Report of the Main Project Submitted in Partial Fulfilment of the Requirements for the Award of Degree of Bachelor of Technology in Electronics and Communication Engineering

COMPARATIVE ANALYSIS OF DISCRETE WAVELET TRANSFORM AND STATIONARY WAVELET TRANSFORM TECHNIQUES IN DATA HIDING

Done By

Akhil Mathew	**Reg. No. 12002231**
Angel Kurien	**Reg. No. 12002353**
Carmel Mary Jose	**Reg. No. 12002373**
Cyril Wilson	**Reg. No. 12002376**

Under the guidance of

Mr. Anu Abraham Mathew

Assistant Professor, Department of ECE

BACHELOR OF TECHNOLOGY

in

ELECTRONICS & COMMUNICATION ENGINEERING

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

AMAL JYOTHI COLLEGE OF ENGINEERING

(Affiliated to Mahatma Gandhi University)
Kanjirappally – 686 518

April - 2016

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

AMAL JYOTHI COLLEGE OF ENGINEERING
(Affiliated to Mahatma Gandhi University)
Kanjirappally – 686 518

BONAFIDE CERTIFICATE

This is to certify that the report entitled **"COMPARATIVE ANALYSIS OF DISCRETE WAVELET TRANSFORM AND STATIONARY WAVELET TRANSFORM TECHNIQUES IN DATA HIDING"** is the bonafide report of the Eighth Semester Main project done by **Akhil Mathew – Reg. No. 12002231, Angel Kurien – Reg. No. 12002353, Carmel Mary Jose – Reg.No. 12002373, Cyril Wilson – Reg. No. 12002376,** in partial fulfillment of requirements for the award of Bachelor of Technology in Electronics and Communication Engineering from Mahatma Gandhi University, Kottayam, during the year 2015-2016. They have done the project with prior approval from the Department.

Mr. Anu Abraham Mathew
Assistant Professor, ECE
Project Guide

Mr. Jaison C.S.
Assistant Professor, ECE
Project Coordinator

Prof. K G Satheesh Kumar
Head of the Department

Place: Kanjirappally

Date:

ACKNOWLEDGEMENT

First of all we sincerely thank **the Almighty God** who is the most efficient and merciful for giving us knowledge and courage to complete the project successfully.

We derive immense pleasure in expressing our sincere thanks to the Principal **Rev. Dr. Jose Kannampuzha**, for his permission and infrastructural facilities for the successful completion of our main project.

We extend our sincere gratitude to **Prof. K G Satheesh Kumar**, Head of the Department for his encouragements and motivation during our project.

We express our heartfelt gratefulness to **Mr. Anu Abraham Mathew**, Assistant Professor, Department of ECE, project guide, for his valuable guidance and suggestion during the main project.

We also extend our sincere thanks to **Mr. Jaison C.S.** and **Mr. Mathew George**, Assistant Professors, Department of ECE, project coordinators for their kind support and coordination.

We also express our gratitude to all teaching and non-teaching staff of the college especially to all the faculty members of Electronics and Communication Department for their encouragement and help done during our work.

Finally we appreciate the patience and solid support of our parents and enthusiastic friends for their moral support and encouragement for this effort.

Akhil Mathew
Angel Kurien
Carmel Mary Jose
Cyril Wilson

ABSTRACT

Digital image being one of the best media to store data, provides large capacity for hiding secret information imperceptible to human vision. Hence data hiding finds its application in covert communications, copy control, traitor tracing, authentication of digital images, etc. The aim of this project is a comparative analysis of data hiding using two techniques: Discrete Wavelet Transform (DWT) and Stationary Wavelet Transform (SWT). The basic data hiding technique consists of choosing a cover image, encrypting the image to be hidden, performing DWT/SWT and hiding the encrypted image into the cover image and finally retrieving the hidden image.

An analysis is performed on the retrieved image and parameters such as Peak Signal to Noise Ratio and Mean Square Error are calculated. On basis of this analysis, the most efficient technique is proposed.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1
INTRODUCTION

Data hiding is the process of hiding an image or text into another cover image. Data hiding is also frequently termed as steganography and is closely related to cryptography. The purpose of cryptography is to make messages unintelligible so that those who do not possess secret keys cannot recover the messages. Sometimes, it may be desirable to achieve security and privacy by masking the very presence of communication instead of exchanging encrypted messages. This problem is addressed by steganography. Historically, the first steganographic techniques included invisible writing using special inks or chemicals. It was also fairly common to hide messages in text. By recovering the first letters from words or sentences of text, a secret message was communicated. Today, it seems natural to use binary files with certain degree of irrelevancy and redundancy to hide data. Digital images, videos, and audio tracks are ideal for this purpose. The hidden message may have no relationship to the carrier image in which it is embedded as in case of covert communication. Alternatively, the message may supply important information about the carrier image, such as copyright notice, authentication information, captions, date and time of creation, serial number of the digital camera that took the picture, information about image content etc.

In this digitalized world, sharing or passing of data from one place to another takes place through internet. Providing security to the confidential data which is passing through internet becomes a major concern. Nowadays, security measures have grown rapidly all over the world. Cryptography, steganography and watermarking are the widely used techniques for securing data. In cryptography original message itself is made unreadable so that it cannot be easily understood by any third party other than the authorized party. Figure 1.1 represents the different branches of the security system.

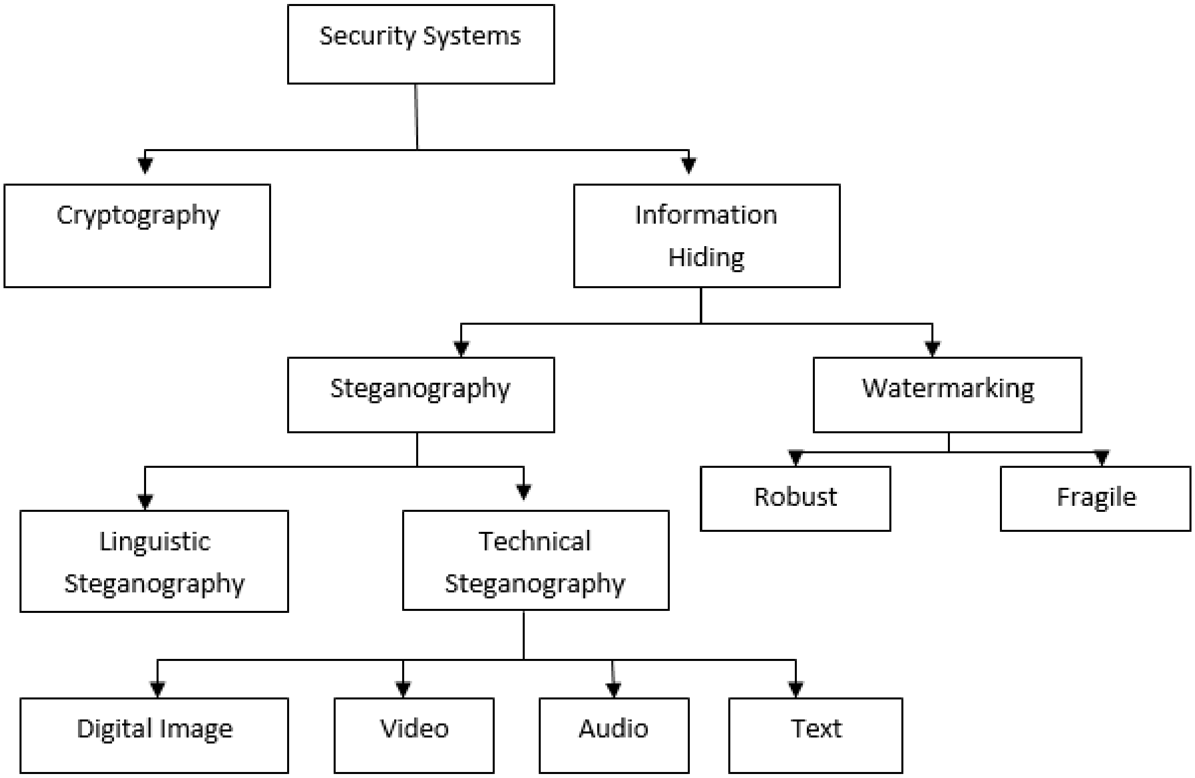

Figure 1.1 Different branches of security system

1.1 Steganography

Steganography is one of the methods which provide security to the data communication system. In this method, secret original data is hidden in cover image without altering original data. Multimedia signals like audio, video and images are used as carrier for original message. The image or text in which object is hidden is called cover image. The hidden confidential data may be plain text, encrypted text or an image. Stego-image is the image procured after the embedding process i.e., it is a combination of original data and cover image. To protect against harmful threats, an additional assurance or barrier is provided before embedding process by using a security key. This key ensures that only the advised person will be able to access confidential data.

1.2 Cryptography

Cryptography is the process of converting ordinary information (plain text) into unintelligible text (cipher text). A cipher is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a secret key. The key, ideally known only to the communicants, is usually a short string of characters, which is needed to decrypt the cipher text.

Cryptanalysis is the study of methods used for obtaining the encrypted information without access to the key which is normally required i.e., it is the study of how to crack encryption algorithms or their implementations.

The terms cryptography and cryptology are used interchangeably in English. Cryptography refers specifically to the use and practice of cryptographic techniques and cryptology refers to the combined study of cryptography and cryptanalysis. The study of characteristics of languages that have some application in cryptography or cryptology is called crypto-linguistics. For example, frequency data, letter combinations, universal patterns etc.

1.3 Watermarking

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as an audio, video or image data. It is typically used to identify ownership of the copyright of such signal. Watermarking is the process of hiding digital information in a carrier signal. The hidden information should, but does not need to contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright infringements and for banknote authentication.

Like traditional watermarks, digital watermarks are only perceptible under certain conditions and imperceptible otherwise. If a digital watermark distorts the carrier signal in a way that it becomes imperceivable, then it is of no use. Traditional watermarks may be applied to visible media (like images or video), whereas in digital watermarking, the signal may be audio, pictures, video, texts or 3D models. A signal may carry several different watermarks at the same time.

Unlike metadata that is added to the carrier signal, a digital watermark does not change the size of the carrier signal. The needed properties of a digital watermark depend on the case in which it is applied. For marking media files with copyright information, a digital watermark has to be rather robust against modifications that can be applied to the carrier signal. Instead, if integrity has to be ensured, a fragile watermark would be applied.

Both steganography and digital watermarking employ steganographic techniques to embed data covertly in noisy signals. While steganography aims for imperceptibility to human senses, digital watermarking tries to control the robustness as top priority.

Since a digital copy of data is the same as the original, digital watermarking is a passive protection tool. It just marks data but does not degrade it or control access to the data. One application of digital watermarking is source tracking. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known. This technique reportedly has been used to detect the source of illegally copied movies.

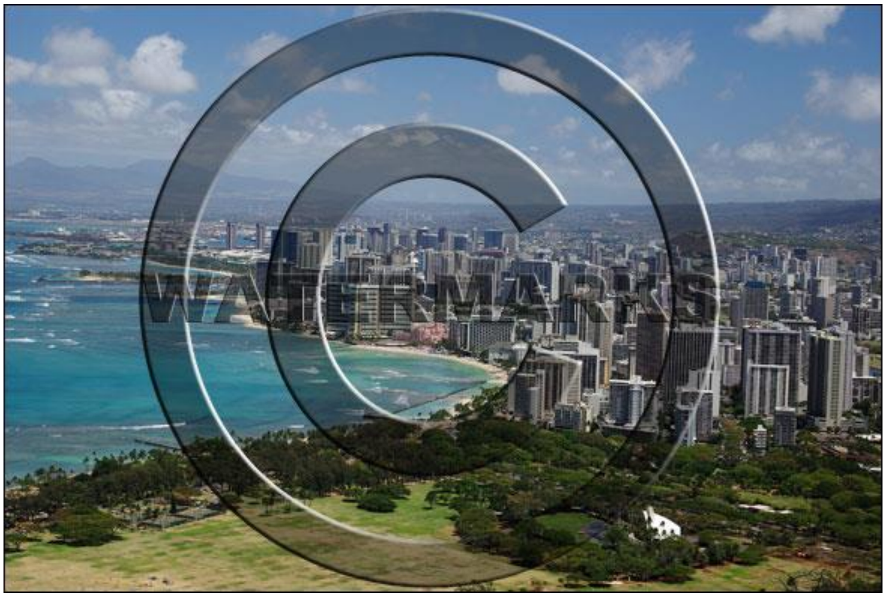

Figure 1.2 An example of watermarking

CHAPTER 2
DATA HIDING

Data hiding is referred to as a process to hide data into cover media. That is, the data hiding process links two sets of data, a set of the embedded data and another set of the cover media data. In most cases of data hiding, the cover media becomes distorted due to data hiding and cannot be inverted back to the original media. That is, cover media has permanent distortion even after the hidden data has been removed. In some applications, such as medical diagnosis and law enforcement, it is desired that the original cover media should be recovered efficiently with no loss. The marking techniques satisfying this requirement are referred to as reversible, lossless, distortion-free or invertible data hiding techniques. Reversible data embedding, which is also called lossless data embedding, embeds invisible data (payload) into a digital image in a reversible fashion. As a basic requirement, the quality degradation on the image after data embedding should be low. An exciting feature of reversible data embedding is the reversibility, that is, one can remove the embedded data to restore the original image. Reversible data embedding hides some information in a digital image in such a way that an authorized party could decode the hidden information and also restore the image to its original state.

In the basic steganographic process, the secret message is hidden into a cover object. The cover object can be text, image, audio, video etc. A secret key is also used and the secret message is embedded into the cover object using the secret key. This new message obtained is called stego message. The stego message is transmitted over the public channel. The receiver gets the message and retrieves the message using the stego key which is same as that used by the sender. In this way security is achieved by hiding the existence of the message.

Image steganography is a process that hides the message into cover image and generates a stego-image. The stego-image is then sent to the receiver without anyone else knowing that it contains the hidden message. The receiver can extract the message with or without stego-key. This depends on the scheme used for data hiding.

Stego-medium = Cover medium + Secret message + Stego key

Some of the basic term used in steganography:

1. **Message:** Actual information which is to be hidden into images. Message can be a plain text or other image.
2. **Cover-object:** It refers to the object used as a carrier in which message is embedded
3. **Stego-object:** Object which is carrying a hidden message.
4. **Stego-key:** Key which refers to a password used to hide and later retrieve the message.
5. **Embedding algorithm:** An algorithm used to hide the message.
6. **Extracting algorithm:** An algorithm used to unhide/uncover the message.

A few key properties that must be considered while creating a digital data hiding system are:

1. Capacity: Indicates the amount of confidential data that can be embedded without worsening the quality of the cover image.

2. Robustness: Indicates by how much the stego image is immune to possible attacks.

3. Invisibility: Third party or attacker should not figure out the existence of secret data in cover image except the intended person.

4. Mean square error: It indicates the difference in quality of stego-image and cover image.

5. Imperceptibility: Imperceptibility is the property in which a person should be unable to

distinguish the original and the stego-image.

A large number of embedding techniques have been proposed for steganography in literatures. These techniques modify the cover image with different approaches as well as constrains. But all embedding techniques share the important goal of maximizing the capacity of the stego channel. In other words, their aim is to embed at the highest possible rate while remaining undetectable to steganalysis attack.

2.1 Classification based on domain:

All the popular data hiding methods can be divided into two major classes: spatial domain embedding and transform domain embedding.

2.1.1 Spatial Domain

Spatial domain techniques embed information in the intensity of the original image pixels. Basically least significant bit (LSB) method is used where it replaces the least significant bit of original pixel with the message bit.

2.1.2 Transform Domain

Transform domain is also known as frequency domain. Here, the image is transformed from time domain to frequency domain using mathematical operators called transforms. There are many transforms like Discrete wavelet transform, Fourier transform, Discrete cosine transform, Z-transform and so on. Transform domain enables operation on the frequency content of an image, and therefore high frequency content such as edges and other subtle information can easily be modified. Low frequency band consists of smooth region of an image and hence it contains more information of an image as compared to high frequency band.

2.2 Classification based on key:

Steganography can be of three types based on the key used,

2.2.1 Pure steganography

Here, there is no stego-key. It is based on the assumption that no other party is aware of the communication.

2.2.2 Secret key steganography

Here, the stego-key is exchanged prior to communication. This is most susceptible to interception.

2.2.3 Public key steganography

Here, a public key and a private key is used for secure communication.

2.3 Classification based on encoding technique

Steganography methods can be classified mainly into six categories:

1. **Substitution methods** substitute redundant parts of a cover with a secret message
2. **Transform domain techniques** embed secret information in a transform space of the signal
3. **Spread spectrum techniques** adopt ideas from spread spectrum communication.
4. **Statistical methods** encode information by changing several statistical properties of a cover and use hypothesis testing in the extraction process.
5. **Distortion techniques** store information by signal distortion and measure the deviation from the original cover in the decoding step.
6. **Cover generation methods** encode information in the way a cover for secret communication is created.

CHAPTER 3
REVERSIBLE DATA HIDING

Reversible data hiding in images is a technique that hides data in digital images for secret communication. It is a technique to hide additional message into cover media in a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message. Traditionally, data hiding is used for secret communication. In some applications, the embedded carriers are further encrypted to prevent the carrier from being analysed to reveal the presence of embedment. Other applications could be for when the owner of the carrier might not want the other person, including data hider, to know the content of the carrier before data hiding is actually performed, such as military images or confidential medical images. In this case, the content owner has to encrypt the content before passing it to the data hider for data embedment. It may be hopeful that the original content can be recovered without any error after decryption and retrieve the additional message at receiver side. Many reversible data hiding methods have been proposed recently.

As is well known, encryption is an effective and popular means of privacy protection. In order to securely share a secret image with other person, a content owner may encrypt the image before transmission. In some application scenarios, an inferior assistant or a channel administrator hopes to append some additional message, such as the origin information, image notation or authentication data, within the encrypted image though he does not know the original image content. For example, when medical images have been encrypted for protecting the patient privacy, a database administrator may aim to embed the personal information into the corresponding encrypted images.

A major recent trend is to minimize the computational requirements for secure multimedia distribution by selective encryption where only parts of the data are encrypted. There are two levels of security for digital image encryption: low level and high-level security encryption. In low-level security encryption, the encrypted image has degraded visual quality compared to that of the original one, but the content of the image is still visible and understandable to the viewers. In the high-level security case, the content is completely scrambled and the image just looks like random noise. In this case, the image is not understandable to the viewers at all. Selective encryption aims at avoiding the encryption of all bits of a digital image and yet ensuring a secure encryption.

Reversible data hiding is a technique to embed additional message into some distortion-unacceptable cover media, such as military or medical images, with a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message. As an effective and popular means for privacy protection, encryption converts the ordinary signal into incomprehensible data, so that the general signal processing typically takes place before encryption or after decryption. However, in circumstances that a content owner does not trust the service provider, the ability to manipulate the encrypted data when keeping the plain content secret is desired. When the secret data to be transmitted are encrypted, a channel provider without any knowledge of the cryptographic key may compress the encrypted data due to the limited channel resource. Encryption is an effective means of privacy protection. To share a secret image with other person, a content owner may encrypt the image before transmission. In some cases, a channel administrator needs to add some additional message, such as the origin information, image notation or authentication data, within the encrypted image however he does not know the original image content. It may be also expected that the original content can be recovered without any error after decryption and retrieval of additional message at receiver side. That means a reversible data hiding scheme for encrypted image is desirable.

CHAPTER 4
METHODS FOR IMAGE ENCRYPTION

4.1 Hashing Encryption

Hashing is an encryption method that creates a unique, fixed-length signature for a message or data set. It is created with hash function and is commonly used to compare sets of data. Since a hash is unique to a specific message, even minor changes to that message results in dramatically different hash, there by alerting a user to potential tampering.

4.2 Symmetric Encryption

Symmetric cryptography, also called private-key cryptography, is one of the oldest and most secure encryption methods. The term private key comes from the fact that the key used to encrypt and decrypt data must remain secure because anyone with access to it can read the coded messages. A sender encodes a message into cipher text using a key, and the receiver uses the same key to decode.

4.3 Asymmetric Encryption

Asymmetric or public key cryptography is potentially more secure than symmetric method of encryption. This type of cryptography uses two keys, a private key and a public key to perform encryption and decryption. The use of two keys overcomes a major weakness in symmetric key cryptography. This is so because a single key does not need to be securely managed among multiple users. In asymmetric cryptography, a public key is freely available to everyone and is used to encrypt messages before sending them. A different private key remains with the receiver of cipher text messages, who uses it to decrypt them. Algorithms that use public key encryption methods include RSA and Differ-Hellman.

4.4 AES Encryption

The algorithm is flexible in supporting any combination of data and key size of 128, 192, and 256 bits. However, AES merely allows a 128 bit data length that can be divided into four basic operation blocks. These blocks operate on array of bytes and organized as a 4x4 matrix that is called the state. For full encryption, the data is passed through N rounds (N = 10, 12, 14)

4.5 Block-Based Transformation

In block based transformation technique, the original image is divided into a random number of blocks that are then shuffled within the image. The generated (or transformed) image is then fed to the Blowfish encryption algorithm. The main idea is that an image can be viewed as an arrangement of blocks. The intelligible information present in an image is due to the correlation among the image elements in a given arrangement. This perceivable information can be reduced by decreasing the correlation among the image elements using certain transformation techniques. The secret key of this approach is used to determine the seed. The seed plays a main role in building the transformation table, which is then used to generate the transformed image with different random number of block sizes. The transformation process refers to the operation of dividing and replacing an arrangement of the original image.

CHAPTER 5
METHODS FOR DATA EMBEDDING

5.1 Discrete Wavelet Transform

Wavelet transform is a time domain localized analysis method. The basic idea of discrete wavelet transform (DWT) in image processing is to decompose the image into sub-images of different spatial domain and independent frequency district. The original image is first high-pass filtered, yielding the three large images, each describing local changes in brightness (details) in the original image. It is then low-pass filtered and downscaled, yielding an approximation image. This image is high-pass filtered to produce the three smaller detail images, and low-pass filtered to produce the final approximation image in the upper-left. After the original image has been DWT transformed, it is decomposed into four frequency districts which is one low-frequency district(LL) and three high-frequency districts (LH, HL, HH). LL represents low pass in both horizontal and vertical. It is also called approximate band. LH is horizontally low pass and vertically high pass it is also called horizontal band. HL is Horizontally high pass and vertically low pass. It is also called the vertical band. HH is horizontally and vertically high pass and is also called diagonal detail band. DWT outperforms DCT because time consumption in DCT is more and also complexity is increased.

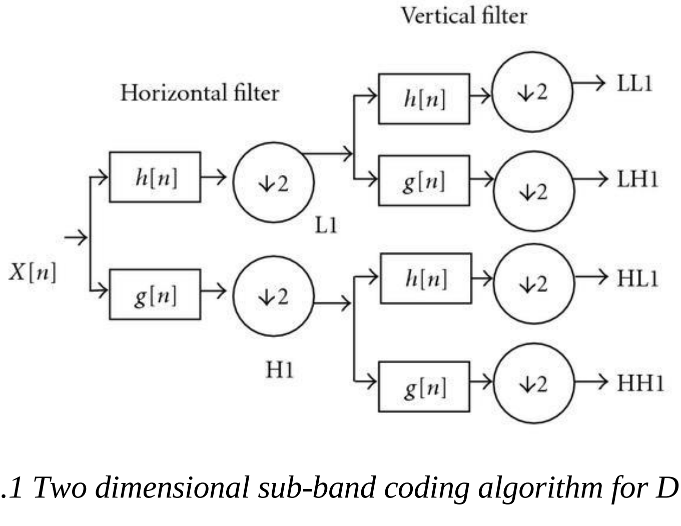

Figure 5.1 Two dimensional sub-band coding algorithm for DWT

If the information of low-frequency district is DWT transformed, the sub-level frequency district information will be obtained. A two dimensional image after two-times DWT decomposed is shown as Figure 5.1. Here, L represents low-pass filter, H represents high-pass filter. The image can be decomposed into frequency districts of HL1, LH1, HH1.

In numerical analysis and functional analysis, a Discrete Wavelet Transform (DWT) is any wavelet transform for which the wavelets are discretely sampled. As with other wavelet transforms, a key advantage it has over fourier transforms is temporal resolution. It captures both frequency and location information (location in time).

The DWT of a signal x is calculated by passing it through a series of filters. First the samples are passed through a low pass filter with impulse response g resulting in a convolution of the two:

$$y[n] = (x * g)[n] = \sum_{k=-\infty}^{\infty} x[k]g[n-k] \tag{5.1}$$

The signal is also decomposed simultaneously using a high-pass filter h. The outputs giving the detail coefficients (from the high-pass filter) and approximation coefficients (from the low-pass). It is important that the two filters are related to each other and they are known as a quadrature mirror filter.

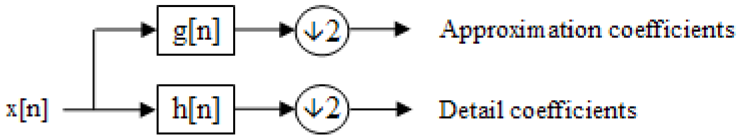

Figure 5.2 Block diagram of filter analysis

However, since half the frequencies of the signal have now been removed, half the samples can be discarded according to Nyquist’s rule. The filter outputs are then sub sampled by two.

$$y_{low}\,[n] = \sum_{k=-\infty}^{\infty} x[k]h[2n-k] \tag{5.2}$$

$$y_{high}[\text{n}]=\sum_{k=-\infty}^{\infty} x[k]g[2n-k] \tag{5.3}$$

This decomposition has halved the time resolution since only half of each filter output characterizes the signal. However, each output has half the frequency band of the input so the frequency resolution has been doubled.

However computing a complete convolution $x \times g$ with subsequent down sampling would waste computation time. The lifting scheme is an optimization where these two computations are interleaved.

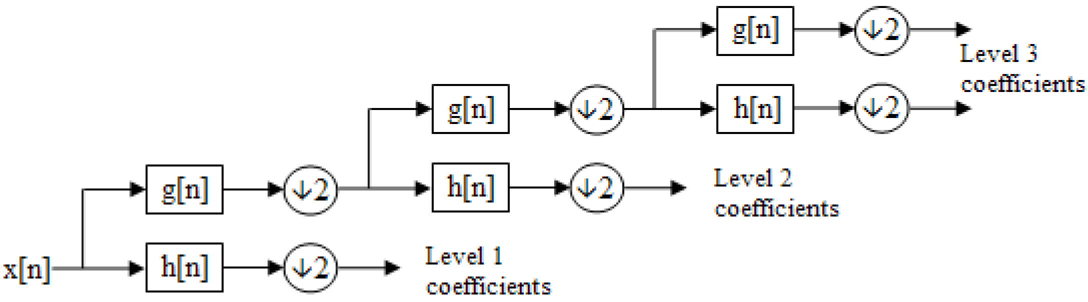

Figure 5.3 Three level filter bank

This decomposition is repeated to further increase the frequency resolution and the approximation coefficients are decomposed with high and low pass filters and then down-sampled. This is represented as a binary tree with nodes representing a sub-space with a different time-frequency localization. The tree is known as a filter bank.

At each level in the above diagram the signal is decomposed into low and high frequencies. Due to the decomposition process the input signal must be a multiple of 2^n where 'n' is the number of levels.

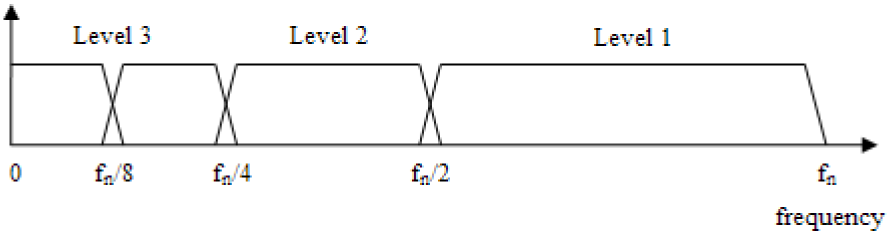

Figure 5.4 Frequency domain representation of DWT

The Discrete Wavelet Transform has huge number of applications in science, engineering, mathematics and computer science. Most notably, it is used for signal coding, to represent a discrete signal in a more redundant form, often as a preconditioning for data compression. Practical applications can also be found in signal processing of accelerations for gait analysis in digital communications and many others.

5.2 Stationary Wavelet Transform

The Stationary Wavelet Transform (SWT) is a wavelet transform algorithm designed to overcome the lack of translation-invariance of the Discrete Wavelet Transform (DWT). The way to restore the translation invariance is to average some slightly different DWT, called un-decimated DWT, to define the stationary wavelet transform (SWT). It does so by removing the down-samplers and up-samplers in the DWT and up-sampling the filter coefficients by a factor of $2^{(j-1)}$ in the j^{th} level of the algorithm. The SWT is therefore an inherently redundant scheme in which the output of each level of SWT contains the same number of samples as the input. So for a decomposition of N levels, there is a redundancy of N in the wavelet coefficients. As with the decimated algorithm, the filters are first applied to the rows and then to the columns. Although four images are produced (one approximation and three detail images) at half the resolution of the original, they are of the same size as the original image. The approximation images from the un-decimated algorithm are therefore represented as levels in a parallel-piped, with the spatial resolution becoming coarser at each higher level with the size remaining the same.

The 2D Stationary Wavelet Transform (SWT) is based on the idea of no decimation. SWT omits both down-sampling in the forward and up-sampling in the inverse transform. More precisely, it applies the transform at each point of the image and saves the detail coefficients. This algorithm is more famously known as "*algorithme à trous*" in French which refers to inserting zeros in the filters. It was introduced by Holschneider et al.

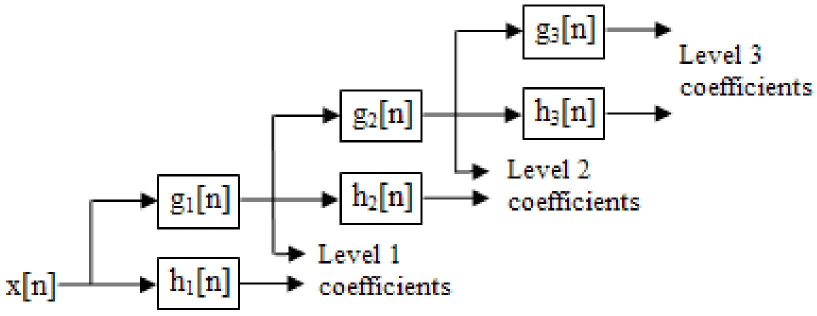

Figure 5.5 Three level SWT filter bank

Few applications of SWT are specified below:

- Signal denoising
- Pattern recognition
- Brain image classification

5.3 LSB compression method

LSB is the most basic method and is commonly used for creating the sparse space. The sparse space created is useful for hiding the additional payload data. In this, some parameters are added into small number of encrypted pixels, and the LSB of the other encrypted pixels are compressed to create a space for accommodating additional data.

Least Significant Bit (LSB) insertion is a common and simple approach to embed information into an image file. In this method the LSB of a byte is replaced with an M bit. This technique works good for image steganography. To the human eye the stego image will look identical to the carrier image. For hiding information inside the images, the LSB method is usually used. To a computer, an image file is simply a file that shows different colours and intensities of light on different areas of an image. The best type of image file to hide information inside is a 24 Bit BMP (Bitmap) image. When an image is of high quality and resolution, it is a easier to hide information inside image. Although 24 bit images are best for hiding information due to their size, some people may choose 8 Bit BMP or possibly another image format such as GIF. The reason is that posting of large images on the internet may arouse suspicion. The least significant bit i.e. the eighth bit is changed to a bit of the secret message. When using a 24-bit image, one can store 3 bits in each pixel by changing a bit of each of the red, green and blue colour components. Suppose that we have three adjacent pixels (9 bytes) with the RGB encoding

10010101 00001101 11001001

10010110 00001111 11001011

10011111 00010000 11001011

If the number 300, whose binary representation is 100101100 is to be embedded into the least significant bits of this part of the image, these 9 bits are overlayed over the LSB of the 9 bytes above to get the following (where bits in bold have been changed)

1001010**1** 0000110**0** 1100100**0**

1001011**1** 0000111**0** 1100101**1**

1001111**1** 0001000**0** 1100101**0**

Here the number 300 was embedded into the grid and only 5 bits were needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size.

5.4 Discrete Cosine Transform:

A Discrete Cosine Transform (DCT) expresses a finite sequence of data points in terms of sum of cosine functions oscillating at different frequencies. DCTs are important to numerous applications in science and engineering, from lossy compression of audio (e.g. MP3) and images (e.g. JPEG) where small high-frequency components can be discarded, to spectral methods for the numerical solution of partial differential equations. The use of cosine rather than sine functions is critical for compression, since it turns out that fewer cosine functions are needed to approximate a typical signal, whereas for differential equations the cosines express a particular choice of boundary conditions.

In particular, a DCT is a fourier-related transform similar to the Discrete Fourier transform (DFT), but using only real numbers. DCTs are equivalent to DFTs of roughly twice the length, operating on real data with even symmetry where in some variants of the input and/or output data are shifted by half a sample.

Like any fourier-related transform, DCT expresses a function or a signal in terms of sum of sinusoids with different frequencies and amplitudes. Like the DFT, a DCT operates on a function at a finite number of discrete data points. The obvious distinction between a DCT and a DFT is that the former uses only cosine functions, while the latter uses both cosines and sines (in the form of complex exponentials). However, this visible difference is merely a consequence of a deeper distinction i.e. DCT implies different boundary conditions from the DFT or other related transforms.

However, as DCTs operate on finite, discrete sequences, two issues arise that do not apply for the continuous cosine transform.

- It should specify whether the function is even or odd at both the left and right boundaries of the domain
- It should specify around what point the function is even or odd.

CHAPTER 6
PROPOSED METHOD

The proposed scheme consists of three main phases: image encryption, data embedding and data extraction. The cover image is first selected from the database. DWT and SWT is performed before embedding the secret image to get the stego-image. A key is used by the sender for the embedding procedure. The same key is used by the recipient to extract the cover image in order to view the secret image. The stego image should look identical to the cover image.

6.1 Embedding Algorithm

Step 1: Select cover image and perform DWT/SWT transform to get LL, LH, HL and HH components

Step 2: Find size of HH component

Step 3: Select secret image and convert to grayscale

Step 4: Resize the secret image to the size of HH component

Step 5: Generate random number which serves as key and create key array

Step 6: Encrypt the secret image by performing bitwise XOR operation with the key array

Step 7: Place the encrypted image on the HH component

Step 8: Perform IDWT/ISWT with the renewed HH component to get the intermediate image

Step 9: This intermediate image is again put into the HH component of another cover image to get the stego image

6.2 Extraction Algorithm

Step 1: Perform DWT over the received image and original cover image

Step 2: Subtract the HH portions of the cover image with from the received image

Step 3: Perform DWT on this subtracted data

Step 4: Remove normal HH from the HH received from step 3

Step 5: Generate key array

Step 6: Perform bitwise XOR operation of the key array and the result of step 4 to get the secret image

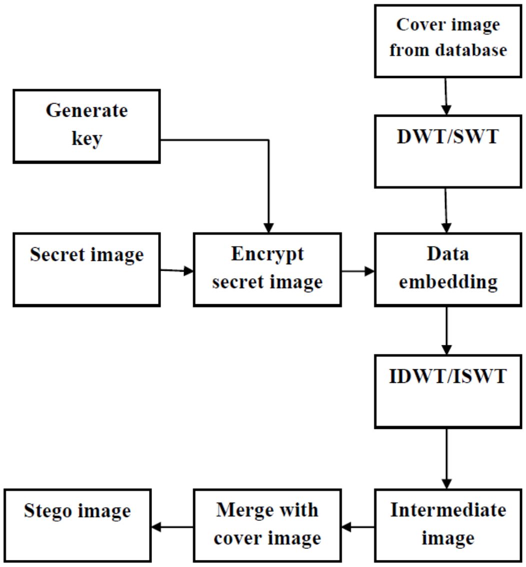

Figure 6.1 Block diagram of embedding process

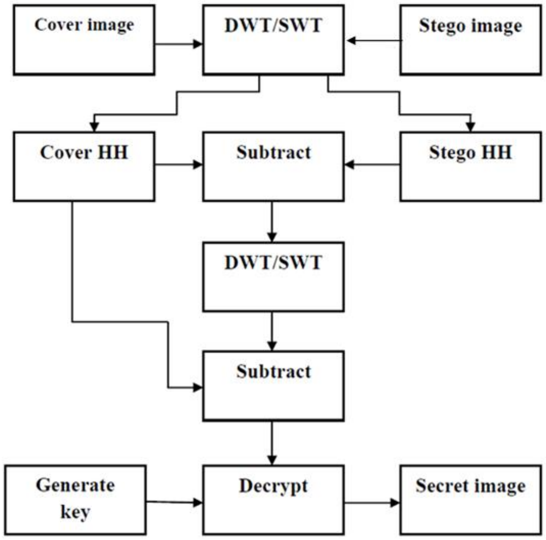

Figure 6.2 Block diagram of extraction process

6.3 Performance Parameters

The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to compare image quality. The MSE represents the cumulative squared error between the extracted hidden image and the original secret image. PSNR represents a measure of the peak signal to noise. Peak Signal to Noise Ratio (PSNR) is calculated to analyze quality of image. Here, a comparison of the PSNR results of the two techniques DWT and SWT is done by this algorithm. The PSNR calculation of two images, one original secret image and extracted image, describes how far the two images are equal. PSNR in dB given as

$$\mathrm{PSNR(dB)} = 10\log_{10}\left(\frac{\mathrm{R}^2}{\mathrm{MSE}}\right) \tag{6.1}$$

where R= maximum pixel dimension

The mean square error is calculated by the equation

$$\frac{1}{\mathrm{MSE}} = \frac{1}{\mathrm{MN}}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[\mathrm{I}(i,j) - \mathrm{K}(i,j)]^2 \tag{6.2}$$

where M represents the number of rows and N represents the number of columns. I and K are the matrix of the extracted image and the original secret image at (i,j)th pixel respectively.

6.4 Advantages of proposed method

The following are the advantages of the proposed method:

1. Hiding data only in certain regions of the cover data increases the security level.

2. No one can extract the data until and unless they get the value of the key.

3. Data is hidden in the higher frequency band rather than the lower frequency band. Hence a good stego image quality is obtained.

CHAPTER 7
SIMULATED RESULTS

Simulation is carried by using MATLAB software. The simulation results obtained after compiling and running the program are shown below. The cover image is shown in figure 7.1 and the secret image which is to be hidden is shown in figure 7.2

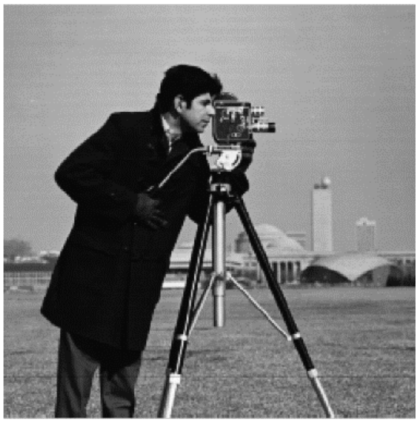

Figure 7.1 Cover image

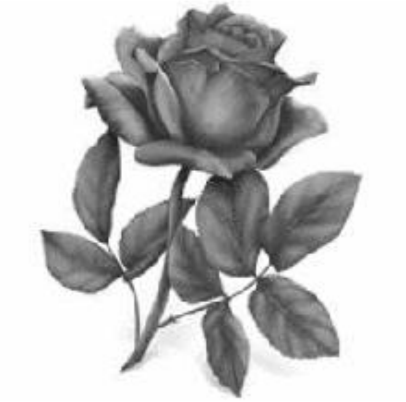

Figure 7.2 Secret image “flower.jpg”

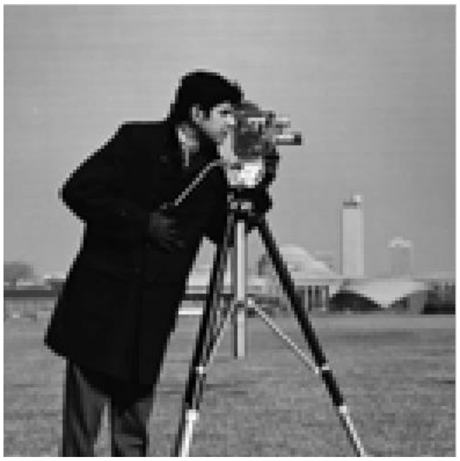

Figure 7.3 Image after embedding using DWT technique

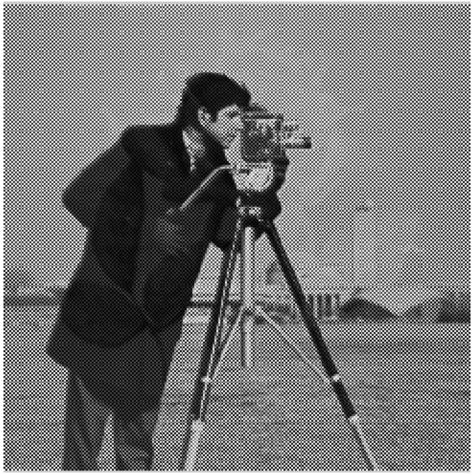

Figure 7.4 Image after embedding using SWT technique

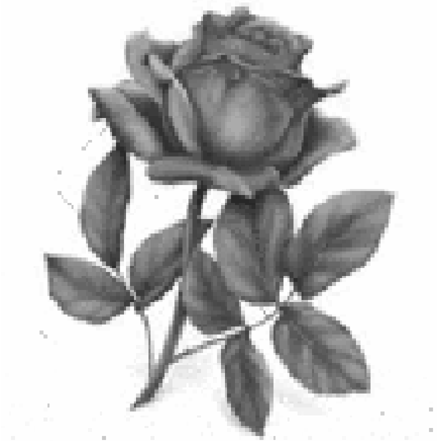

Figure 7.5 Secret image after extraction using DWT technique

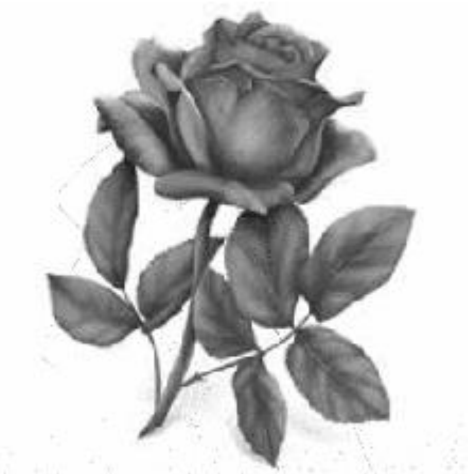

Figure 7.6 Secret image after extraction using SWT technique

The proposed method is performed on various images like Lena, Football, Baboon and Flower as shown in figure 7.7. The PSNR and MSE values are obtained and the comparison is noted as shown in Table 7.1.

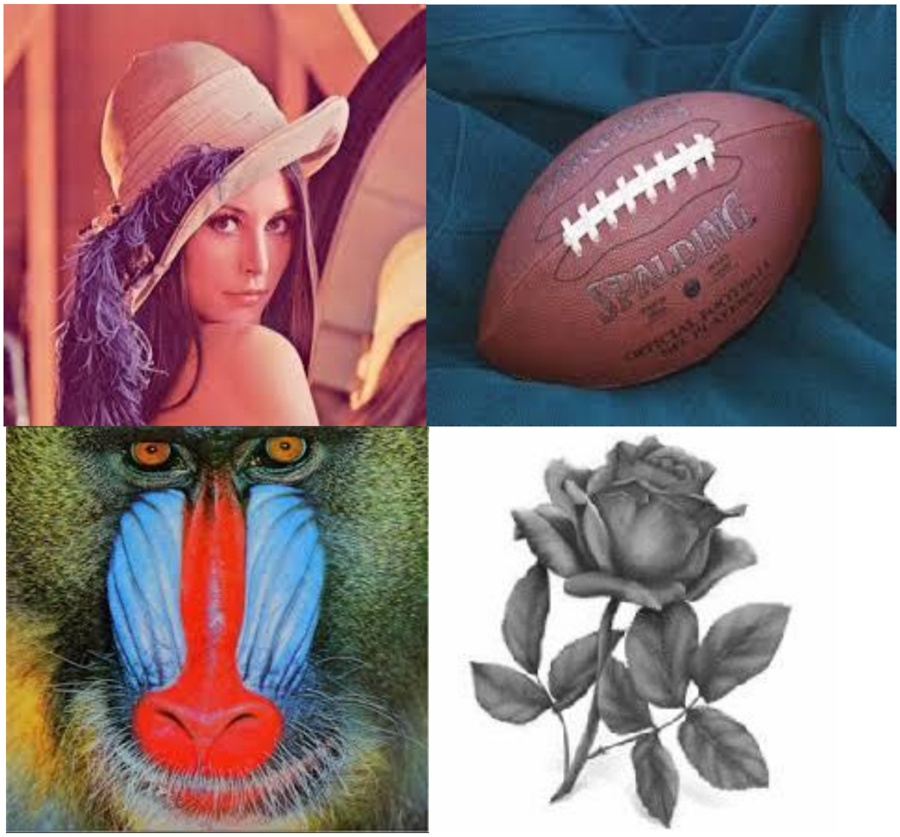

Figure 7.7 Images Lena, Football, Baboon and Flower used as secret images

Table 7.1 Comparison of PSNR and MSE values

Secret image	PSNR value	MSE value	Method
Baboon	42.84	3.41	DWT
	40.81	5.44	SWT
Football	51.25	0.49	DWT
	46.86	1.35	SWT
Lena	55.48	0.05	DWT
	68.59	0.01	SWT
Flower	35.7	4.48	DWT
	39.86	6.77	SWT

CHAPTER 8
CONCLUSION

This work is a comparison of data hiding using the transform based techniques – Discrete Wavelet Transform and Stationary Wavelet Transform. The proposed technique uses DWT/SWT to decompose an image into various sub-bands, and then the encrypted secret image is hidden in the high frequency sub-band of the image. Afterwards, by performing IDWT with the altered frequency sub-bands, the image is reconstructed. The proposed technique has been tested on various images and image quality is assessed by using performance parameters like PSNR and MSE. The embedded image should be absolutely invisible to human eye to achieve a good stego image quality. It is observed that for Baboon and Football, the PSNR values are higher for DWT than for SWT but is the reverse for Lena and Flower. Thus we reach the conclusion that SWT performs better than DWT for lesser variation between cover image and secret image whereas DWT performs better for higher variation conditions.

REFERENCES

[1] Shilparani Noubade and Hemavathi.N.V, "*Private Confidential Data Hiding by Using Wavelet Approach"*, International Journal of Electronics & Communication Technology, Vol. 5, Issue 4, 2014.

[2] Patel Roshni, Aslam Durvesh and Patel Urvisha, "*Lossless Method for Data Hiding In Encrypted Image"*, International Conference on Innovations in Information Embedded and Communication Systems, 2015.

[3] Swapnali Zagade and Smita Bhosale, "*Secret data hiding by using DWT"*, International Journal of Engineering and Advanced Technology, 2014.

[4] Suchi Sharma and Uma kumara, "*High capacity data hiding technique using steganography"*, International journal of emerging trends and technology in computer science, 2013.

[5] Komal Hirachandani, Gaurav Soni and Rajesh Nigam, "*New Approach of Information Security through Steganography by using Wavelet Transformation and Symmetric Encryption*", International Journal of Computer Science and Information Technologies, Vol. 5, 2014.

[6] Kanzariya Nitin K., Nimavat Ashish V, *"Comparison of Various Images Steganography Techniques"*, International Journal of Computer Science and Management Research Vol 2, 2013.

APPENDIX

PROGRAM

Program code in DWT domain:

```
clc ;
clear all;
close all;
ck=imread('cameraman.tif'); %first cover data
i=imread('cameraman.tif');%second cover data
figure(1)
imshow(i);
sX=size(i);
[LL,LH,HL,HH]=dwt2(i,'db2');
HH9=HH;%saving HH band
[LL7,LH7,HL7,HH7]=dwt2(ck,'db2');
figure(1)
subplot(2,2,1);imshow(LL);title('LL band of image');
subplot(2,2,2);imshow(LH);title('LH band of image');
subplot(2,2,3);imshow(HL);title('HL band of image');
subplot(2,2,4);imshow(HH);title('HH band of image');
%%
figure(2)
himage=HH;
[m,n]=size(himage);
subplot(2,2,1);
imshow(himage);
himage=uint8(himage);
%%
choice = menu('CHOOSE','PIC');
if choice==1
si=imread('flower.jpg');
si=imresize(si,[m,n]);
[si2,map]=rgb2ind(si,200);
simage=ind2gray(si2,map);
simage=imresize(simage,[m,n]);
end
%%
simage=uint8(simage);
[m1,n1]=size(simage);
r1=rand(1,1);
r2=ceil((100*r1));
r=transpose(r2);
r=r2;
r=uint8(r);
r=16
for x=1:m1
    for y=1:n1
        v(x,y)=r;
    end
end
for x=1:m1
    for y=1:n1
z(x,y)=bitxor(simage(x,y),v(x,y));
    end
end
subplot(2,2,2);
imshow(z);
%%
%encryption
himage2=himage+z;
subplot(2,2,3);
```

```
imshow(himage2);
%%
X = idwt2(LL,LH,HL,himage2,'db2',sX);
X=imresize(X,[m,n]);
X=uint8(X);
HH7=uint8(HH7);
HH8=HH7+X;
HH11=HH8;
X = idwt2(LL,LH,HL,himage2,'db2',sX);
ckX = idwt2(LL7,LH7,HL7,HH8,'db2',sX);
ckX=imresize(ckX,[m,n]);
y=uint8(X);
y1=uint8(ckX);
figure(3)
imshow(y1);
%%
%decryption
[LL7,LH7,HL7,HH8]=dwt2(ckX,'db2');
HH8=imresize(HH8,[m,n]);
q1=uint8(HH9);
q2=uint8(HH8);
q3=q2-q1;
[LL5,LH5,HL5,HH5]=dwt2(X,'db2');
figure(5);
subplot(2,2,1);
imshow(q3);
q3=himage2;
q3=imresize(q3,[m1,n1]);
q=uint8(q3);
q1=uint8(HH9);
Hi=q-q1;
for x=1:m1
    for y=1:n1
z1(x,y)=bitxor(Hi(x,y),v(x,y));
    end
end
[X1, map] = gray2ind(z1,65536);
y1 = ind2rgb(X1,map);
subplot(2,2,2);
imshow(y1);
temp=(double(simage)-double(z1)).^2;
mse=sum(sum(temp),2)/(m*n);
PSNR = 10 * log10( m^2 / mse)
Message=sprintf('The MSE is %.2f.\nThe PSNR = %.2f',mse,PSNR);
msgbox(Message);
```

Program code in SWT domain:

```
clc ;
clear all;
close all;
ck=imread('cameraman.tif');%first cover data
i=imread('cameraman.tif');% second cover data
figure(1)
imshow(i);
sX=size(i);
[LL,LH,HL,HH]=swt2(i,1,'db2');
HH9=HH;%saving HH band
[LL7,LH7,HL7,HH7]=swt2(ck,1,'db2');
```

```
figure(2)
subplot(2,2,1);imshow(LL);title('LL band of image');
subplot(2,2,2);imshow(LH);title('LH band of image');
subplot(2,2,3);imshow(HL);title('HL band of image');
subplot(2,2,4);imshow(HH);title('HH band of image');
%%
figure(3)
himage=HH;
[m,n]=size(himage);
subplot(2,2,1);
imshow(himage);
himage=uint8(himage);
%%
choice = menu('CHOOSE','PIC');
if choice==1
si=imread('flower.jpg');
si=imresize(si,[m,n]);
[si2,map]=rgb2ind(si,200);
simage=ind2gray(si2,map);
simage=imresize(simage,[m,n]);
end
%%
simage=uint8(simage);
%r=rem(himage,2);
%himage1=himage-r;
%himage3=uint8(himage1);
[m1,n1]=size(simage);
r1=rand(1,1);
r2=ceil((100*r1));
r=transpose(r2);
r=r2;
r=16
r=uint8(r);
for x=1:m1
    for y=1:n1
        v(x,y)=r;
    end
end
for x=1:m1
    for y=1:n1
z(x,y)=bitxor(simage(x,y),v(x,y));
    end
end
subplot(2,2,2);
imshow(z);
%%
%encryption
himage2=himage+z;
subplot(2,2,3);
imshow(himage2);
%%
X = iswt2(LL,LH,HL,himage2,'db2');
X=imresize(X,[m,n]);
X=uint8(X);
HH7=uint8(HH7);
HH8=HH7+X;
HH11=HH8;
X = iswt2(LL,LH,HL,himage2,'db2');
ckX = iswt2(LL7,LH7,HL7,HH8,'db2');
ckX=imresize(ckX,[m,n]);
y=uint8(X);
```

```
y1=uint8(ckX);
figure(4)
imshow(y1);
%%
%decryption
[LL7,LH7,HL7,HH8]=swt2(ckX,1,'db2');
HH8=imresize(HH8,[m,n]);
q1=uint8(HH9);
q2=uint8(HH8);
q3=q2-q1;
[LL5,LH5,HL5,HH5]=swt2(X,1,'db2');
figure(5);
subplot(2,2,1);
imshow(q3);
q3=himage2;
q3=imresize(q3,[m1,n1]);
q=uint8(q3);
q1=uint8(HH9);
Hi=q-q1;
for x=1:m1
    for y=1:n1
z1(x,y)=bitxor(Hi(x,y),v(x,y));
    end
end
[X1, map] = gray2ind(z1,65536);
y1 = ind2rgb(X1,map);
subplot(2,2,2);
imshow(y1);
temp=(double(simage)-double(z1)).^2;
mse=sum(sum(temp),2)/(m*n);
PSNR = 10 * log10( 256^2 / mse)
Message=sprintf('The MSE is %.2f.\nThe PSNR = %.2f',mse,PSNR);
msgbox(Message);
```