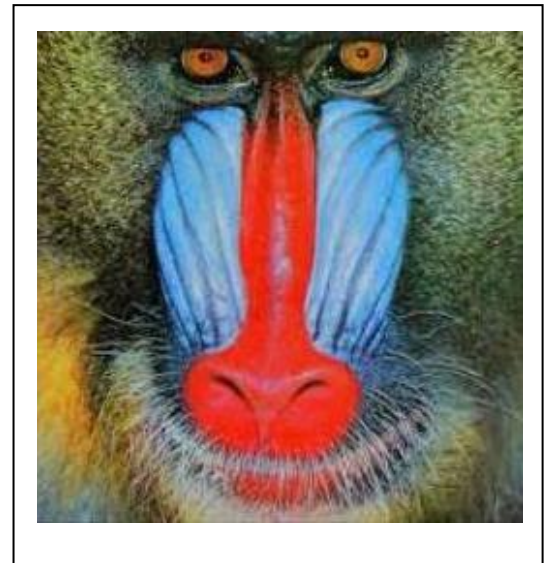
Stego Image using DCT



Stego Image using DCT with DWT



Stego Image using DWT



3. Input Image Peppers. Jpg size: 512*512

Secret Message Embedded: The quick brown fox jumped from wall

Original Image



Stego Image Using DCT



Stego Image using DCT with DWT



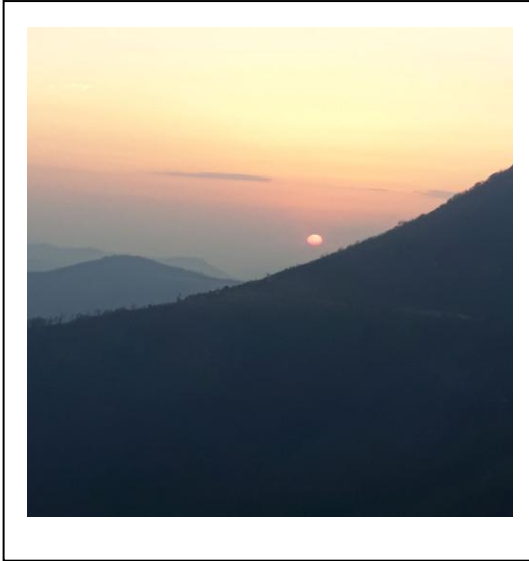
Stego Image using DWT



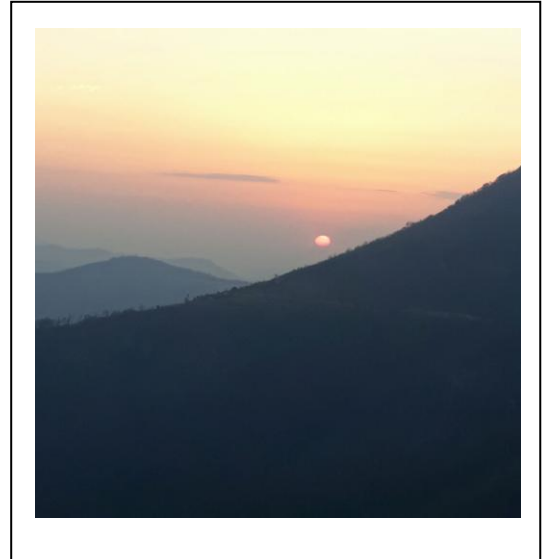
4. Input image: scene.jpg size: 1024 *1024

Secret Message Embedded: The quick brown fox jumped from wall

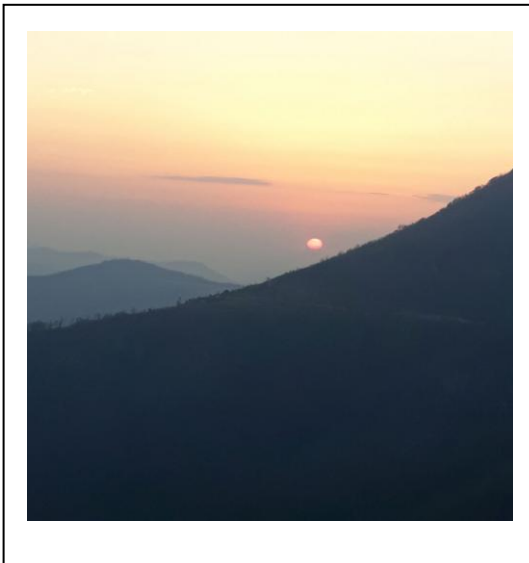
Original Image



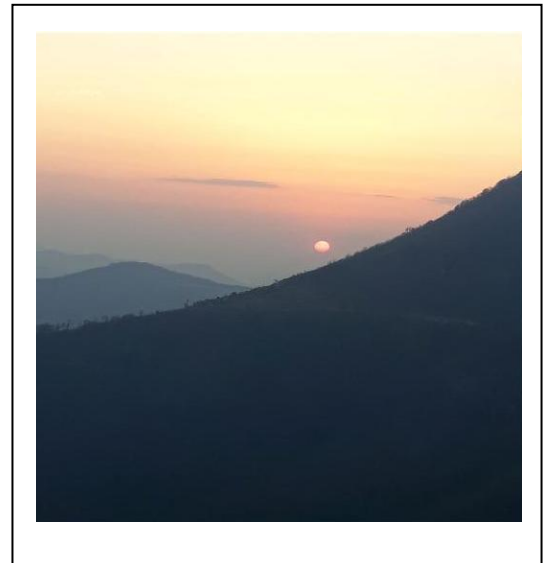
Stego Image using DCT



Stego Image using DCT with DWT



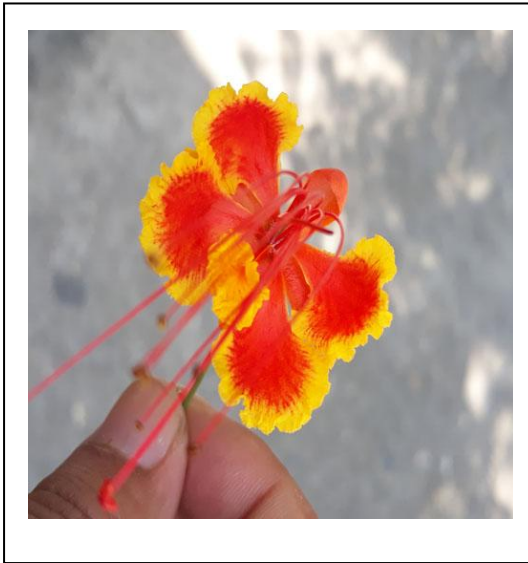
Stego Image using DWT



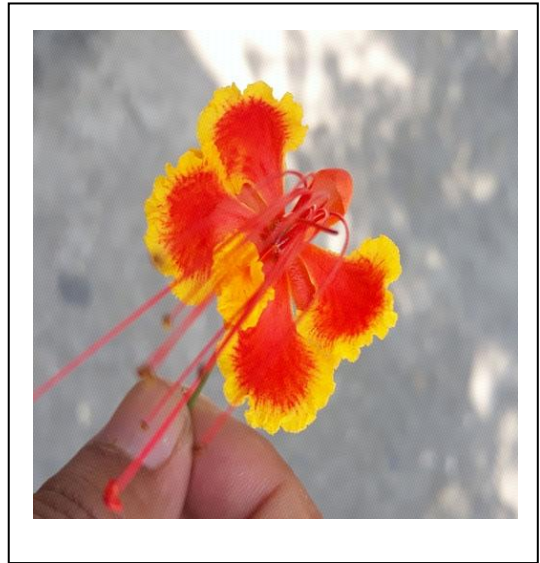
5. Input Image: Flower.jpg size: 512*512

Secret Message Embedded: The quick brown fox jumped from wall

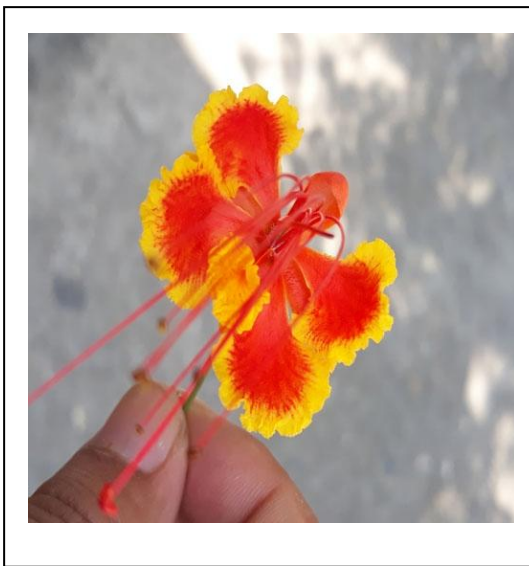
Original Image



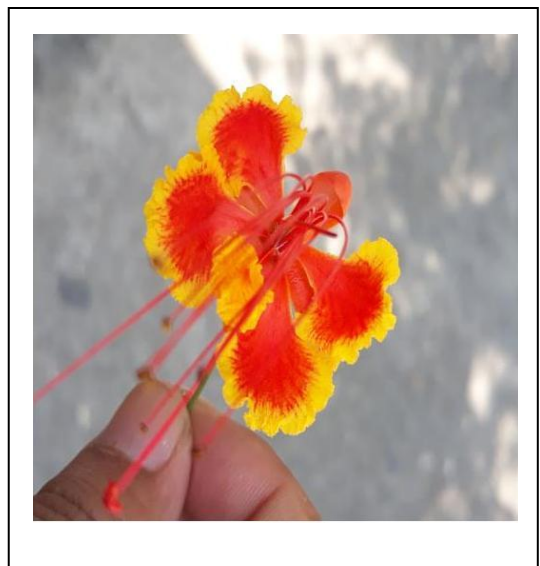
Stego Image using DCT



Stego Image using DCT with DWT



Stego Image using DWT



6. Input Image : Juice.jpg size: 512*512

Secret Message Embedded: The quick brown fox jumped from wall

Original Image



Stego Image using DCT



Stego Image using DCT with DWT



Stego Image using DWT

