

A Wavelet Based Audio Steganography System

A Thesis

Submitted to the College of Engineering
of Nahrian University in Partial Fulfillment
of the Requirements for the Degree of
Master of Science

In

Electronic and Communications Engineering/
Electronic Circuits and Systems

by

Riam Majeed Zaal

(B.Sc 2005)

**Rabie al auwal
March**

**1430
2009**

Certification

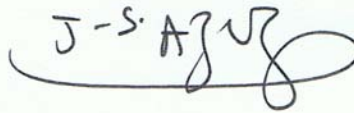
I certify that this thesis entitled “ **A Wavelet Based Audio Steganography System**” was prepared by **Riam Majeed Zaal** under my supervision at Nahrain University / College of Engineering in partial fulfillment of the requirements for the degree of **Master of Science in Electronic and Communications Engineering / Electronic Circuits and Systems**

Signature: 

Name: Dr. Rajaa aldeen A. Khalid

(Supervisor)

Date: 3/3/2009



Signature:

Name: Asst. Prof. Dr. Jabir S. Aziz

Head of Department

Date: 15/3/2009

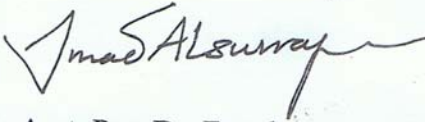
Certificate

We certify, as an examining committee, that we have read this thesis entitled "**A Wavelet Based Audio Steganography System**", examined the student **Riam Majeed Zaal** in its content and found it meets the standard of thesis for the degree of Master of Science in **Electronic and Communications Engineering / Electronic Circuits and Systems**.

Signature: 

Name : Dr. Rajaa aldeen A. Khalid
(Supervisor)

Date : 3/3/2009

Signature: 

Name : Asst. Pro. Dr. Emad
S. Ahmed (Member)

Date 3/3/2009

Signature: 

Name : Dr. Firas Abdullah
Thweny (Member)

Date : 3/3/2009

Signature: 

Name : Pro. Dr. Waleed A.
Mahmoud (Chairman)

Date : 15/3/2009

Approval of the College of Engineering

Signature: 

Name : Prof. Dr. Muhsin J. Jweeg
(Dean)

Date 29/3/2009

ABSTRACT

Steganography is the art of information hiding in ways that prevent its detection. A message in cipher text may raise suspicion, while an invisible message will not. Digital steganography uses a host data or message, known as a "container" or "cover" to hide another data or message called "secret" in it.

An Image in audio steganography system had been proposed in this thesis in order to embed a secret image data in audio data. One embedding method is implemented in the proposed system (Least Significant Bit in time domain, and transform domain Discrete Wavelet Transform).

The technique (Least Significant Bit) is implemented in time domain where the secret data is embedded directly in the cover data. This technique is implemented in frequency domain that results from using discrete wavelet transform; where the secret data are embedded in wavelet transform (WT) coefficients of cover data.

Most of the fidelity measures (Mean Square Error, Normalized Root Mean Square Error, Signal to Noise Ratio, Peak Signal to Noise Ratio and Correlation) obtained in the test has indicated good results for PSNR (187.28db) and MSE (0.214). The reconstructed data is exactly the same original data if the wavelet transform is used, while a small unrecognizable error may occur when the technique is used in time domain. MATLAB programming environment is used to simulate the entire system.

CONTENTS

ABSTRACT	i
Contents	ii
List of Abbreviations (alphabetic)	v
List of Symbols (alphabetic)	vi
List of Tables	vii
List of Figures	vii
	i
Chapter One :Overview	
1.1 Overview	1
1.2 information Hiding	2
1.3 information Hiding Techniques	2
1.3.1 Hiding in Text	2
1.3.2 Hiding in Disc Space	2
1.3.3 Hiding in Network Packets	3
1.3.4 Hiding in Software and Circuitry	3
1.3.5 Hiding in Image	4
1.3.6 Hiding in Video	4
1.3.7 Hiding in Audio	4
1.4 Information hiding Features and Applications	5
a) Features	5
b) Applications	6
1.5 Steganography	7
1.6 Steganography Advantages and Disadvantages	7
a) Advantage	7
b) Disadvantages	8
1.7 Literature Survey	9
1.8 The Aim of the Work	11
1.9 Thesis Layout	12
Chapter Two: Theoretical Considerations	
2.1 Introduction	13
2.2 Steganography	13
2.3 Steganography Uses	15
2.4 Data-Hiding in Audio	15
a) Least Significant Bit Insertion	16

b) Phase Coding	17
c) Spread Spectrum Coding	18
d) Echo Data Hiding	18
2.5 Digital Sound Representation	19
2.6 Transform Domain Techniques	21
2.7 Wavelet Transform	22
2.8 The Continuous Wavelet Transform and the Wavelet Series	24
2.9 The Discrete Wavelet Transform	25
2.10 DWT and Filter Bank	26
2.10.1 Multi-Resolution Analysis using Filter Banks	26
2.11. Daubechies Wavelets:dbN	28
2.12 Why Wavelet Analysis Effective	30
Chapter Three: System Design and Implementation	
3.1 Introduction	32
3.2 The Overall System Model	32
3.3 The Proposed Stego system	34
3.3.1 Embedding in Time Domain	34
3.3.2 The Extracting Algorithm	38
3.3.3 Embedding in Transform Domain	40
3.3.4 The Extracting Algorithm	45
3.4 Fidelity Measures	47
Chapter Four : Experimental Results and System Evaluation	
4.1 Introduction	52
4.2 Test on Hiding Methods	52
4.2.1 Test on Hiding in the Time domain, and DWT using LSB method	55
Chapter Five : Conclusions and Suggestions for Future Work	
5.1 Conclusion	69
5.2 Suggestions for Future Work	70
REFERENCES	71
Appendix A.1	
Appendix A.2	
Appendix A.3	

List of Abbreviations

DSP	Digital Signal Processing
FFT	Fast Fourier Transform
DVD	Digital Versatile Disk
HAS	Human Auditory System
A/D	Analog to Digital
DSSS	Direct Sequence Spread Spectrum
LSB	Least Significant Bit
PCM	Pulse Code Modulation
STFT	Short Time Fourier Transform
WT	Wavelet Transform
CWT	Continuous Wavelet Transform
DWT	Discrete Wavelet Transform
DHWT	Discrete Haar Wavelet Transform
ASCII	American Standard Code for Information Interchange
WAV	Window Audio Visual
SNR	Signal to Noise Ratio
PSNR	Peak Signal to Noise Ratio
NRMSE	Normalized Root Mean Square Error
JPEG	Joint Photography Expert Group
MSE	Mean Square Error
DbN	N-th order duabechies Filter

List of Symbols

$C(u)$	Discrete Cosine Transform
$F(x)$	Inverse discrete Cosine Transform
T	Translation Parameter
S	Scale Parameter
$\psi(t)$	Time domain wavelet function
Ψ	Called the mother wavelet
$\phi(t)$	Time domain scaling function
X	Original audio signal
H°	High pass filter
G°	Low pass filter
ω	Analog radian frequency
t	Continuous time variabl

List of Tables

Table	Page
	53
4.1 The test sample applied to the system	
4.2 Test Results for hiding of the sample " song1 wave" Framing 16-bit	55
4.3 Test Results for hiding of the sample "song2 wave" Framing 16-bit	56
4.4 Test Results for hiding of the sample " song3 wave" Framing 16-bit	57
4.5 Test Results for hiding of the sample " song4 wave" Framing 16-bit	58
4.6 Test Results for hiding of the sample " song5 wave" Framing 16-bit	59
4.7 Test Results for hiding of the sample "song6 wave" Framing 16-bit	60
4.7 Test Results for hiding of the sample "song6 wave" Framing 16-bit	61
4.9 Test Results for hiding of the sample "song8 wave" Framing 16-bit	62
4.10 Test Results for hiding of the sample "song9 wave" Framing 16-bit	63
4.11 Test Results for hiding of the sample "song10 wave" Framing 16-bit	64

List of Figures

Figure	Page
Figure (2.1) Steganography Model	14
Figure (2.2) the classification of covers	20
Figure (2.3) PCM for the computer programmer	21
Figure (2.4) Time-Frequency resolution of STFT	23
Figure (2.5) Time-frequency resolution of WT	23
Figure (2.6) Three-level wavelet decomposition tree	26
Figure (2.7) Three-level wavelet reconstruction tree	27
Figure (2.8) Daubechies Wavelet db4 on the Left and db8 on the Right	28
Figure (2.9) Haar Wavelet	29
Figure (2.10) Haar Scaling Function	30
Figure (3.1) the Overall System Model	33
Figure (3.2) Block Diagram of Time Domain Embedding Technique	34
Figure (3.3) Original secret image	36
Figure (3.4) Gray scale of image	36
Figure (3.5) Block Diagram of Time Domain Extracting Technique	39
Figure (3.6) Block Diagram of Transform Domain Embedding Technique	41
Figure (3.7) Block Diagram of Transform Domain Extracting Technique	46
Figure (3.8) the embedding LSB system flowchart	50
Figure (3.9) the embedding wavelet system flowchart	51
Figure (4.1) Image Used as a secret message	54
Figure (4.2) Signal to Noise Ratio when using Song Cover with size 169K	67
Figure (4.3) Mean Square Error when using Song cover with size 169KB	67
Figure (4.4) Signal to Noise Ratio when using Song cover with size 1.4MB	68
Figure (4.5) Mean Square Error when using Song cover with size 1.4MB	68

Chapter One

INTRODUCTION

1.1 Overview

Digital multimedia communication is of the essence to the Internet. In numerous applications it is required that communication be private or secure. The two most common methods for secure communication are cryptography and steganography [1]. In cryptography the secure message (of any media format) is encrypted, while in steganography the message or payload is hidden, on an imperceptible manner, in a "carrier" media. Steganography is an alternative to cryptography because of the ease to develop customized steganographic systems and appeal that, unlike cryptography, the secure of communication is not apparent to any third party [2]. In the study of communications security, cryptography techniques have received more attention from the research community and from industry than information hiding, but in the recent years a rapid growth of this discipline is seen [3]. The reasons for this growth are:

1. The availability of multimedia content in digital form so that digital image as well as audio and video files a rich environment for hiding unlimited types of data.
2. Senses/perceptions of human being are not acute enough to distinguish minor changes.

1.2 Information Hiding

Information hiding, in general is covering sensitive information within normal information, this creates a hidden communication channel between sender and receiver such that the existence of channel is unnoticeable. The main goal of information hiding is to send message without creating suspicion.

One of the more interesting parts of information hiding is steganography, different from cryptography that is about protecting the contents of message, steganography is a concealing its existence [4].

1.3 Information Hiding Techniques

There is several information hiding techniques that should be classified according to the media where the information is hidden.

1.3.1 Hiding in Text

Documents may be modified to hide information by manipulating of lines and words. HTML files can be used to carry information since adding spaces, tabs, "invisible" characters, and extra lines breaks are ignored by web browsers. The "extra" spaces and lines are not perceptible until revealing the source of the web page. There are many methods for hiding information in text such as line-shift coding, word shift coding ...etc [5].

1.3.2 Hiding in Disc Space

Another way to hide information relies on finding unused space is that not reading apparent to an observer. Taking advantage of unused space or reversed space to hold covert information provides a mean of hiding information without

perceptually degrading the carrier. The way operating system stores files typically results in unused space that appears to be allocated to files. Another method of hiding information in the file system is to create hidden partition. These partitions are not seen if the system is started normally [5].

1.3.3 Hiding in Network Packets

Various network protocols characteristics can be used to hide information. TCP/IP packets are used to transport information and an uncountable number of packets are transmitted daily over the Internet. Any of these packets can provide covert communication channel. The headers have unused space or other values that can be manipulated to hide information. The areas encoded in the packet can be:

1. The IP packet identification field.
2. The TCP initial sequence number field.
3. The TCP acknowledged sequence number field.

The fields are replaced with numerical ASCII representation of the characters to be encoded. These fields are less likely to be distorted due to the network routing or filtering [5].

1.3.4 Hiding in Software and Circuitry

Data can also be hidden based on the physical arrangement of a carrier. The arrangement itself may be an embedded signature that is unique to creator. An example of this is in the layout of code distributed in a program and the layout of electronic circuits on a board. This type of 'marking" can be used to uniquely identify the design origin and cannot be removed without significant change to the network [5].

1.3.5 Hiding in Image

Digital image is likely candidate for information hiding. There are many attributes of human vision system (HVS) that are potential candidates for exploitation in an information hiding system, including our varying sensitivity to contrast as a function of spatial frequency and the masking effect of the edges (both in luminance and chrominance). The HVS has low sensitivity to small changes in luminance, being able to perceive change of no less than one part in 30 for random patterns. Another HVS "hole" is our relative insensitivity to very low spatial frequencies such as continuous changes in brightness across an image. Additional advantage of working with images is that they are non-casual data hiding techniques can have access to any pixel or block of whid at random [6].

1.3.6 Hiding in Video

Video files are generally a collection of images and sounds, so most of the presented techniques on images and audio can be applied to video files too. The two advantages of video are: the large amount of data can be hidden inside each frame, and the video is a moving stream of images and sounds, therefore any small but otherwise noticeable distortions might be unobserved by humans because of the continuous of the continuous flow of the information [7].

1.3.7 Hiding in Audio

Data hiding in audio is especially challenging because Human Auditory system (HAS) perceives over a range of power greater than one billion to one and rang of frequencies greater than one thousand to one [6].

1.4 Information hiding Features and Applications

a) Features

Data-hiding techniques should be capable of embedding data in a host signal with the following restrictions and features:

1. The host signal should be nonobjectionally degraded and the embedded data should be minimally perceptible. (The goal is for data to remain *hidden*. We will use the words *hidden*, inaudible, imperceivable, and invisible to mean that an observer does not notice the presence of the data, even if they are perceptible.)
2. The embedded data should be directly encoded into the media, rather than into a header or wrapper, so that the data remain intact across varying data file formats.
3. The embedded data should be immune to modifications ranging from intentional and intelligent attempts at removal to anticipated manipulations, e.g., channel noise, filtering, resampling, cropping, encoding, lossy compressing, printing and scanning, digital-to-analog (D/A) conversion, and analog-to-digital (A/D) conversion.
4. Asymmetrical coding of the embedded data is desirable, since the purpose of data hiding is to keep the data in the host signal, but not necessarily to make the data difficult to access.
5. Error correction coding may be used to ensure data integrity. It is inevitable that there will be some degradation to the embedded data when the host signal is modified.
6. The embedded data should be self-clocking or arbitrarily re-entrant. This ensures that the embedded data can be recovered, when only fragments of

the host signal are available, e.g., if sound bits are extracted from an interview, data embedded in the audio segment can be recovered. This feature also facilitates automatic decoding of the hidden data, since there is no need to refer to the original host signal (this feature is vital in watermarking) [8].

b) Applications

Trade-off exists between the quantity of embedded data and the degree of immunity to host signal modification. By constraining the degree of host signal degradation, a data-hiding method can operate with either high-embedded data rate, or high resistance to modification, but not both. As one increases, the other must decrease. While this can be shown mathematically for some data-hiding systems such as a spread spectrum, it seems to hold true for all data-hiding systems. In any system, one can trade bandwidth for robustness by exploiting redundancy.

The quantity of embedded data and the degree of host signal modification vary from application to application. Consequently, different techniques are employed for different applications. Several prospective applications of data hiding are discussed in this section.

An application that requires a minimal amount of embedded data is the placement of digital watermark. The embedded data are used to place an indication of ownership in the host signal, serving the same purpose as an author's signature or a company logo.

A second application for data hiding is tamper-proofing; it is used to indicate that the host signal has been modified from its authored state.

Modification to the embedded data indicates that the host signal has been change in some way.

A third application, feature location, requires more data to be embedded. In this application, the embedded data are hidden in specific locations within an image. It enables one to identify individual content features, e.g., the name of the person on the left versus the right side of an image. Typically, feature location data are not subject to intentional removal. However, it is expected that the host signal might be subjected to a certain degree of modification, e.g., images are routinely modified by scaling, cropping, and tone scale enhancement. As a result, feature location data hiding techniques must be immune to geometrical and no geometrical modifications of a host signal [8].

1.5 Steganography

Steganography is the art and science of communication in a way which hides the existence of communication.

The word steganography literally means covered writing as derived from Greek. It includes a vast array of methods of secret communication that conceal the very existence of the message. Among, these are invisible inks, covert channel and spread-spectrum communication [5].

1.6 Steganography Advantages and Disadvantages

a. Advantage

The advantage of using steganography is to hide information, such that the transmission of messages is transparent to any given viewer. Messages can be hidden in different formats that are undetectable and un-readable to the human

eye. Steganographic technologies are very important in Internet privacy today. With the use of steganography and encryption, corporation, governments, and law enforcement agencies can communicate secretly.

Encryption protects data that can be detected; the only thing missing is the secret key for decryption. Steganography is harder to detect under traditional traffic pattern analysis, while steganography enhances the privacy of personal communication. Since encryption can be detected and some governments prohibit the use of encryption, steganography can be used to supplement encryption. Additional layers of security are of benefit to secrecy. If a steganographic message is detected, there is still the need for the encryption key.

The method of encrypting a message and then using steganography is most widely used by steganographers. [15,9]

b. Disadvantages

One of the biggest disadvantages is that quite frequently the size of a secret message is usually larger than the original cover. There can be color changes, or detectable sound changes, they are evident, especially if well-known images or audios are chosen as the steganographic cover. Another issue to mention, text messages are limited in size for the hiding of data, they need redundant data to replace a secret message. Changing the type of the format or replacing the readable text can alter text messages.

Through the use of the new technology, some Internet firewalls can detect steganographic messages. As this technology evolves, detecting steganographic messages can be considered as a drawback because an important message may be deleted or quarantined, and this message may be the one that will save a country. [9]

1.7 Literature Survey

A lot of research work has been conducted by several researchers concerned with developing information hiding techniques, whose reports have been published. These researchers tried to insert new additional features to increase the system robustness and invisibility; some of these are summarized below:

- In 2008, V. Vijaya Kumar, U.S.Raju, proposed a system for "Wavelet based Texture Segmentation methods based on Combinatorial of Morphological and Statistical Operations" This research divides the wavelet combinatorial segmentation algorithm into three groups based on number of operations and type of operations, used. The present method using wavelet transforms is applied on Brodatz textures and a good segmentation is resulted.
- In 2007, Mohammad Pooyan, Ahmad Delforouzi, proposed a system for "LSB-based Audio Steganography Method Based on Lifting Wavelet Transform", this research presents a novel method for digital audio steganography where encrypted covert data is embedded into the wavelet coefficients of host audio signal. To avoid extraction error the searcher uses lifting wavelet transform. For using the maximum capacity of audio signals, we calculate hearing threshold in wavelet domain. Then according to this threshold data bits are embedded in the least significant bits of lifting wavelet coefficients. Inverse lifting wavelet transform is applied to modified coefficients to construct stego signal in time domain. Experimental results show that proposed method has large payload, high audio quality and full recovery.

- In 2003, Jianyun Xu, Andrew H. Sung, Peipei Shi, Qingzhong Liu, proposed a system for "Text steganography using wavelet transform" This research involves an algorithm to limit errors in lossy transforms to achieve high capacity text hiding in image files using Discrete Haar Wavelet Transform (DHWT). It also discusses robust text steganography using multiple-level lossless DHWT. Experimental results validated the method for high capacity plain text hiding, and demonstrated that lossless recovery of the hidden text from JPEG images with compression rate as high as 67% is possible [12].
- In 2003, Yasmeen I. Dieab proposed a system to embed a digital watermark in audio signal, while retaining perceptual to the listener. The system uses two techniques: Low Bit Encoding in time domain and the human auditory characteristics in frequency domain. In the frequency domain method, the Fast Fourier Transform (FFT) with segmentation is used to embed the watermarks. The imperceptibility of the watermarking is measured by using the PSNR metrics, It has been proven that it has a good quality (PSNR=40db) [13].

1.8 The Aim of the Work

The aim of this work is developing and implementing a system for embedding information, whether they are audio, text, image or video, into audio files by using Least Significant Bit steganography technique and implementing in special domain and frequency domain using (Discrete Wavelet Transform) by using Matlab. The algorithms would be tested on audio files with quantization levels and sampling frequencies ranging from 8 kHz to 44.1 kHz.

1.9 Thesis Layout

This thesis is organized in five chapters. The contents of these chapters are:

- Chapter Two includes the concept of steganography, methods of information hiding in spatial domain and transform domain (Discrete Wavelet Transform) using Least Significant Bit Technique.
- Chapter Three is dedicated to present the layout of proposed system, and all ideas and algorithms used for hiding operations.
- Chapter Four contains the results of comprehensive tests performed on the proposed system using different test samples.
- Chapter Five is dedicated to introduce some conclusions that are derived from the test results, also some new ideas that can be added to the suggested system as future work, are given in this chapter.

Chapter Two

Theoretical Considerations

2.1 Introduction

This chapter is concerned with the main fundamental concepts needed to understand the ideas applied in the proposed hiding system. In fact, the main concepts were covered, they are: Information Hiding Techniques, Wavelet Transform. Data compression and fidelity measures were also explained

2.2 Steganography

Steganography encompasses methods of transmitting secret messages in such a manner that the existence of the embedded messages is undetectable. Carriers of such message may resemble innocent sounding text, disks and storage device, network traffic and protocols, the way software or circuits are arranged, [audio, images, video, or any other digitally represented code or transmission]. Figure (2.1) provides an illustration of a Steganographic model or process. Together, the cover carrier and the embedded message create a stego-carrier [14].

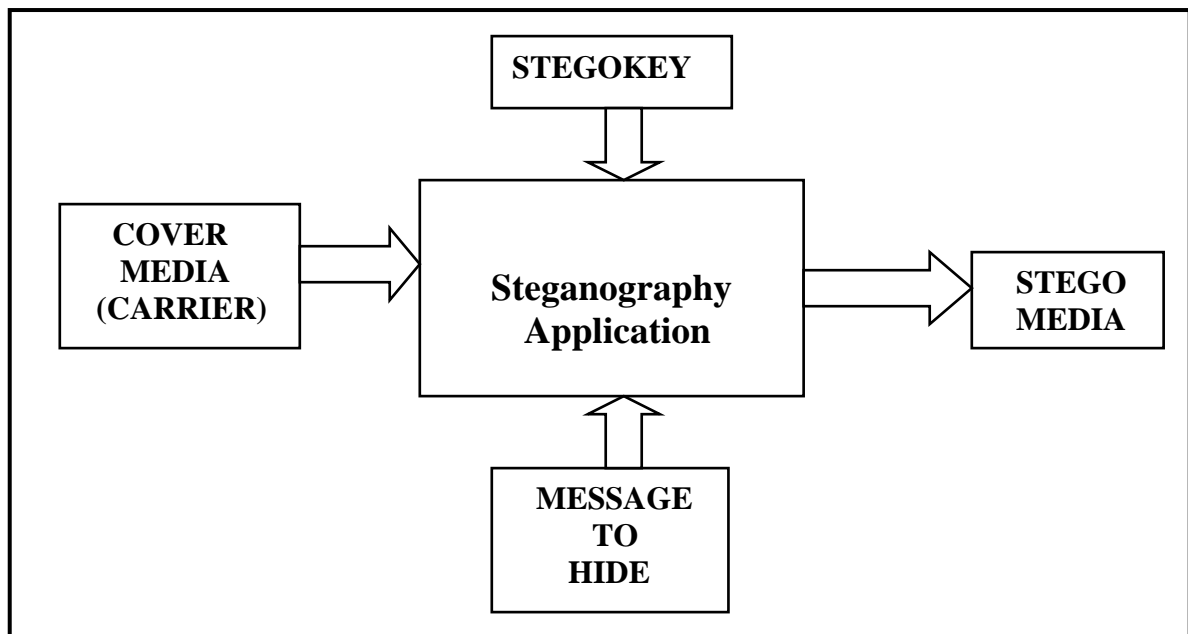


Figure (2.1) Steganography Model

Where:

- Cover media carrier: The cover data in which embedded message will be hidden.
- Message: The message to embed.
- Steganography application: It is the process that is done from sender to hide the secret image in the cover image.
- Stego media: Cover data embed message.
- Stegokey: It is the data that is needed for embedding and reconstruction. Hiding information may require a stegokey or password that is additional secret information and may be used to select cover regions to hide or even encrypt the embedded message.

2.3 Steganography Uses

The use of steganography undeniably means of dishonest activity, but there is a peaceful aspect to consider. Steganography is used in map making, where cartographers add a nonexistent street or lake in order to detect copyright offenders. Or similarly, fictional names are added to mailing lists to catch unauthorized resellers. Modern techniques use steganography as a watermark to inject encrypted copyright marks and serial numbers into electronic media such as books, audio, and video. For example, DVD recorders detect copy protection on DVDs that contain embedded authorizations.

Potential uses of steganography are undoubtedly vast. Companies could advertise public Web pages containing private, hidden text that only internal members could intercept. An attempt to decipher the hidden text would be unwarranted since no encryption (or code) was used. Steganography could also be used to hide the existence of sensitive files on storage media. This would entail a cover folder and an embedded hidden folder [15].

2.4 Data-Hiding in Audio

Audio files can also be used to hide information. Steganography is often used to copyright audio files to protect the rights of music artists. Techniques such as least significant bit insertion, phase coding, spread spectrum coding, and echo hiding can be used to protect the content of audio files. The biggest challenge that faces all these methods is the sensitivity of the human auditory

system or HAS [16]. Because the HAS is so sensitive, people can often pick up randomly added noise making it hard to successfully hide data within audio data. To fully understand the different techniques of hiding data information in audio data, transmission of audio signals must first be understood. When working in audio the transmission medium must always be considered.

The transmission medium of an audio signal refers to the environment in which a signal might go through to reach its destination. Bender and his colleagues categorize the possible transmission environment into the four following groups [17]:

1. Digital end-to-end environment, where the sound files are copied directly from one machine to another.
2. Increased/decreased resampling environment, where the signal is resampled to a higher or lower sampling rate.
3. Analog transmission and resampling, where a signal is converted to an analog state, played on a clean analog line, and resampled.
4. "Over the air" environment, where the signal is played into the air, passed through a microphone.

By understanding the different media in which audio signals may travel, the appropriate technique for embedding data in audio files can be determined.

The most commonly used methods for hiding data in audio media are the following methods:

a) Least Significant Bit Insertion

Like image files, the least significant bit insertion method can also be used to store data in the least significant bit of audio files. However, like image files,

by using this method, the hidden data can be easily destroyed and detected. Resampling and channel noise may alter the hidden data, while changing the least significant bit may introduce audible noise [17]. Information may also be destroyed through compression, cropping, or A/D, D/A conversion [18]. Although this technique is simple to perform, its lack of dependability makes other methods more appealing.

b) Phase Coding

It is another technique used to hide data in audio files. This is done by substituting the phase of an initial audio segment with a reference phase that represents the data. The phase of the following segments is adjusted accordingly to preserve the relative phase between segments [18]. The steps to phase coding are as follows [16]:

1. The original sound sequence is broken into a series of S_n short segments.
2. A discrete Fourier transform is applied to each segment.
3. The phase difference between each adjacent segment is calculated.
4. For segment S_0 the first segment, an artificial absolute phase P_0 is created.
5. For all other segments, new phase frames are created.
6. The new phase and original magnitude are combined to get a new segment, S_n
7. The new segment is concatenated to create the encoded output.

To enable the receiver to decode the hidden data, one must know the length of the segments, the discrete Fourier transform points, and the intervals in

which the data are hidden. Phase coding is one of the most effective schemes in terms of the signal-to-perceived noise ratio because listeners often do not hear a difference in the altered audio file when the phase shift is smooth [18].

c) Spread Spectrum Coding

Spread spectrum coding can also be used to hide data in audio files. Usually when audio files travel through communication channels, the channels try to concentrate audio data through narrow regions of the frequency spectrum in order to conserve bandwidth and power [17]. However, this technique requires the embedded data to be spread across the frequency spectrum as much as possible. Unlike the LSB insertion, spread spectrum coding uses the entire spectrum of the file to embed data [19]. Many methods can be used to spread the embedded data over the frequency spectrum. Direct Sequence Spread Spectrum (DSSS) encoding spreads the signal by multiplying it by a certain maximal length pseudorandom sequence called chip [17]. Unfortunately, like the LSB method, DSSS may add random noise that the listener can detect. For frequency hopped spread spectrum encoding, the original audio signal is divided into small pieces and each piece is carried by a unique frequency [18]. The main advantage of using spread spectrum coding is its resistance to modification. Because the embedded data is spread throughout the cover data, it would be difficult to modify the embedded data without causing noticeable harm to the cover data.

d) Echo Data Hiding

Echo data hiding hides data in a host signal by introducing an echo. The embedded data is hidden by varying three parameters of the echo: initial

amplitude, decay rate, and delay. As the timing between the original signal and echo decreases, the two signals may blend, making it hard for the human ear to distinguish between the two signals. The value of the hidden data corresponds to the time delay of the echo and its amplitude. By using different time delays between the original signal and the echo to represent binary one or zero, data can be embedded into the audio file. To embed more than one bit, the original signal is divided into smaller segments and each segment can then be echoed to embed the desired bit. The final cover data consists of the reconstruction of all the independently encoded segments [16]. Echo hiding works particularly well with high quality audio files. Audio files with no additional degradation and no gaps of silence are preferred when using this technique [17].

2.5 Digital Sound Representation

When developing a data hiding method on sound waves, like speech or music, the first consideration is how sound is represented digitally. Audio refers to the sound within the human hearing range (20 Hz to 20 KHz). An audio signal in nature is analog, analog sounds are waves detected by human ears. These waves are continuous in both time and amplitude which represents the height or (volumes), of the sound [21]. The analog signal should be converted to digital form to be stored and processed by computers and transmitted through computer networks.

An A/D (analog to digital) conversion consists of two steps: sampling and quantization.

1. Sampling: Sampling or approximating involves periodically measuring the analog signal and use these measurements (samples) instead of the original signal; a sampled wave is shown in figure (2.2)

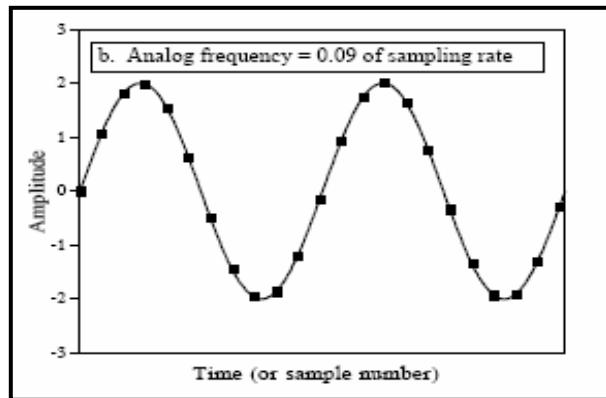


Figure (2.2) Sampled wave

Usually samples are stored as binary numbers, but they can be stored in other ways. A very well known way is to represent each sample by a series of pulses that represent its binary code; such representation is called Pulse Code Modulation (PCM).

There are various modulation types, but PCM is the widely used in digital audio. For a programmer, various modulation techniques are irrelevant. In a computer's memory, the successive binary values are simply stored as numbers. For most programmers PCM can be thought of as that shown in figure (2.3) [20, 22].

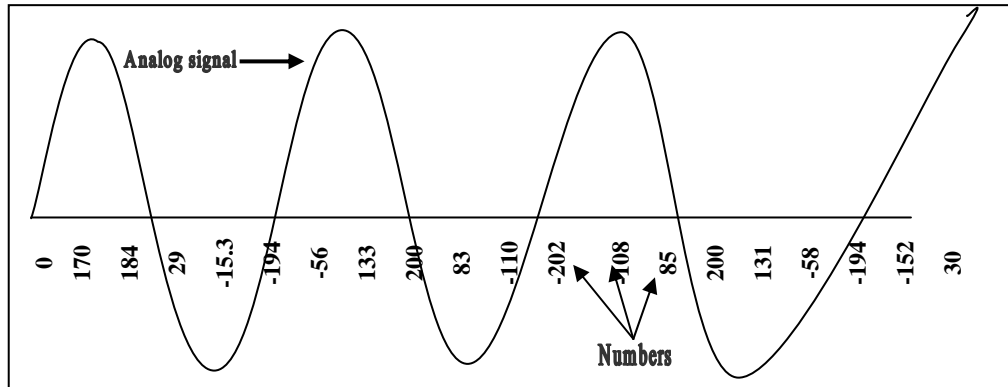


Figure (2.3) PCM for the computer programmer

2. Quantization: to quantize a signal means to determine the signal's value to some degree of accuracy. Because the finiteness of computer ability, the digital representation is also finite. For example if an 8-bit or 16-bit integers are used, either 256 or 65,536 discrete integer sample value can be obtained, but the original samples are not integers. The process of routing the exact sample value to less-precise value is referred to as quantization [23].

2.6 Transform Domain Techniques

We have seen that LSB modification techniques are easy ways to embed information, but they are highly vulnerable to even small cover modifications. An attacker can simply apply signal processing techniques in order to destroy the secret information entirely. In many cases even the small changes resulting out of lossy compression system yield total information loss. It has been noted early in the development of steganographic system that embedding information in the frequency domain of a signal can be much more robust than embedding rules

operating in the time domain. Most robust steganographic systems known today actually operate in some sort of transform domain [16].

The discrete form of these transforms is created by sampling the continuous form of the functions depending on the basis functions [24]. In many cases the inverse transform equation is the same as the forward ones, but possibly weighted by a constant. The next section represents some examples for this type of transformation.

2.7 Wavelet Transform

Fourier transform is based on spectral analysis; it is the dominant analytical tool for frequency domain analysis. However, Fourier transform can not provide any information about the spectrum changes with respect to time. Fourier transform assumes the signal stationary, but real signals are always non-stationary. To overcome this deficiency, a modified method (called short time Fourier transform) allows to represent the signal in both time and frequency domain time windowing function [25]. The window length determines a constant time and frequency resolution, as shown in Figure (2.4). Thus, a shorter time windowing is used in order to capture the transient behavior of a signal; we sacrifice the frequency resolution.

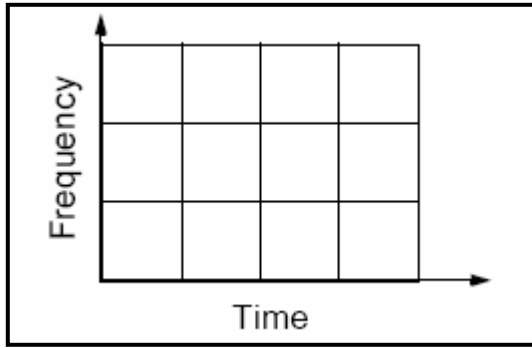


Figure (2.4) Time-Frequency resolution of STFT

The nature of the real signal is nonperiodic and transient (such as sound, image and video signals); such signals cannot easily be analyzed by conventional transform. So, an alternative mathematical tool- wavelet transform must be selected to extract the relevant time-amplitude information from a signal [26].

Wavelets cut up data into different frequency components, and then analyze each component with a resolution matched to its scale, instead of fixing the time and the frequency, as shown in Figure (2.5).

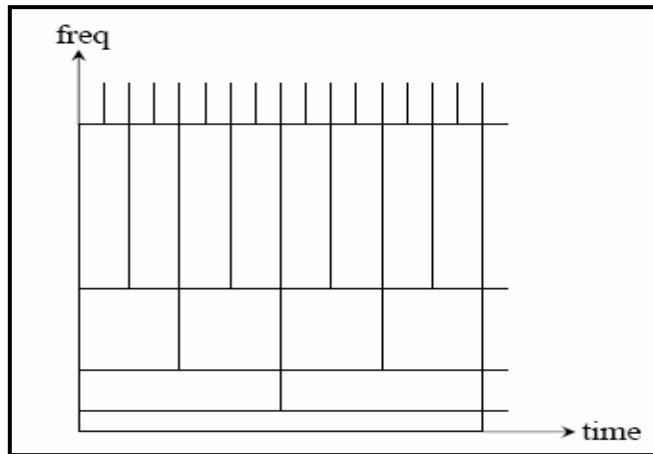


Figure (2.5) Time- Frequency resolution of WT

2.8 The Continuous Wavelet Transform and the Wavelet Series

The Continuous Wavelet Transform (CWT) is expressed by equation 2.6, where $x(t)$ is the signal to be analyzed. $\psi(t)$ is the mother wavelet or the basis function. All the wavelet functions used in the transformation are derived from the mother wavelet through translation (shifting) and scaling (dilation or compression).

$$cwt_x^\psi(T,S) = \psi_s^\psi(T,S) = \frac{1}{\sqrt{|S|}} \int x(t) \psi^* \left(\frac{t-T}{S} \right) dt \dots\dots\dots (2.1)$$

The mother wavelet used to generate all the basis functions is designed, based on some desired characteristics associated with that function. The translation parameter T relates to the location of the wavelet function as it is shifted through the signal. Thus, it corresponds to the time information in the Wavelet Transform. The scale parameter S is defined as $|1/\text{frequency}|$ and corresponds to frequency information. Scaling either dilates (expands) or compresses a signal. Large scales (low frequencies) dilate the signal and provide detailed information hidden in the signal, while small scales (high frequencies) compress the signal and provide global information about the signal. Notice that the Wavelet Transform merely performs the convolution operation of the signal and the basis function. The above analysis becomes very useful as in most practical applications, high frequencies (low scales) do not last for a long duration, but instead, appear as short bursts, while low frequencies (high scales) usually last for entire duration of the signal.

The Wavelet Series is obtained by discretizing CWT. This aids in computation of CWT using computers and is obtained by sampling the time-scale plane. The sampling rate can be changed accordingly with scale change

without violating the Nyquist criterion. Nyquist criterion states that, the minimum sampling rate that allows reconstruction of the original signal is 2ω radians, where ω is the highest frequency in the signal. Therefore, as the scale goes higher (lower frequencies), the sampling rate can be decreased thus reducing the number of computations. [27]

2.9 The Discrete Wavelet Transform

The Wavelet Series is just a sampled version of CWT and its computation may consume significant amount of time and resources, depending on the resolution required. The Discrete Wavelet Transform (DWT), which is based on sub-band coding, is found to yield a fast computation of Wavelet Transform. It is easy to implement and reduces the computation time and resources required.

The foundations of DWT go back to 1976 when techniques to decompose discrete time signals were devised. Similar work was done in speech signal coding which was named as sub-band coding. In 1983, a technique similar to sub-band coding was developed which was named pyramidal coding. Later many improvements were made to these coding schemes which resulted in efficient multi-resolution analysis schemes.

In CWT, the signals are analyzed using a set of basis functions which relate to each other by simple scaling and translation. In the case of DWT, a time-scale representation of the digital signal is obtained using digital filtering techniques. The signal to be analyzed is passed through filters with different cutoff frequencies at different scales. [28]

2.10 DWT and Filter Banks

2.10.1 Multi-Resolution Analysis using Filter Banks

Filters are one of the most widely used signal processing functions. Wavelets can be realized by iteration of filters with rescaling. The resolution of the signal, which is a measure of the amount of detail information in the signal, is determined by the filtering operations, and the scale is determined by upsampling and downsampling (subsampling) operations [28].

The DWT is computed by successive lowpass and highpass filtering of the discrete time-domain signal as shown in figure (2.6). This is called the Mallat algorithm or Mallat-tree decomposition. Its significance is in the manner it connects the continuous-time multiresolution to discrete-time filters. In the figure, the signal is denoted by the sequence $x[n]$, where n is an integer. The low pass filter is denoted by G_0 while the high pass filter is denoted by H_0 . At each level, the high pass filter produces detailed information; $d[n]$, while the low pass filter associated with scaling function produces coarse approximations, $a[n]$.

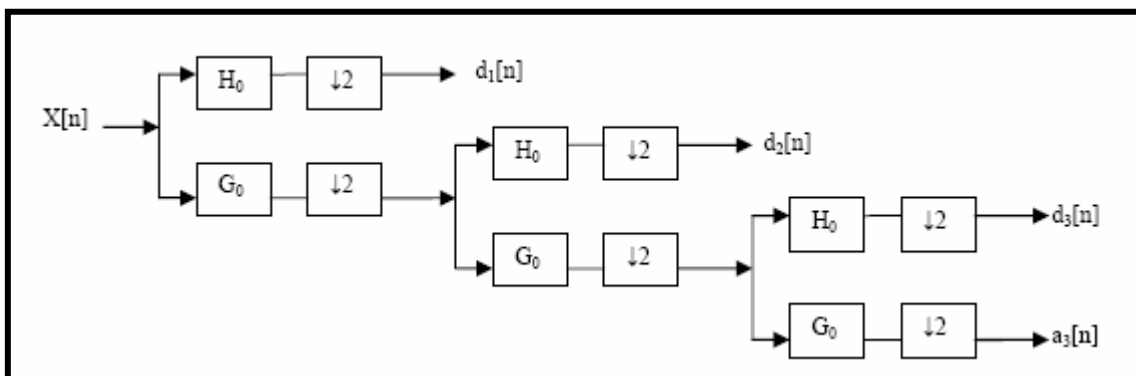


Figure (2.6) Three-level wavelet decomposition tree

At each decomposition level, the half band filters produce signals spanning only half the frequency band. This doubles the frequency resolution as the uncertainty in frequency is reduced by half. In accordance with Nyquist’s rule if the original signal has a highest frequency of ω , which requires a sampling frequency of 2ω radians, then it now has a highest frequency of $\omega/2$ radians. It can now be sampled at a frequency of ω radians thus discarding half the samples with no loss of information. This decimation by 2 halves the time resolution as the entire signal is now represented by only half the number of samples. Thus, while the half band low pass filtering removes half of the frequencies and thus halves the resolution, the decimation by 2 doubles the scale.

With this approach, the time resolution becomes arbitrarily good at high frequencies, while the frequency resolution becomes arbitrarily good at low frequencies. The filtering and decimation process is continued until the desired level is reached. The maximum number of levels depends on the length of the signal. The DWT of the original signal is then obtained by concatenating all the coefficients, $a[n]$ and $d[n]$, starting from the last level of decomposition.

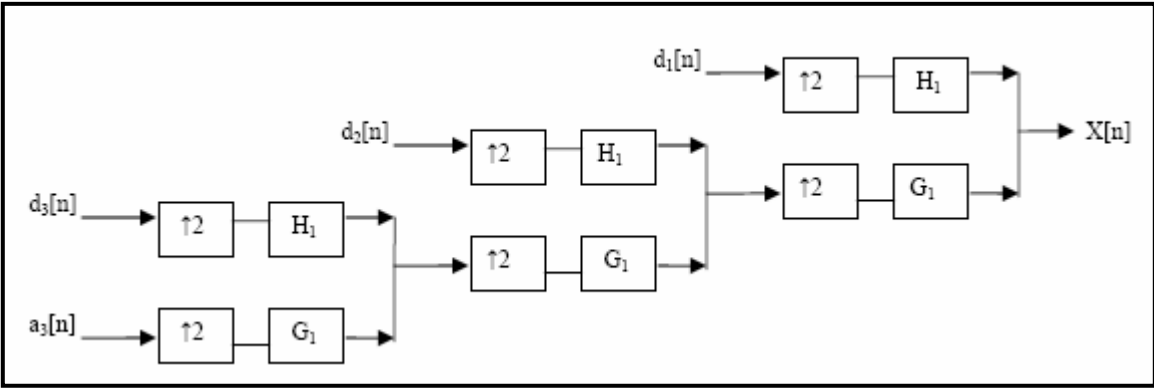


Figure (2.7) Three-level wavelet reconstruction tree

Figure (2.7) shows the reconstruction of the original signal from the wavelet coefficients. Basically, the reconstruction is the reverse process of decomposition. The approximation and detail coefficients at every level are upsampled by two, passed through the low pass and high pass synthesis filters and then added. This process is continued through the same number of levels as in the decomposition process to obtain the original signal. The Mallat algorithm works equally well if the analysis filters, G_0 and H_0 , are exchanged with the synthesis filters, G_1 and H_1 . [29]

2.11. Daubechies Wavelets: dbN

In dbN, N is the order.

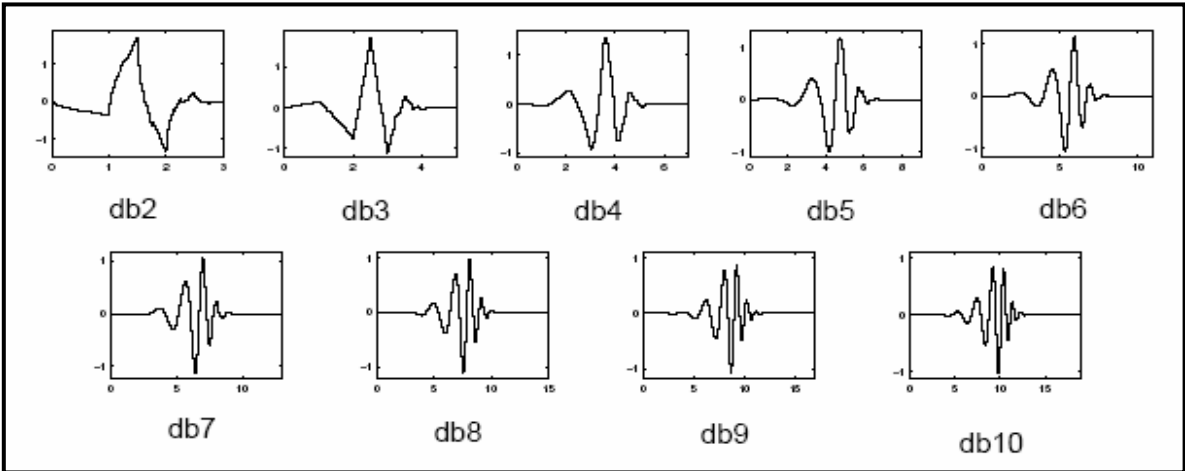


Figure (2.8) Daubechies Wavelets db4 on the Left and db8 on the Right [30]

This family includes the Haar wavelet, written db1, the simplest wavelet imaginable and certainly the earliest. These are compactly supported wavelets

with extreme phase and highest number of vanishing moments for a given support width. Associated scaling filters are minimum-phase filters. They are orthogonal, biorthogonal, provide compact support. Examples are db1 or haar, db4. Number of vanishing moments is N. These wavelets have no explicit expression except for db1, which is the Haar wavelet. However, the square modulus of the transfer function of h is explicit and fairly simple.

The support length of ψ and ϕ is $2N-1$. Most dbN are not symmetrical.

Haar

$\Psi(t)$ the wavelet function and $\phi(t)$ the scaling function are expressed as follows.

$$\psi(t) = \begin{cases} 1 & 0 \leq t < \frac{1}{2}, \\ -1 & \frac{1}{2} \leq t < 1, \\ 0 & \text{otherwise.} \end{cases} \dots\dots\dots (2.7)$$

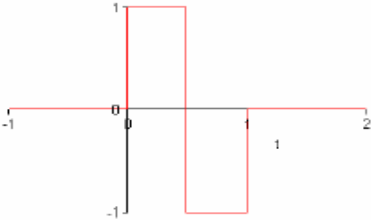


Figure (2.9) Haar Wavelet

$$\phi(t) = \begin{cases} 1 & 0 \leq t < 1, \\ 0 & \text{otherwise} \end{cases} \dots\dots\dots (2.8)$$

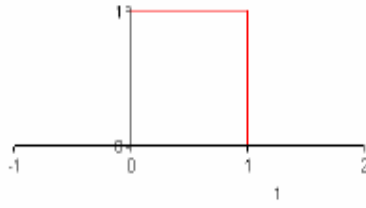


Figure (2.10) Haar Scaling Function

Haar wavelets are the oldest and the simplest wavelets. They are not continuous, but are symmetric. The number of vanishing moments is 1.

2.12 Why Wavelet Analysis Effective

Wavelet transforms have proved to be very efficient and effective in analyzing a very wide class of signals and phenomena. The properties that give the effectiveness are:

- a. The wavelet expansion allows a more accurate local description and separation of signal characteristics. A Fourier coefficient represents components that last for all time and, therefore, temporary events must be described by the phase characteristics that allow cancellation and reinforcement over large time periods. Wavelet expansion coefficients represent a component that itself is local and easier to interpret. The wavelet

expansion may allow a separation of components of a signal that overlaps in both time and frequency.

- b. Wavelet is adjustable and adaptable. Because there is not just one wavelet, they can be designed to fit individual systems that adjust themselves to suit the signal.
- c. The generation of the wavelet coefficients is well matched to the digital computers. There are no derivatives or integrals, just multiplication and addition operations, that are basic to the digital computer. [33]

Chapter Three

System Design and Implementation

3.1 Introduction

This chapter Introduces the total system design and simulation programs used to simulate the Least Significant Bit (LSB) technique used to hide a secret image data into audio media. This technique is implemented in Frequency domain using Discrete Wavelet Transform (DWT) method. Ten types of audio signal are used as a cover to hide the secret image message. The secret image message used in the simulation is of type Joint Photographic Group (jpg). Different sizes of this image are used as a secret message. MATLAB programming environment is used to simulate the total system.

3.2 The Overall System Model

The block diagram of the proposed system is shown in figure (3.1); it can be broken into main parts as follows:

- Read Cover audio (song cover).
- Transform Domain.
- Read Image message.
- Converting Image message to stream bit.
- Hiding in Least Significant Bit.
- Extracting.

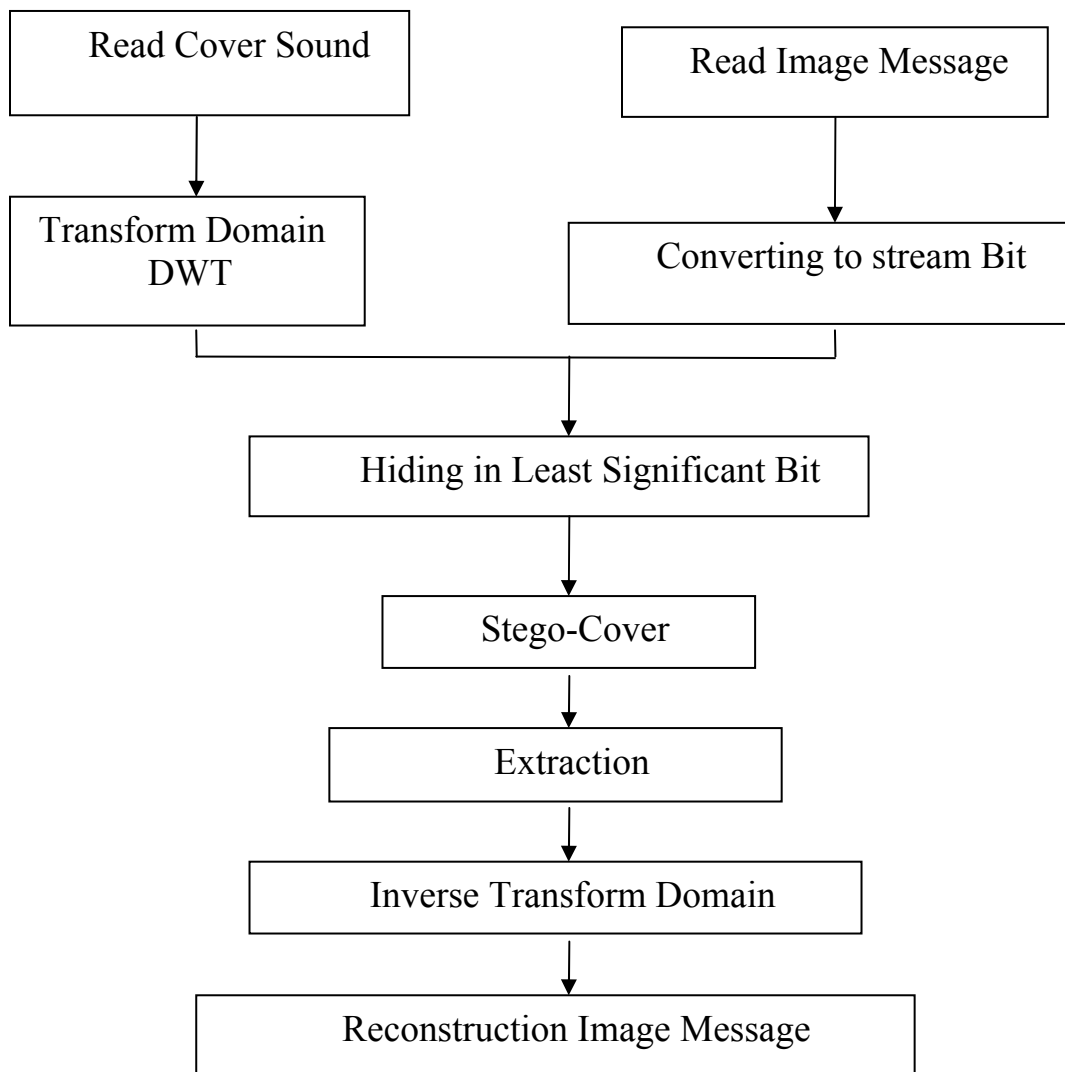


Figure (3.1) The Overall system Model

3.3 The Proposed Stegosystem

The first proposed method is implemented in the time domain and hides each bit of secret audio file in the Least Significant Bit of each host byte of the audio cover.

3.3.1 Embedding in Time Domain

The details of the embedding algorithm steps, shown in figure (3.2) are illustrated as follows:

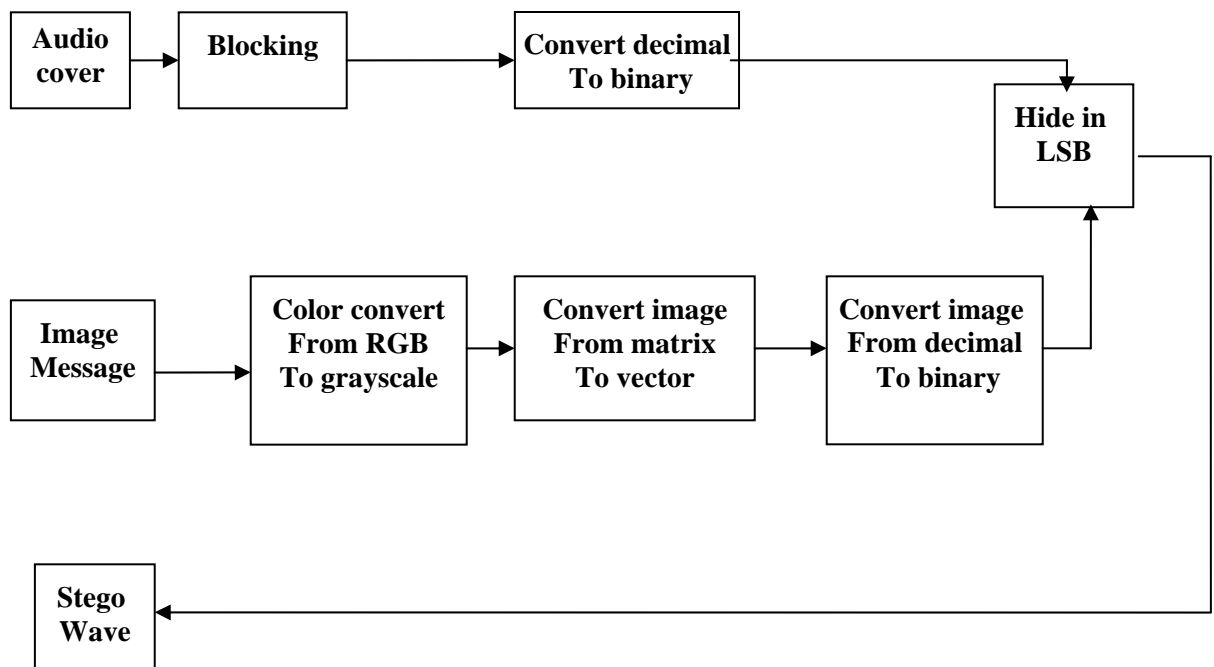


Figure (3.2) Block Diagram of Time Domain Embedding Technique

The above block diagram is explained in more details in the following steps:

1) Select the cover-Audio

The Cover-Audio is carefully selected to prevent the stego-audio from disclosing the existence of an embedded Image. The research used ten types of sound cover (song cover with size (623KB), (243KB), (497KB), (375KB), (568KB), (1.4MB), (819KB), (831KB), (333KB), (169KB)

A size testing operation should be applied here to find if the size of the cover-audio is enough to completely cover the secret message or not, where the size secret message must be smaller than or equal to the permitted size of the cover-audio.

2) Framing Digital Cover Sound Signal:

In this step the digital signal will be divided into samples as (16-bit).

3) Select Image message and convert it from RGB to gray-scale using the well known equation ($\text{gray} = 0.299R + 0.587G + 0.114B$) and then convert it from matrix to vector and framing into 8-bit



Figure (3.3) Original secret image



Figure (3.4) gray scale of image

4) Hiding by using Least Significant Bit Insertion:

The most common steganographic method in audio and image files employ some type of least significant bit substitution or overwriting. The least significant bit term comes from the numeric significance of the bits in a byte. The high-order or most significant bit is the one with the highest arithmetic value (i.e., $2^7=128$), whereas the low-order or least significant bit is the one with the lowest arithmetic value (i.e., $2^0=1$).

As a simple example of least significant bit substitution, imagine "hiding" the character 'G' across the following eight bytes of a carrier file (the least significant bits are underlined):

```
10010101    00001101    11001001    10010110  
00001111    11001011    10011111    00010000
```

A 'G' is represented in the American Standard Code for Information Interchange (ASCII) as the binary string 01000111. These eight bits can be "written" to the least significant bit of each of the eight carrier bytes as follows:

```
10010100    00001101    11001000    10010110  
00001110    11001011    10011111    00010001
```

In the above example, only half of the least significant bits were actually changed (shown above in italics). This makes some sense when one set of zeros and ones are being substituted with another set of zeros and ones.

5) Converting signal from digital to analog:

After implementing the embedding algorithm, convert digital signal to analog, this signal is called stego-wave.

The code of the program is illustrated in Appendix A.

3.3.2 The Extracting Algorithm:

The object must be transmitted to reconstruct the embedded secret message. The Stego-Wave, which contains the embedded secret message that is being transmitted via a public communication channel.

The details of the extracting algorithm steps, shown in Figure (3.5), are given below:

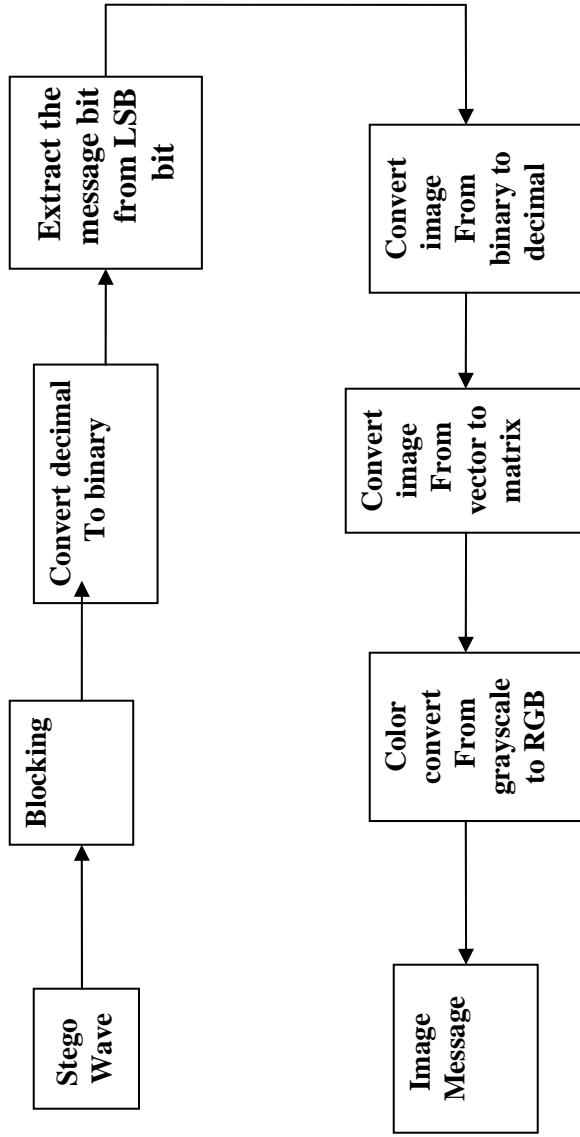


Figure (3.5) Block Diagram of Time Domain Extracting Technique

1) Select the Stego-Wave:

Select the stego-wave in order to extract the secret message from it. Its name is the same name of the cover-wave.

2) Input the Stego-cover file and convert into sequence of bytes.

3) Extract the message from stego wave:

The secret image will be extract from the stego wave, and then the result will be converted from digital to analog and then convert color from grayscale to RGB. This extraction is done on the blocks that are modified in the embedding algorithm. The code of the program used to simulate this analyzing method is illustrated in Appendix A.

3.3.3 Embedding in Transform Domain

The details of the embedding algorithm steps, as shown in figure (3.6), are illustrated as follows:

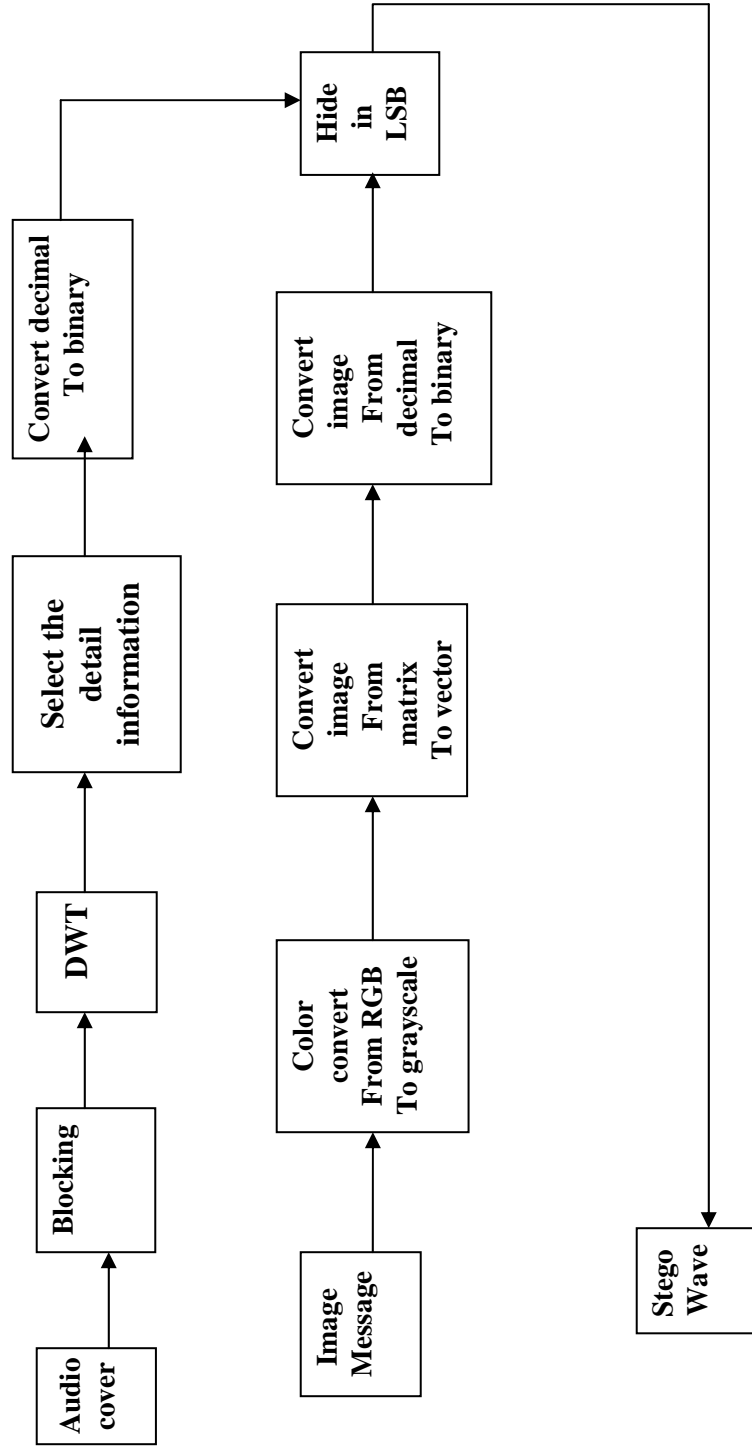


Figure (3.6) Block Diagram of Transform Domain Embedding Technique

The block diagram above is explained in more details in the following steps:

1) Steps 1, 2 and 3 (Select cover-audio, making blocking to song cover and taking the coefficients of DWT and selecting the detail information and then converting from decimal to binary as shown in figure (3.6).

2) Analysis of signal in the Transform Domain (Discrete Wavelet Transform):

Using Discrete Wavelet Transform:

The procedure of DWT is actually computed: The DWT analyzes the signal at different frequency bands with different resolutions by decomposing the signal into a coarse approximation and detailed information. DWT employs two sets of functions, called scaling functions and wavelet functions, which are associated with low pass and highpass filters, respectively. The decomposition of the signal into different frequency bands is simply obtained by successive highpass and lowpass filtering of the time domain signal. The original signal $x[n]$ is first passed through a halfband highpass filter $H[n]$ and a lowpass filter $G[n]$. After filtering, half of the samples can be eliminated according to the Nyquist's rule (which is twice the maximum frequency that exists in the signal), since the signal now has a highest frequency of $\pi/2$ radians instead of π . The signal can therefore be subsampled by 2, simply by discarding every other sample. This constitutes one level of decomposition and can mathematically be expressed as follows :

$$Y_{\text{high}}[K] = \sum_n x[n] \cdot H[2K - n] \dots\dots\dots (3.1)$$

$$Y_{\text{low}}[K] = \sum_n x[n] \cdot G[2K - n] \dots\dots\dots (3.2)$$

Where $Y_{\text{high}} [k]$ and $Y_{\text{low}} [k]$ are the outputs of the highpass and lowpass filters, respectively, after subsampling by 2 .

This decomposition halves the time resolution since only half the number of samples now characterizes the entire signal. However, this operation doubles the frequency resolution, since the frequency band of the signal now spans only half the previous frequency band, effectively reducing the uncertainty in the frequency by half. The above procedure, which is also known as the subband coding, can be repeated for further decomposition. At every level, the filtering and subsampling will result in half the number of samples (and hence half the time resolution) and half the frequency bands spanned (and hence double the frequency resolution).

In this work take the original signal $x[n]$, which has 256 sample points, spanning a frequency band of zero to p rad/s. At the first decomposition level, the signal is passed through the highpass and lowpass filters, followed by subsampling by 2. The output of the highpass filter has 128 points (hence half the time resolution), but it only spans the frequencies $p/2$ to p rad/s (hence double the frequency resolution). These 128 samples constitute the first level of DWT coefficients. The output of the lowpass filter also has 128 samples, but it spans the other half of the frequency band, frequencies from 0 to $p/2$ rad/s. This signal is then passed through the same lowpass and highpass filters for further decomposition. The output of the second lowpass filter followed by subsampling has 64 samples spanning a frequency band of 0 to $p/4$ rad/s, and the output of the second highpass filter followed by subsampling has 64 samples spanning a frequency band of $p/4$ to $p/2$ rad/s. The second highpass filtered signal

Constitutes the second level of DWT coefficients. This signal has half the time resolution, but twice the frequency resolution of the first level signal. In other words, time resolution has been decreased by a factor of 4, and frequency resolution has increased by a factor of 4 compared to the original signal. The lowpass filter output is then filtered once again for further decomposition. This process continues until two samples are left. For this specific example there would be 8 levels of decomposition, each having half the number of samples of the previous level. The DWT of the original signal is then obtained by concatenating all coefficients starting from the last level of decomposition (remaining two samples, in this case). The DWT will then have the same number of coefficients as the original signal. After analyzing cover sound in transform domain and hiding image inside it, the code of the program used to simulate this analyzing method is illustrated in Appendix A. Then compute the Inverse Transform Domain to get stego wave.

3) Compute the Inverse DWT (IDWT):

The signals at every level are upsampled by two, passed through the synthesis filters $H[n]$, and $G[n]$ (highpass and lowpass, respectively), and then added.

3.3.4 The Extracting Algorithm:

The details of the extracting algorithm steps in Transform Domain shown in Figure (3.7) are given below:

The procedure in the Extracting algorithm in the Time Domain is the same in the Transform Domain, but in step 4 in the extraction algorithm in the Time Domain will be changed in Transform Domain as follows:

The DWT coefficients of the cover-Audio will be extract from the stego-wave, coefficient by coefficient, and the result will be converted from binary to decimal, and convert image from vector to matrix and then convert color of the image from grayscale to RGB, then the result will be the secret Image.

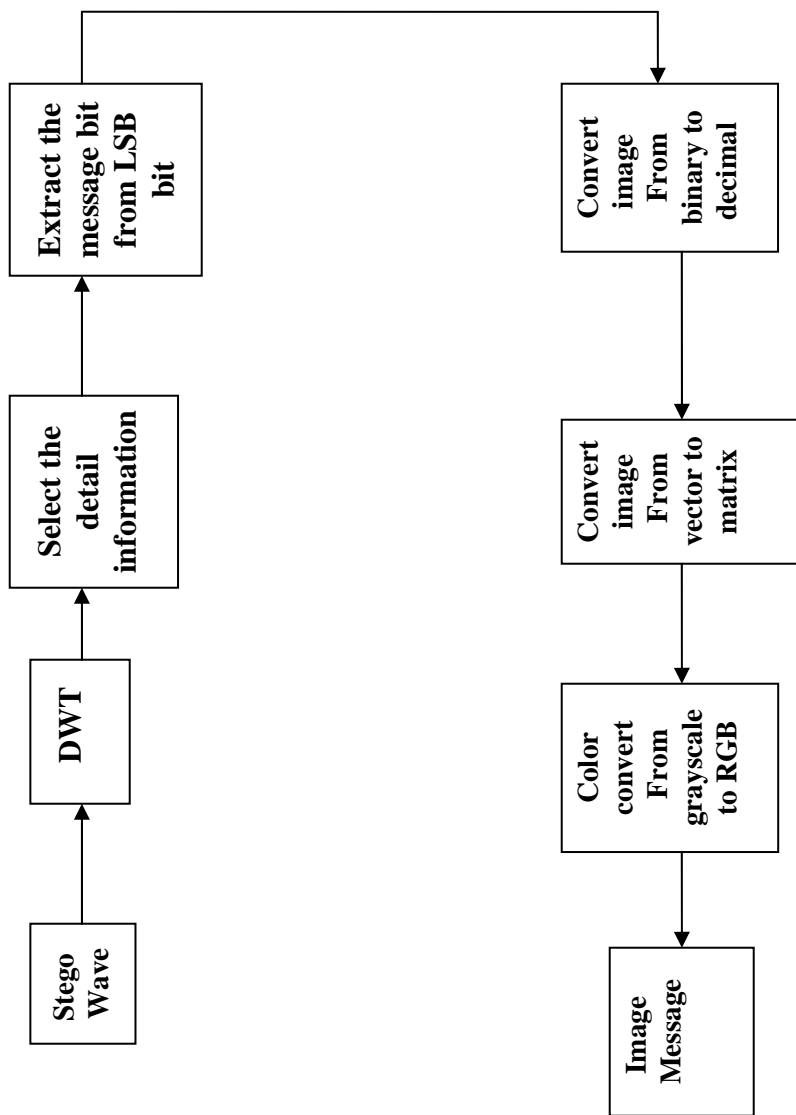


Figure (3.7) Block Diagram of Transform Domain Extracting Technique

3.4 Fidelity Measures

Fidelity measures can be divided into two classes:

- a. Objective Fidelity Criteria.
- b. Subjective Fidelity Criteria.

The objective fidelity criteria are borrowed from digital signal processing and information theory, and provide us with equations that can be used to measure the amount of error in the reconstructed signal (image, sound or video).

Subjective fidelity criteria require the definition of a qualitative scale to assess signal quality. This scale can then be used by human test subjects to determine signal fidelity.

The commonly used objective measures are the Mean Square Error (MSE), Signal to Noise Ratio (SNR), Peak Signal to Noise Ratio (PSNR), Normalized root mean square error (NRMSE), and Correlation.

The MSE is found by taking the summation of the square of the difference between the original and the reconstructed signal, and finally divide it by the total number of samples as shown below:

$$MSE = \frac{1}{N} \sum_{i=0}^{N-1} (R_i - O_i)^2 \dots\dots\dots (3.3)$$

Where

R_i = Reconstructed signal.

O_i = Original signal.

N = number of signal samples.

The smaller value of MSE means the better the reconstructed signal that represents the original signal.

The NRMSE is like MSE, the small value means the better the reconstructed signal that represents the original signal.

$$NRMSE = \sqrt{\frac{\frac{1}{N} \sum_{i=0}^{N-1} (O_i - R_i)^2}{\frac{1}{N} \sum_{i=0}^{N-1} (O_i - M_x)^2}} \dots\dots\dots (3.4)$$

Where M_x = mean of original speech signal

The SNR metrics consider the reconstructed signal to be the “signal” and the error to be “noise”. The SNR can be defined as:

$$SNR = 10 \log_{10} \left(\frac{\frac{1}{N} \sum_{i=0}^{N-1} O_i^2}{MSE} \right) \dots\dots\dots (3.5)$$

A large value of SNR implies a better reconstructed signal.

The PSNR metrics consider the “maximum peak value” and the error to be “noise”. The PSNR can be defined as:

$$PSNR = 10 \log_{10} \left(\frac{Peakvalueof O_i}{MSE} \right) \dots\dots\dots (3.6)$$

PSNR is like SNR, where the large value means a better-reconstructed signal that represents the original signal.

Correlation:

$$Cor = \frac{\sum_{i=0}^{N-1} (R_i - \bar{R}_i)(O_i - \bar{O}_i)}{\sqrt{\sum_{i=0}^{N-1} (R_i - \bar{R}_i)^2 * \sum_{i=0}^{N-1} (O_i - \bar{O}_i)^2}} \dots\dots\dots(3.7)$$

Where \bar{R}_i = average value of R_i

\bar{O}_i = average value of O_i

Figures (3.8), and (3.9) show the flowcharts used to implement some of the above steganography systems. These are Hidden in LSB, and Hidden DWT respectively.

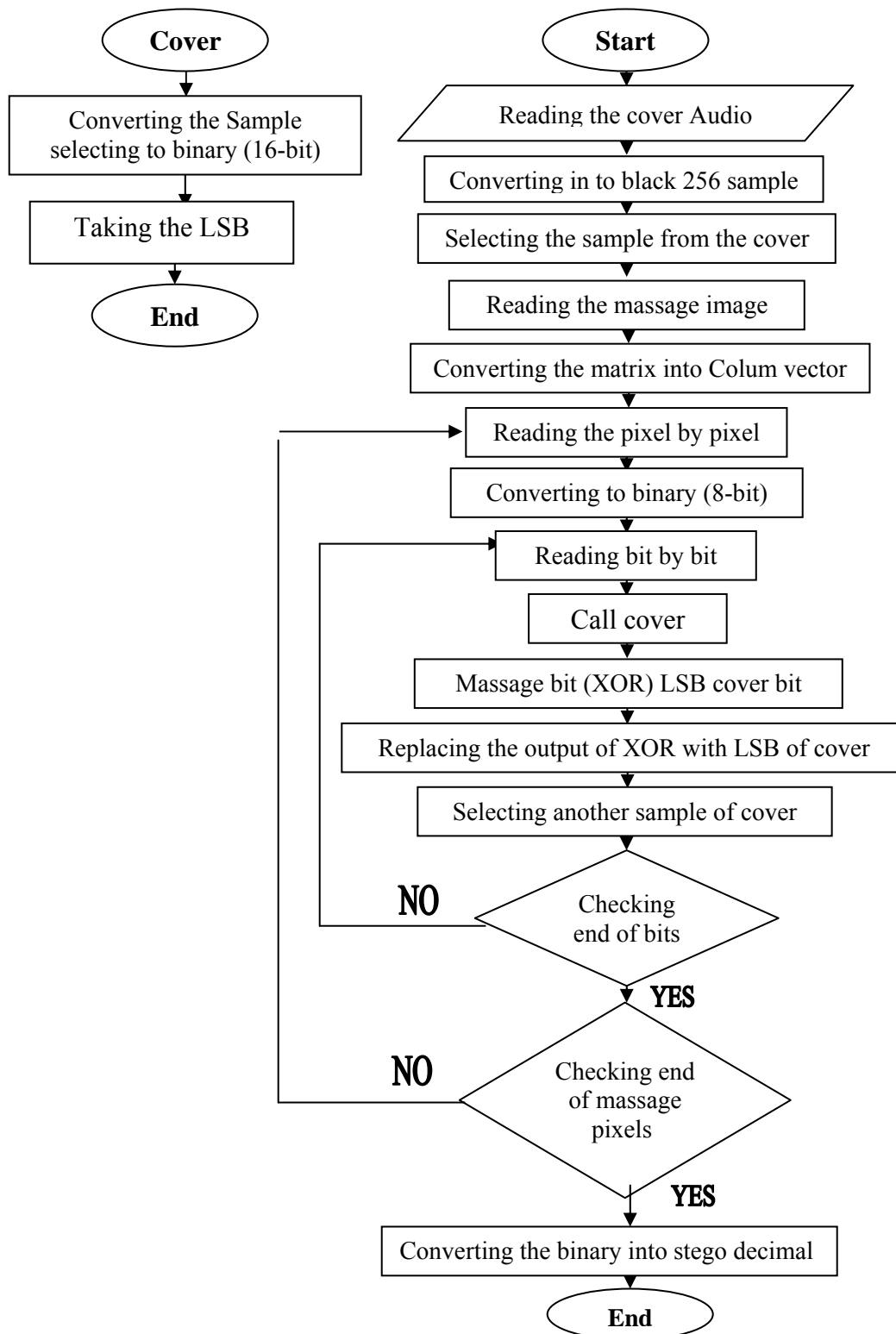


Fig (3. 8) the embedding LSB system flowchart

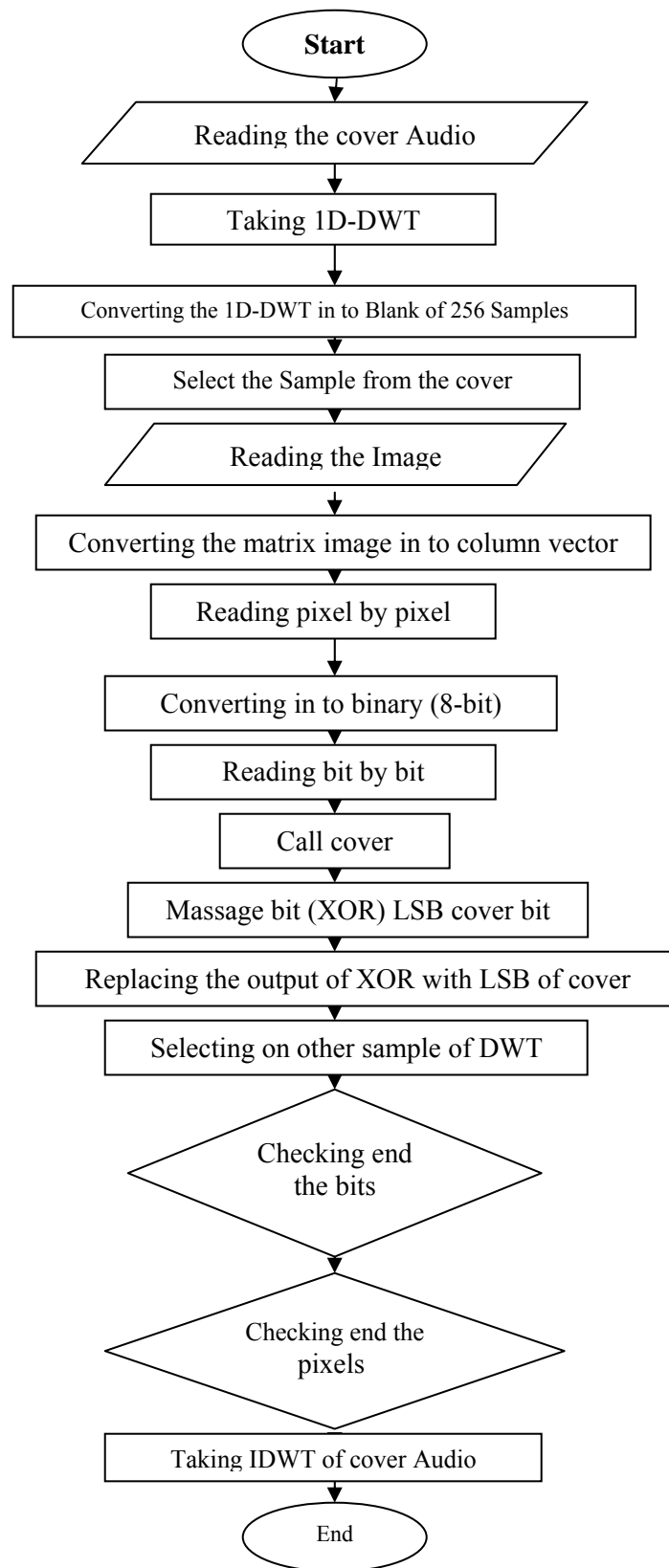


Figure (3.9) the embedding wavelet system flowchart

Chapter Four

Experimental Results and System Evaluation

4.1 Introduction

This chapter demonstrates the results of the designed and implemented scenarios described in chapter three. The tests were performed using standard fidelity criteria such MSE, PSNR, SNR, NRMSE, and COR.

4.2 Tests on the Hiding Methods

In this section, the hiding method was tested. The test strategy is to check the error that might appear in the stego-cover (cover containing the hidden information). Another test was performed on the reconstructed secret files to determine the level of distortion in the secret data due to hiding process. For hiding method, various types of audio file such as Song were used for testing. The following (Table 4.1) gives the properties of the test samples applied to the system.

Table (4.1) the test samples that applied to the system.

File Name	Size (KB)	Length (sec)	Type
Song1 – cover	169	00:38	Song
Song2- cover	243	00:55	Song
Song3- cover	333	01:16	Song
Song4- cover	375	00:47	Song
Song5- cover	497	00:31	Song
Song6- cover	568	00:26	Song
Song7- cover	623	00:28	Song
Song8- cover	819	00:37	Song
Song9- cover	831	00:38	Song
Song10- cover	1.4 MB	01:06	Song

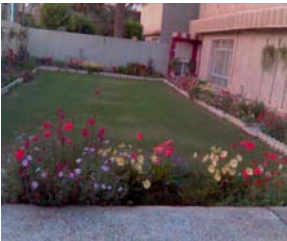
As shown in Table (4.1), the ten cover song files, because we are concerned with hiding in audio steganography, it is frequently needed, where an audio cover is very important because in addition to its information contents, it conveys an embedded authentication signature about the speaker. Information contents convey an embedded authentication signature about the speaker. Figure (4.1), as shown below for test sample of image using as a secret message with different size.



Girl 130 x 121 4.82KB



Flying 145 x 109 3.77 KB



Garden 640x480 58.5 KB



Flower 499x379 20.8KB



Baby 113x150 3.93KB



Students 1152 x 864 208 KB



Riammajeed 197x208 26.5KB



Mall 1280 x 1024 109 KB



Lamees 1536x1152 364KB



Boys 1632 x 1224 407 KB

Figure (4.1) Images used as a secret message

4.2.1 Test on Hiding in the Time domain, and DWT using LSB method.

In this section, we obtain the test results for hiding the secret image file in least bit of each 8 bit, 16 bit of the Speech cover and Song cover, as shown in the following tables, Table (4.2) Test Results for hide on the sample "Song1 wav" Framing 16-bit

Secret File Name	methods	Cover Stego				
		Standard Fidelity Measures				
		SNR	PSNR	NRMSE	Cor	MSE
Secret 1. lena2. Image	Time domain	61.3989	183.6551	3.6914 e ⁻⁰⁰⁵	1.0000	0.4967
	DWT	57.8273	191.3306	1.5255e ⁻⁰⁰⁵	1.0000	0.0848
Secret 2. Flying. Image	Time domain	55.6179	183.6038	3.7132 e ⁻⁰⁰⁵	1.0000	0.5026
	DWT	55.4981	191.1980	1.5490e ⁻⁰⁰⁵	1.0000	0.0875
Secret 3. Garden. Image	Time domain	44.5642	183.7315	3.6590e ⁻⁰⁰⁵	1.0000	0.4880
	DWT	47.6738	191.1321	1.5608e ⁻⁰⁰⁵	1.0000	0.0888
Secret 4. Mall. Image	Time domain	47.4901	183.6515	3.6927e ⁻⁰⁰⁵	1.0000	0.4971
	DWT	50.2736	191.2233	1.5445 e ⁻⁰⁰⁵	1.0000	0.0869
Secret 5. Boys. Image	Time domain	46.1079	183.5771	3.7247e ⁻⁰⁰⁵	1.0000	0.5057
	DWT	50.1186	191.3343	1.5304 e ⁻⁰⁰⁵	1.0000	0.0854
Secret 6 students Image	Time domain	47.0241	183.5909	3.7187e ⁻⁰⁰⁵	1.0000	0.5041
	DWT	51.0526	191.3343	1.5248e ⁻⁰⁰⁵	1.0000	0.0848
Secret 7. Riam. Image	Time domain	43.5022	183.7365	3.6569e ⁻⁰⁰⁵	1.0000	0.4875
	DWT	46.6993	191.0724	1.5715e ⁻⁰⁰⁵	1.0000	0.0900
Secret 8. Riammajeed Image	Time domain	58.1422	183.6265	3.7035 ⁻⁰⁰⁴	1.0000	0.5000
	DWT	63.0179	191.2990	1.5311e ⁻⁰⁰⁵	1.0000	0.0854
Secret 9 Flower. Image	Time domain	44.0339	183.6551	3.6655 ⁻⁰⁰⁵	1.0000	0.4897
	DWT	47.1781	191.1069	1.5653 ⁻⁰⁰⁵	1.0000	0.0848
Secret 10. Baby. Image	Time domain	50.4902	183.6820	3.6799e ⁻⁰⁰⁵	1.0000	0.4936
	DWT	53.0642	191.2632	1.5374e ⁻⁰⁰⁵	1.0000	0.0862

Table (4.3) Test Results for hide on the sample “Song2 .wav” Framing in to 16 bit.

Secret File Name	methods	Cover Stego				
		Standard Fidelity Measures				
		SNR	PSNR	NRMSE	Cor	MSE
Secret 1. lena2. Image	Time domain	54.4892	183.6334	3.6757 e ⁻⁰⁰⁵	1.0000	0.4991
	DWT	58.2710	191.2453	1.5302e ⁻⁰⁰⁵	1.0000	0.0865
Secret 2. Flying. Image	Time domain	52.2048	183.5879	3.6950 e ⁻⁰⁰⁵	1.0000	0.5044
	DWT	55.8646	191.2060	1.5371e ⁻⁰⁰⁵	1.0000	0.0873
Secret 3. Garden. Image	Time domain	44.2020	183.4971	3.7338e ⁻⁰⁰⁵	1.0000	0.5150
	DWT	47.7294	191.1432	1.5483e ⁻⁰⁰⁵	1.0000	0.0886
Secret 4. Mall. Image	Time domain	46.6976	183.5632	3.7055e ⁻⁰⁰⁵	1.0000	0.5072
	DWT	50.3637	191.1432	1.5483e ⁻⁰⁰⁵	1.0000	0.0892
Secret 5. Boys. Image	Time domain	46.7247	183.7043	3.6456e ⁻⁰⁰⁵	1.0000	0.4910
	DWT	50.0514	191.2567	1.5282e ⁻⁰⁰⁵	1.0000	0.0863
Secret 6 students Image	Time domain	47.7945	183.6664	3.6617e ⁻⁰⁰⁵	1.0000	0.4953
	DWT	51.1551	191.2075	1.5368 e ⁻⁰⁰⁵	1.0000	0.0873
Secret 7. Riam. Image	Time domain	43.2466	183.4750	3.7433e ⁻⁰⁰⁵	1.0000	0.5176
	DWT	46.7526	191.1019	1.5556e ⁻⁰⁰⁵	1.0000	0.0894
Secret 8. Riammajeed Image	Time domain	58.8772	183.6265	3.7433 ⁻⁰⁰⁴	1.0000	0.5000
	DWT	62.6599	191.2334	1.5323 e ⁻⁰⁰⁵	1.0000	0.0867
Secret 9 Flower. Image	Time domain	43.7310	183.5884	3.6948 ⁻⁰⁰⁵	1.0000	0.5043
	DWT			⁻⁰⁰⁵	1.0000	
Secret 10. Baby. Image	Time domain	49.1919	183.6052	3.6876e ⁻⁰⁰⁵	1.0000	0.5024
	DWT	52.7823	191.1179	1.5528 e ⁻⁰⁰⁵	1.0000	0.0891

Table (4.4) Test Results for hide on the sample "Song3. Wav "Framing 16-bit

Secret File Name	methods	Cover Stego				
		Standard Fidelity Measures				
		SNR	PSNR	NRMSE	Cor	MSE
Secret 1. lena2. Image	Time domain	59.6658	183.6608	3.6868e ⁻⁰⁰⁵	1.0000	0.4961
	DWT	58.1749	191.2167	1.5447e ⁻⁰⁰⁵	1.0000	0.0871
Secret 2. Flying. Image	Time domain	58.1488	183,6431	3.6943e ⁻⁰⁰⁵	1.0000	0.4982
	DWT	55.5386	191.2621	1.5367e ⁻⁰⁰⁵	1.0000	0.0862
Secret 3. Garden. Image	Time domain	44.7562	183.8367	3.6129 ⁻⁰⁰⁵	1.0000	0.4765
	DWT	47.6693	191.1014	1.5654e ⁻⁰⁰⁵	1.0000	0.0894
Secret 4. Mall. Image	Time domain	47.7391	183.7370	3.6546e ⁻⁰⁰⁵	1.0000	0.4875
	DWT	50.2457	191.1619	1.5545e ⁻⁰⁰⁵	1.0000	0.0882
Secret 5. Boys. Image	Time domain	45.8706	183.5027	3.7545e ⁻⁰⁰⁵	1.0000	0.5145
	DWT	50.0963	191.3455	1.5220e ⁻⁰⁰⁵	1.0000	0.0846
Secret 6 students Image	Time domain	46.7614	183.5261	3.7444e ⁻⁰⁰⁵	1.0000	0.5118
	DWT	51.2228	191.2943	1.5310e ⁻⁰⁰⁵	1.0000	0.0856
Secret 7. Riam. Image	Time domain	43.6817	183.8809	3.5946e ⁻⁰⁰⁵	1.0000	0.4716
	DWT	46.7033	191.0746	1.5702e ⁻⁰⁰⁵	1.0000	0.0900
Secret 8. Riammajeed Image	Time domain	54.9303	183.5985	3.7133e ⁻⁰⁰⁵	1.0000	0.5033
	DWT	62.8233	191.2574	1.5375e ⁻⁰⁰⁵	1.0000	0.0863
Secret 9 Flower. Image	Time domain	44.2037	183.8612	3.6027e ⁻⁰⁰⁵	1.0000	0.4738
	DWT	47.1705	191.1071	1.5644e ⁻⁰⁰⁵	1.0000	0.0893
Secret 10. Baby. Image	Time domain	59.7618	183.6856	3.6763e ⁻⁰⁰⁵	1.0000	0.4933
	DWT	52.5021	191.1730	1.5525e ⁻⁰⁰⁵	1.0000	0.0880

Table (4.5) Test Results for hide on the sample "Song4. Wav "Framing 16-bit

Secret File Name	methods	Cover Stego				
		Standard Fidelity Measures				
		SNR	PSNR	NRMSE	Cor	MSE
Secret 1. lena2. Image	Time domain	71.5355	183.6464	2.7938e ⁻⁰⁰⁵	1.0000	0.4972
	DWT	73.388	188.6704	1.5667e ⁻⁰⁰⁵	1.0000	0.1564
Secret 2. Flying. Image	Time domain	54.4275	183.6299	2.7991e ⁻⁰⁰⁵	1.0000	0.4991
	DWT	56.9737	188.6457	1.5712 e ⁻⁰⁰⁵	1.0000	0.1573
Secret 3. Garden. Image	Time domain	45.4166	183.6341	2.7977e ⁻⁰⁰⁵	1.0000	0.4987
	DWT	47.7631	188.6574	1.5691 e ⁻⁰⁰⁵	1.0000	0.1568
Secret 4. Mall. Image	Time domain	48.1698	183.6440	2.7945e ⁻⁰⁰⁵	1.0000	0.4975
	DWT	50.3809	188.6647	1.5677e ⁻⁰⁰⁵	1.0000	0.1566
Secret 5. Boys. Image	Time domain	47.2432	183.6299	2.7991e ⁻⁰⁰⁵	1.0000	0.4991
	DWT	50.5459	188.7011	1.5612 e ⁻⁰⁰⁵	1.0000	0.1553
Secret 6 students Image	Time domain	48.1707	183.6045	2.8073e ⁻⁰⁰⁵	1.0000	0.5021
	DWT	52.9870	188.5678	1.5410 e ⁻⁰⁰⁵	1.0000	0.1532
Secret 7. Riam. Image	Time domain	44.3953	183.6551	2.7910e ⁻⁰⁰⁵	1.0000	0.4963
	DWT	46.7455	188.6841	1.5642e ⁻⁰⁰⁵	1.0000	0.1559
Secret 8. Riammajeed Image	Time domain	64.5945	183.6459	2.7939e ⁻⁰⁰⁵	1.0000	0.4973
	DWT	63.5878	188.6821	1.5646 e ⁻⁰⁰⁵	1.0000	0.1560
Secret 9 Flower. Image	Time domain	44.9214	183.6568	2.7904e ⁻⁰⁰⁵	1.0000	0.4961
	DWT	47.3000	188.6489	1.5706e ⁻⁰⁰⁵	1.0000	0.1572
Secret 10. Baby. Image	Time domain	51.3436	183.6427	2.7949e ⁻⁰⁰⁵	1.0000	0.4977
	DWT	54.0198	188.6250	1.5749e e ⁻⁰⁰⁵	1.0000	0.1580

Table (4.6) Test Results for hide on the sample "Song5. Wav "Framing 16-bit

Secret File Name	methods	Cover Stego				
		Standard Fidelity Measures				
		SNR	PSNR	NRMSE	Cor	MSE
Secret 1. lena2. Image	Time domain	69.3410	183.6360	2.7644e ⁻⁰⁰⁵	1.0000	0.4991
	DWT	67.6259	188.6312	1.5554e ⁻⁰⁰⁵	1.0000	0.1580
Secret 2. Flying. Image	Time domain	54.8898	183.6223	2.7688e ⁻⁰⁰⁵	1.0000	0.5007
	DWT	56.4491	188.5788	1.5648 e ⁻⁰⁰⁵	1.0000	0.1599
Secret 3. Garden. Image	Time domain	45.4196	183.6243	2.7682e ⁻⁰⁰⁵	1.0000	0.5005
	DWT	47.8505	188.6967	1.5437 e ⁻⁰⁰⁵	1.0000	0.1556
Secret 4. Mall. Image	Time domain	48.1683	183.6481	2.7606e ⁻⁰⁰⁵	1.0000	0.4977
	DWT	50.5224	188.7051	1.5423e ⁻⁰⁰⁵	1.0000	0.1553
Secret 5. Boys. Image	Time domain	47.2185	183.6152	2.7711e ⁻⁰⁰⁵	1.0000	0.5015
	DWT	49.7183	188.6225	1.5570e ⁻⁰⁰⁵	1.0000	0.1583
Secret 6 students Image	Time domain	48.1961	183.6287	2.7668e ⁻⁰⁰⁵	1.0000	0.5000
	DWT	50.7344	188.6446	1.5530 e ⁻⁰⁰⁵	1.0000	0.1575
Secret 7. Riam. Image	Time domain	44.3987	183.6527	2.7591e ⁻⁰⁰⁵	1.0000	0.4972
	DWT	46.8018	188.6631	1.5497 e ⁻⁰⁰⁵	1.0000	0.1569
Secret 8. Riammajeed Image	Time domain	76.4733	183.6476	2.7608e ⁻⁰⁰⁵	1.0000	0.4978
	DWT	69.6316	188.6884	1.5452 e ⁻⁰⁰⁵	1.0000	0.1559
Secret 9 Flower. Image	Time domain	44.9172	183.6730	2.7527e ⁻⁰⁰⁵	1.0000	0.4949
	DWT	47.3559	188.6592	1.5504e ⁻⁰⁰⁵	1.0000	0.1570
Secret 10. Baby. Image	Time domain	51.1461	183.6265	2.7675e ⁻⁰⁰⁵	1.0000	0.5002
	DWT	53.3853	188.6636	1.5496e ⁻⁰⁰⁵	1.0000	0.1568

Table (4.7) Test Results for hide on the sample "Song6. Wav "Framing 16-bit

Secret File Name	methods	Cover Stego				
		Standard Fidelity Measures				
		SNR	PSNR	NRMSE	Cor	MSE
Secret 1. lena2. Image	Time domain	53.5819	183.5239	2.6811e ⁻⁰⁰⁵	1.0000	0.5071
	DWT	58.4851	188.3148	1.5444e ⁻⁰⁰⁵	1.0000	0.1683
Secret 2. Flying. Image	Time domain	52.3759	183.5520	2.6725e ⁻⁰⁰⁵	1.0000	0.5039
	DWT	57.0099	188.3494	1.5383 e ⁻⁰⁰⁵	1.0000	0.1669
Secret 3. Garden. Image	Time domain	45.0781	183.4038	2.7185e ⁻⁰⁰⁵	1.0000	0.5213
	DWT	47.7657	188.2290	1.55558e ⁻⁰⁰⁵	1.0000	0.1716
Secret 4. Mall. Image	Time domain	56.0024	183.6016	2.6572 ⁻⁰⁰⁵	1.0000	0.4981
	DWT	50.4173	188.2979	1.5475e ⁻⁰⁰⁵	1.0000	0.1689
Secret 5. Boys. Image	Time domain	48.0241	183.7411	2.6149e ⁻⁰⁰⁵	1.0000	0.4824
	DWT	49.7426	188.3238	1.5428e ⁻⁰⁰⁵	1.0000	0.1679
Secret 6 students Image	Time domain	49.0680	183.7155	2.6226e ⁻⁰⁰⁵	1.0000	0.4852
	DWT	50.6606	188.2877	1.5493 e ⁻⁰⁰⁵	1.0000	0.1693
Secret 7. Riam. Image	Time domain	44.1528	183.3447	2.7370e ⁻⁰⁰⁵	1.0000	0.5285
	DWT	46.6957	188.2188	1.5616e ⁻⁰⁰⁵	1.0000	0.1720
Secret 8. Riammajeed Image	Time domain	56.0024	183.6016	2.6572e ⁻⁰⁰⁵	1.0000	0.4981
	DWT	66.4006	188.2195	1.5615 e ⁻⁰⁰⁵	1.0000	0.1720
Secret 9 Flower. Image	Time domain	44.6477	183.3514	2.7349e ⁻⁰⁰⁵	1.0000	0.5277
	DWT	47.2220	188.2568	1.5548e ⁻⁰⁰⁵	1.0000	0.1705
Secret 10. Baby. Image	Time domain	49.9690	183.5205	2.6822e ⁻⁰⁰⁵	1.0000	0.5075
	DWT	53.2848	188.3306	1.5416e ⁻⁰⁰⁵	1.0000	0.1677

Table (4.8) Test Results for hide on the sample "Song7. Wav "Framing 16-bit

Secret File Name	methods	Cover Stego				
		Standard Fidelity Measures				
		SNR	PSNR	NRMSE	Cor	MSE
Secret 1. lena2. Image	Time domain	78.3233	183.6362	2.9742e ⁻⁰⁰⁵	1.0000	0.4958
	DWT	55.9649	189.0626	1.5924e ⁻⁰⁰⁵	1.0000	0.1421
Secret 2. Flying. Image	Time domain	56.8529	183.6248	2.9781e ⁻⁰⁰⁵	1.0000	0.4971
	DWT	54.2140	189.0616	1.5926 e ⁻⁰⁰⁵	1.0000	0.1421
Secret 3. Garden. Image	Time domain	45.2635	183.6614	2.9656e ⁻⁰⁰⁵	1.0000	0.4929
	DWT	47.2355	188.9238	1.6180e ⁻⁰⁰⁵	1.0000	0.1467
Secret 4. Mall. Image	Time domain	48.1161	183.6498	2.9696e ⁻⁰⁰⁵	1.0000	0.4942
	DWT	49.6680	188.9723	1.6090e ⁻⁰⁰⁵	1.0000	0.1415
Secret 5. Boys. Image	Time domain	46.7845	183.5931	2.9890e ⁻⁰⁰⁵	1.0000	0.5007
	DWT	50.5451	189.3434	1.5417e ⁻⁰⁰⁵	1.0000	0.1332
Secret 6 students Image	Time domain	47.6439	183.5814	2.9930e ⁻⁰⁰⁵	1.0000	0.5020
	DWT	51.4734	189.2488	1.5586 e ⁻⁰⁰⁵	1.0000	0.1361
Secret 7. Riam. Image	Time domain	44.2230	183.6801	2.9592e ⁻⁰⁰⁵	1.0000	0.4908
	DWT	46.3258	188.8088	1.6396e ⁻⁰⁰⁵	1.0000	0.1507
Secret 8. Riammajeed Image	Time domain	58.5030	183.6639	2.9647e ⁻⁰⁰⁵	1.0000	0.4926
	DWT	57.2404	189.0875	1.5878 e ⁻⁰⁰⁵	1.0000	0.1413
Secret 9 Flower. Image	Time domain	44.7450	183.6831	2.9582e ⁻⁰⁰⁵	1.0000	0.4904
	DWT	47.2220	188.2568	1.5548e ⁻⁰⁰⁵	1.0000	0.1705
Secret 10. Baby. Image	Time domain	51.4632	183.6164	2.9810e ⁻⁰⁰⁵	1.0000	0.4980
	DWT	51.7988	189.0586	1.5931e ⁻⁰⁰⁵	1.0000	0.1422

Table (4.9) Test Results for hide on the sample "Song8. Wav "Framing 16-bit

Secret File Name	methods	Cover Stego				
		Standard Fidelity Measures				
		SNR	PSNR	NRMSE	Cor	MSE
Secret 1. lena2. Image	Time domain	61.2694	183.6572	3.2443e ⁻⁰⁰⁵	1.0000	0.4960
	DWT	69.3124	189.9488	1.5723e ⁻⁰⁰⁵	1.0000	0.1165
Secret 2. Flying. Image	Time domain	53.9441	183.7024	3.2274e ⁻⁰⁰⁵	1.0000	0.4908
	DWT	57.0170	189.9531	1.5715e ⁻⁰⁰⁵	1.0000	0.1164
Secret 3. Garden. Image	Time domain	44.9446	183.6132	3.2607e ⁻⁰⁰⁵	1.0000	0.5010
	DWT	47.6920	189.9327	1.5752e ⁻⁰⁰⁵	1.0000	0.1169
Secret 4. Mall. Image	Time domain	47.6073	183.6558	3.2448e ⁻⁰⁰⁵	1.0000	0.4961
	DWT	50.5194	189.9852	1.5657 e ⁻⁰⁰⁵	1.0000	0.1155
Secret 5. Boys. Image	Time domain	46.9623	183.7438	3.22121e ⁻⁰⁰⁵	1.0000	0.4862
	DWT	49.6365	189.9683	1.5688 e ⁻⁰⁰⁵	1.0000	0.1160
Secret 6 students Image	Time domain	48.0965	183.7317	3.2165e ⁻⁰⁰⁵	1.0000	0.4875
	DWT	50.7293	189.9184	1.5778e ⁻⁰⁰⁵	1.0000	0.1173
Secret 7. Riam. Image	Time domain	43.9502	183.5934	3.2674e ⁻⁰⁰⁵	1.0000	0.5031
	DWT	46.7036	189.9375	1.5743e ⁻⁰⁰⁵	1.0000	0.1168
Secret 8. Riammajeed Image	Time domain	68.5337	183.7042	3.2268e ⁻⁰⁰⁵	1.0000	0.4906
	DWT	65.5727	189.9714	1.5682e ⁻⁰⁰⁵	1.0000	0.1159
Secret 9 Flower. Image	Time domain	44.4086	183.5962	3.2672e ⁻⁰⁰⁵	1.0000	0.5030
	DWT	47.1494	189.9338	1.5750 ⁻⁰⁰⁵	1.0000	0.1169
Secret 10. Baby. Image	Time domain	49.9211	183.6815	3.2352e ⁻⁰⁰⁵	1.0000	0.4932
	DWT	52.5554	189.9345	1.5749e ⁻⁰⁰⁵	1.0000	0.1169

Table (4.10) Test Results for hide on the sample "Song9. Wav "Framing 16-bit

Secret File Name	methods	Cover Stego				
		Standard Fidelity Measures				
		SNR	PSNR	NRMSE	Cor	MSE
Secret 1. lena2. Image	Time domain	57.9775	183.5817	2.6612e ⁻⁰⁰⁵	1.0000	0.4993
	DWT	58.7662	188.0783	1.5858e ⁻⁰⁰⁵	1.0000	0.1773
Secret 2. Flying. Image	Time domain	54.7567	183.5773	2.6625e ⁻⁰⁰⁵	1.0000	0.4998
	DWT	56.9339	188.0749	1.5864e ⁻⁰⁰⁵	1.0000	0.1416
Secret 3. Garden. Image	Time domain	45.3855	183.5881	2.6592e ⁻⁰⁰⁵	1.0000	0.4986
	DWT	47.6920	189.9327	1.5752e ⁻⁰⁰⁵	1.0000	0.1169
Secret 4. Mall. Image	Time domain	48.0709	183.5891	2.6589e ⁻⁰⁰⁵	1.0000	0.4985
	DWT	50.5194	189.9852	1.5657 e ⁻⁰⁰⁵	1.0000	0.1155
Secret 5. Boys. Image	Time domain	42.3781	183..5783	2.6622e ⁻⁰⁰⁵	1.0000	0.4997
	DWT	49.7509	188.1173	1.5787 e ⁻⁰⁰⁵	1.0000	0.1757
Secret 6 students Image	Time domain	48.3449	183.5597	2.6679e ⁻⁰⁰⁵	1.0000	0.5018
	DWT	50.7226	188.1327	1.5759e ⁻⁰⁰⁵	1.0000	0.1751
Secret 7. Riam. Image	Time domain	44.3829	183.5707	2.6645e ⁻⁰⁰⁵	1.0000	0.5006
	DWT	46.6041	188.0502	1.5909e ⁻⁰⁰⁵	1.0000	0.1785
Secret 8. Riammajeed Image	Time domain	64.4391	183.5670	2.6657e ⁻⁰⁰⁵	1.0000	0.5010
	DWT	63.5598	188.1619	1.5706e ⁻⁰⁰⁵	1.0000	0.1739
Secret 9 Flower. Image	Time domain	44.8827	183.5790	2.6620e ⁻⁰⁰⁵	1.0000	0.4996
	DWT	47.1494	189.9338	1.5750 ⁻⁰⁰⁵	1.0000	0.1169
Secret 10. Baby. Image	Time domain	50.8207	183.5639	2.6666e ⁻⁰⁰⁵	1.0000	0.5014
	DWT	52.8778	188.0081	1.5987e ⁻⁰⁰⁵	1.0000	0.1802

Table (4.11) Test Results for hide on the sample "Song10. Wav "Framing 16-bit

Secret File Name	methods	Cover Stego				
		Standard Fidelity Measures				
		SNR	PSNR	NRMSE	Cor	MSE
Secret 1. lena2. Image	Time domain	58.2115	183.5843	2.3758e ⁻⁰⁰⁵	1.0000	0.5021
	DWT	58.2931	187.2886	1.5858e ⁻⁰⁰⁵	1.0000	0.1773
Secret 2. Flying. Image	Time domain	55.8146	183.5826	2.3763e ⁻⁰⁰⁵	1.0000	0.5023
	DWT	56.5149	187.2960	1.5497e ⁻⁰⁰⁵	1.0000	0.2136
Secret 3. Garden. Image	Time domain	45.9828	183.6453	2.3592e ⁻⁰⁰⁵	1.0000	0.4951
	DWT	47.7392	187.2191	1.5634e ⁻⁰⁰⁵	1.0000	0.2174
Secret 4. Mall. Image	Time domain	48.7377	183.5573	2.3832e ⁻⁰⁰⁵	1.0000	0.5052
	DWT	50.3583	187.2710	1.5541 e ⁻⁰⁰⁵	1.0000	0.2148
Secret 5. Boys. Image	Time domain	47.7887	183.6300	2.3634e ⁻⁰⁰⁵	1.0000	0.4968
	DWT	49.8686	187.3361	1.5425 e ⁻⁰⁰⁵	1.0000	0.2116
Secret 6 students Image	Time domain	48.6396	183.5970	2.3724e ⁻⁰⁰⁵	1.0000	0.5006
	DWT	50.7286	187.2984	1.5992e ⁻⁰⁰⁵	1.0000	0.2135
Secret 7. Riam. Image	Time domain	44.9460	183.6384	2.3611e ⁻⁰⁰⁵	1.0000	0.4959
	DWT	46.7075	187.2261	1.5622e ⁻⁰⁰⁵	1.0000	0.2171
Secret 8. Riammajeed Image	Time domain	59.7318	183.5639	2.3814e ⁻⁰⁰⁵	1.0000	0.5044
	DWT	62.7710	187.2841	1.5518e ⁻⁰⁰⁵	1.0000	0.2142
Secret 9 Flower. Image	Time domain	45.4722	183.6515	2.3575e ⁻⁰⁰⁵	1.0000	0.4944
	DWT	47.2366	187.2263	1.5621 ⁻⁰⁰⁵	1.0000	0.2165
Secret 10. Baby. Image	Time domain	51.8784	183.6167	2.3670e ⁻⁰⁰⁵	1.0000	0.4983
	DWT	53.6192	187.2378	1.5601e ⁻⁰⁰⁵	1.0000	0.2165

The tables (4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, and 4.11) don't contain the comparison results between the original and reconstructed audio data. Also these tables indicate that the noise level of the stego-cover increases when increasing the hiding bit using 16 bit for hidden, but is still an acceptable range for the noise level.

The results listed in these tables indicate that:

1. In tables 4.2,4.3,4.4,4.5,4.6,4.7,4.8,4.9,4.10 and 4.11, when using the song cover, the value of the MSE ranges from (0.0848-0.0900), (0.0863-0.0891),(0.0846-0.0900),(0.1553-0.1559),(0.1556-0.1599),(0.1669-0.1720),(0.1159-0.1173),(0.1332,0.15070),(0.1416-0.1785),(0.2116-0.2171) respectively.
2. Hiding method produces an acceptable range of PSNR, which is between (191.0724-191.3343) in song cover with size 169KB, (187.2261-187.3361) in song cover with size 1.4MB.
3. In the hiding method, the song _cover gives best results with large size (Song cover 10 with size 1.4MB) less error than in (Song cover with size 169KB).1. The hiding ratio (the size of secret data to the size of the cover data).

Depends on which hiding method is used. So that the results from Song cover with large size is better than song cover with small size, because the size of song cover is larger than speech cover from the secret file.

4. DWT gives best results (i.e. produces less error than Time Domain), and the results of MSE, PSNR are best in DWT.

The question now what is the best between Time Domain and Transform Domain? The answer to that question depends on the meaning of the word “best”; if it means the method which provides the largest hiding ratio then the “Least Significant Bit Insertion” is the best. If the word “best” means the strongest method against attack, then the “Discrete Wavelet Transform” is the best, because it has gained its power from the wavelet transform.

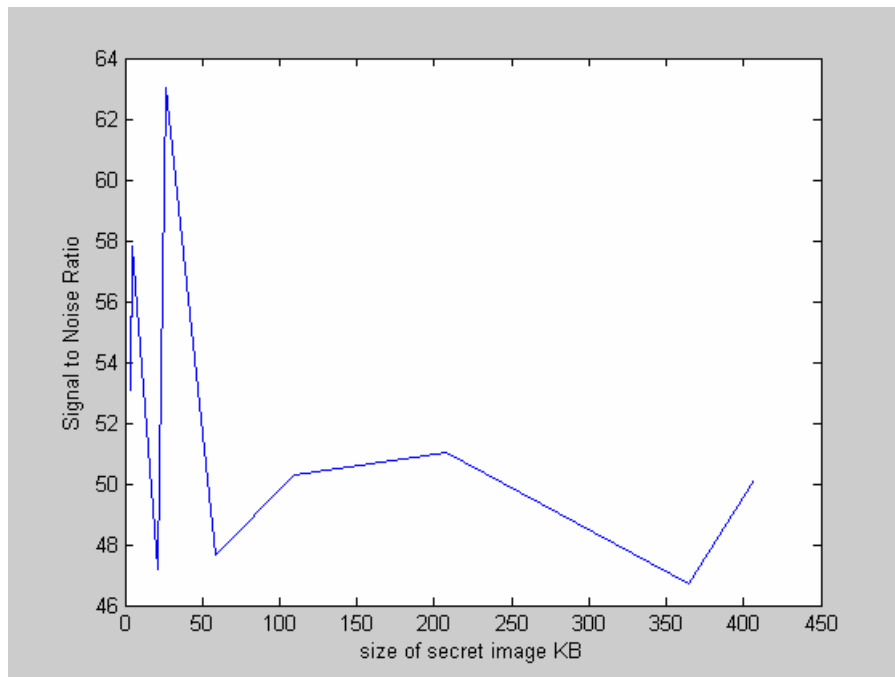


Figure (4.2) Signal to Noise Ratio when using Song Cover with size 169KB

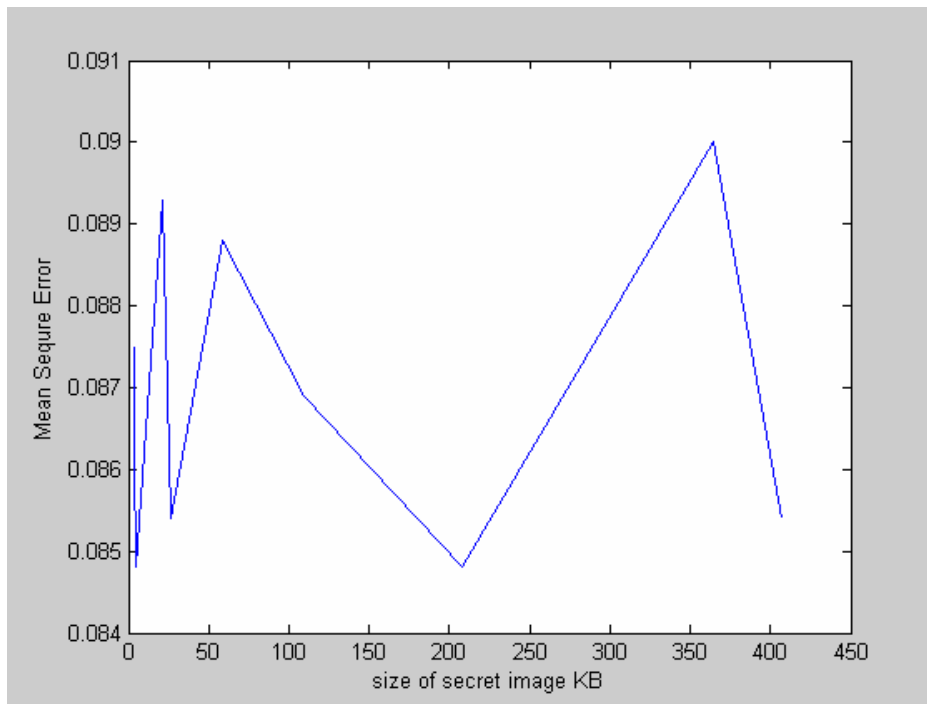


Figure (4.3) Mean Square Error when using Song cover with size 169KB

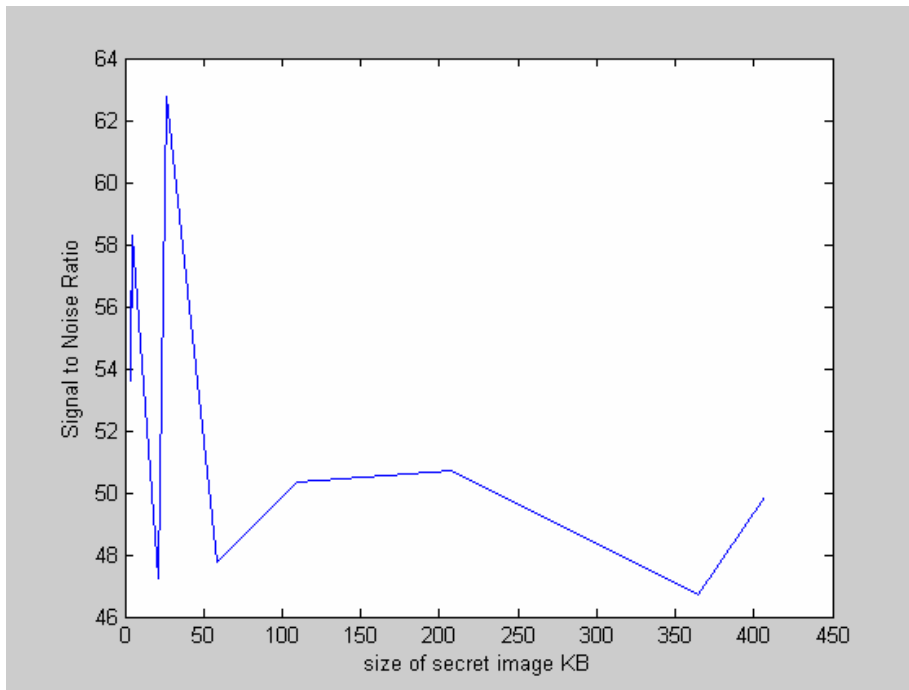


Figure (4.4) Signal to Noise Ratio when using Song cover with size 1.4MB

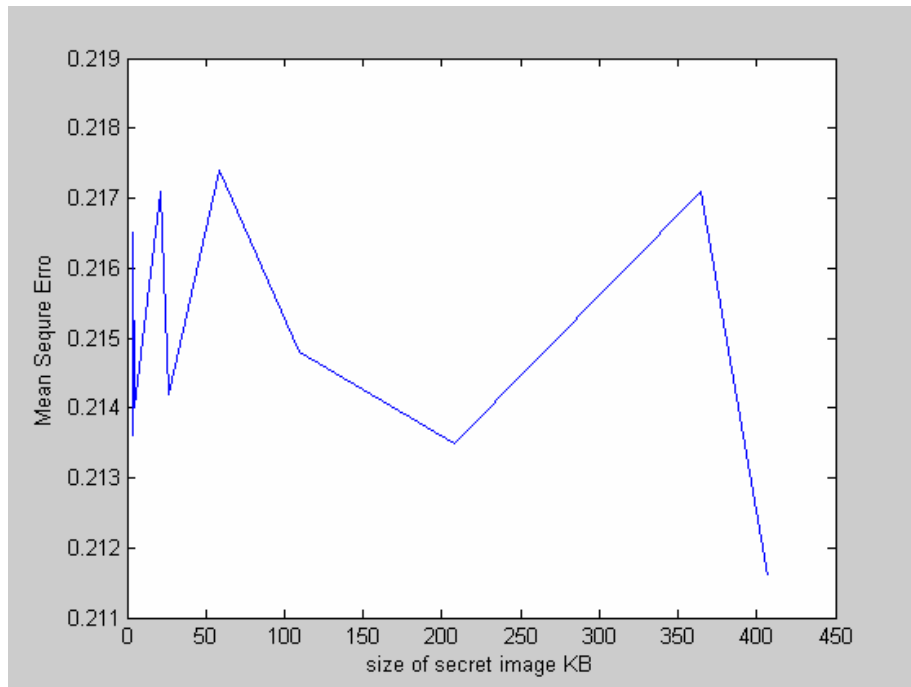


Figure (4.5) Mean Square Error when using Song cover with size 1.4MB.

Chapter Five

Conclusions and Suggestions

for Future Work

5.1 Conclusions

From the test results regarding on the proposed system, the following remarks are derived:

1. The use of Discrete Wavelet Transform (DWT) adds small error to the reconstructed data, because very small hidden data are lost in transformation process.
2. The use of song audio cover is better than speech audio cover, since the first causes greatest SNR (52.88), PSNR (195.64) and the smallest MSE (0.499). Another reason is that the size of song audio cover is larger than speech audio cover.
3. From practical point of view, the size of the secret message in Steganographic system compared with cover size has a great effect on the detection rates.
4. The number of bits embedded by using Least Significant Bit Insertion in Discrete Wavelet Transform is large in comparison with number of bits embedded, by using the same technique in Time Domain.

5.2 Suggestions for Future Work

During the development of the proposed system, many suggestions for future work have emerged to increase the system efficiency; among these suggestions are the following:

1. Compressing the secret data before embedding in the cover; this will lead to an increase in hiding rate.
2. Develop a system for hiding audio in image or image in image using the same techniques used in the proposed system.
3. Develop a system that uses other hiding methods like (phase coding, spread spectrum and echo data hiding) techniques.
4. Develop a system to use other file format like (MP3 and ADPCM wave file).

References

- [1] Ira S. Moskowitz, Grrth E. Longdon and Liwu Chang, "***A new paradigm hidden in steganography***", Naval research laboratories, Washington, DC20375, 2000.
- [2] x.Jianyun, Andrew H. Suig, Peipei Shi and Qingzhong Lin, "***Text steganography using wavelet transform***", Dep. Of Computer Science, New Maxico Tech, Socorro, NM87801, USA, 2003.
- [3] Smith, A., "***Information Hiding***", Proceeding of Second International Workshop, Lecture Notes In Computer Science, Springer, Verlag, Vol. 1525, 1998.
- [4] K. Ahmad, "***Image in Image Steganography System***", University of Baghdad, College of Science, Oct., 2002.
- [5] Johnson N.F., Duricn Z., Jajodia S., "***information Hiding: Steganography and watermarking Attack and Countermeasurments***", Kluwer Academic Publishers, USA, 2001.
- [6] W.Bender, D. Cruhl, N. Morimoto and A. Lu, "***Techniques for Data Hiding***", IBM System Journal, Vol. 36, Nos.2&4, 1996.
- [7] Karen R., "***Steganography and Steganalysis***", 2001, URL:
<http://www.krenn.nl/univ/cry/steg/article.pdf>.
- [8] W. Bender, D. Cruhl, N. Morimoto and A. Lu, "***Techniques for Data Hiding***", IBM systems journal, Vol. 36, Nos. 3&4, 1996.
- [9] Deborah A. Whitiak, "***The art of steganography***", GSEC practical, SANS institute, 2003.

- [10] X. Jianyun, Andrew H. Sung, Peipei Shi and Qingzhong Lin, "***Text steganography using wavelet transform***", Dept. of computer science, New Mexico Tech, Socorro, NM87801, USA, 2003.
- [11] Yasmeeen I. Dieab, "***Audio Watermarking***", M.Sc. Thesis, Dept. of Computer Science, Al-Nahrain University, Iraq, 2003.
- [12] V. Vijaya Kumar, U.S.N.Raju, "***Wavelet based Texture Segmentation methods based on Combinatorial of Morphological and Statistical Operations***", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.8, August 2008.
- [13] Mohammad Pooyan, Ahmad Delforouzi, "***LSB-based Audio Steganography Method Based on Lifting Wavelet Transform***", Department of Electrical and Computer Engineering, Shahed University, delforouzi@shahed.ac.ir, pooyan@shahed.ac.ir, 2007.
- [14] N.Johnson, Z. Duric and S. Jajodia, "***Steganalysis: The Investigation of Hidden Information***", Kluwer Academic Publisher, 2001.
- [15] James Cadwell, "***Steganography***", US Air Force, 2000.
- [16] Katezbeisser, Stefan Petitcolas and A. Fabian, "***Information hiding techniques for steganography and digital watermarking***", Artech House Inc., Norwood, 2000.
- [17] Sellars Duncan, "***Introduction to Steganography***", 1999.
- [18] Yang Yang and faculty of computer science, Dalhousie University, "***Digital watermarking technologies***", 2001.
- [19] Ferrill, Elizabeth, Moyer and Mathew, "***A survey of digital watermarking***", 1998.
- [20] Kientzle Tim, "***Programmers Guide to sound***", Addison Wesley Developers Press, 1998.

- [21] L. Decamro, "*New technologies for audio copy protection*", Electronic Media Article, 1999.
- [22] Qu Shaohong, "*Beyond the basics: real time audio and video*", prentice Hall Inc., 1996.
- [23] Auday A. Al-Dulaimy, "*Fractal Image Compression with Fastig Approach*", M.Sc., Thesis, Dept. of Computer Science, Al-Nahrian University, Iraq, 2003.
- [24] H. Hameed M., "*Text in Image Steganography Techniques*", M.Sc., Thesis, Computer Science dept., College of Science, University of Baghdad, 2001.
- [25] Ibraheem N. Ibraheem , "*Image Compression using Wavelet Transform*", M.Sc. Thesis Dept. of Computer Science, Baghdad University, Iraq, 2004.
- [26] Ibraheem H. Mohamed, "*Application of The Wavelet Transform in Denoising Flow Signal*", M.Sc. Thesis, Electronic and Communications Engineering , College of Engineering, Al-Nahrian University, 2005.
- [27] R. Polikar, "*The wavelet tutorial part3: Multiresolution analysis*", Dept. of electrical and computer engineering Rowan University, Oct. 1998.
- [28] C. Burrus, R. Gopinath and H. Gao, "*Introduction to wavelets and wavelet transform*", Prentice Hall Inc., 1998.
- [29] Mustafa Dhiaa T. Al-Hassani, "*Design of a Fingerprint Recognition System Using Wavelet Transform*" M.Sc. Thesis, Dept. of Computer Science, Al-Nahrian University, Iraq, 2003.
- [30] Mathworks , Matlab Wavelet Toolbox Use's Guide, V6.5, 2002.

Appendix A

A-1 Computer program for hiding secret data inside audio signal using Least Significant Bit (LSB) method in Time Domain

```
clc
clear all
tic
W=randperm(255);
index=[ ];

Lenc=0;
len_speech=18000; %%% length of speech signal
%%%% read the cover speech signal
fid=fopen('rr.wav','rb');
[x]=fread(fid,len_speech,'int16');
origdata=x(250:end);
origdata(length(origdata)+1:2*length(origdata))=x(250:end);

% read the image
x_i=imread('flying.jpg');

y_i=double(rgb2gray(x_i));
[r c]= size(y_i);
y_i_v=reshape(y_i,1,r*c);% vector of the image

y_i_b=dec2bin(y_i_v) ;% binary

[a1 a2]=size(y_i_b);
im=reshape(y_i_b,1,a1*a2);

len_speech=length(origdata);
len_frame=255;
nf=floor(len_speech/len_frame); %%% no. of frames required
index=1;
```

```
for tt=0:nf-1
    %%% framing into blocks of length =len_frame
    xr=origdata(1+tt*len_frame:len_frame+tt*len_frame);

    sign_xr=sign(xr);
    xa=abs(xr);
```

```

xrej=xa;

for k=1:length(xa)

    xb=dec2bin(xa(W(k)),16);

    if index < (a1*a2)
        xb(16)=im(index) ; % hid information in the LSB
        index=index+1;
    end

    xd=bin2dec(xb);
    xrej(W(k))=xd ;

end

xf=xrej.*sign_xr;

for k1=1:length(xf)
rS(k1+tt*len_frame)=xf(k1);
end

end
origdata=origdata(1:length(rS));

rS = rS';%(1:length(origdata));

% [1] Signal to Noise Ratio

sqdata = origdata.^2; % Square of original speech signal
sqrS = rS.^2; % Square of reconstructed signal
msqdata = mean(sqdata); % Mean square of speech signal
sqdiff = (sqdata-sqrS); % Square difference
msqdiff = mean(sqdiff); % Mean s      difference
SNR = 10*log10(abs(msqdata/ms      % Signal to noise ratio

```

`%[2] Peak Signal to Noise Ratio`

`N = length(rS); % Length of reconstructed signal`

`X = max(abs(sqdata)); % Maximum absolute square of original
signal`

`diff = origdata - rS; % Difference signal`

```
enddiff = (norm(diff))^2; % Energy of the difference between the  
% original and reconstructed signal  
PSNR = 10*log10((N*(X^2))/enddiff) % Peak Signal to noise ratio
```

```
%[3] Normalised Root Mean Square Error
```

```
difffsq = diff.^2; % Difference squared  
mdifffsq = mean(difffsq); % Mean of difference squared  
mdata = mean(origdata); % Mean of original speech signal  
scaledsqS = (origdata - mdata).^2; % Squared scaled data  
mscaledsqS = mean(scaledsqS); % Mean of squared scaled data  
NRMSE = sqrt(mdifffsq/mscaledsqS)% Normalized Root Mean  
Square Error
```

```
% [4] correlation
```

```
xx=rS-mean(rS);  
yy=origdata-mean(origdata);  
Cor=sum(xx.*yy)/((sum(xx.^2)*sum(yy.^2))^0.5)
```


A-2 Computer program for hiding secret data inside audio signal using Least Significant Bit (LSB) method in Transform Domain using Discrete Wavelet Transform (DWT).

```
clc
clear all
tic
W=randperm(255);
index=[];
wname= 'db10';
depth=2;% level;
Lenc=0;
len_speech=18000; %%% length of speech signal
%%%% read the cover speech signal
fid=fopen('sound6.wav','rb');
[x]=fread(fid,len_speech,'int16');
origdata=x(250:end);
origdata(length(origdata)+1:2*length(origdata))=x(250:end);

% read the image
x_i=imread('students.jpg');
y_i=double(rgb2gray(x_i));
[r c]= size(y_i);
y_i_v=reshape(y_i,1,r*c);% vector of the image

y_i_b=dec2bin(y_i_v) ;% binary
[a1 a2]=size(y_i_b);
im=reshape(y_i_b,1,a1*a2);

len_speech=length(origdata);
len_frame=255;
nf=floor(len_speech/len_frame); %% no. of frames required
index=1;
for tt=0:nf-1
    %%% framing into blocks of length =len_frame
```

```
xf=origdata(1+tt*len_frame:len_frame+tt*len_frame);  
[c,l] = wavedec(xf,depth,wname);  
Wout=c;  
for kk=1:length(W)  
  
    yd=c(W(kk))*100;
```

```

sign_yd=sign(yd);

xb=dec2bin(abs(yd),16);
if index < (a1*a2)
    xb(16)=im(index) ; % hid information in the LSB
    index=index+1;
end
Wout(W(kk))=sign_yd*bin2dec(xb)/100;

end

rC=Wout;

xf=waverec(rC,l,wname);

for k1=1:length(xf)
rS(k1+tt*len_frame)=xf(k1);
end

end
origdata=origdata(1:length(rS));

rS = rS';%(1:length(origdata));

% [1] Signal to Noise Ratio

sqdata = origdata.^2; % Square of original speech signal
sqrS = rS.^2; % Square of reconstructed signal
msqdata = mean(sqdata); % Mean square of speech signal
sqdiff = (sqdata-sqrS); % Square difference
msqdiff = mean(sqdiff); % Mean square difference
SNR = 10*log10(abs(msqdata/msqdiff)) % Signal to noise ratio

```

`%[2] Peak Signal to Noise Ratio`

`N = length(rS); % Length of reconstructed signal`

`X = max(abs(sqdata)); % Maximum absolute square of original
signal`

`diff = origdata - rS; % Difference signal`

`enddiff = (norm(diff))^2; % Energy of the difference between the`

```
% original and reconstructed signal
PSNR = 10*log10((N*(X^2))/endiff) % Peak Signal to noise ratio
```

```
%[3] Normalised Root Mean Square Error
```

```
diffsq = diff.^2; % Difference squared
mdiffsq = mean(diffsq); % Mean of difference squared
mdata = mean(origdata); % Mean of original speech signal
scaledsqS = (origdata - mdata).^2; % Squared scaled data
mscaledsqS = mean(scaledsqS); % Mean of squared scaled data
NRMSE = sqrt(mdiffsq/mscaledsqS)% Normalized Root Mean
Square Error
```

```
% [4] correlation
```

```
xx=rS-mean(rS);
yy=origdata-mean(origdata);
Cor=summation(xx.*yy)/((summation(xx.^2)*summation(yy.^2))^0.5)
```

A-3 Computer program for extracting secret message from audio signal in Transform domain using Discrete Wavelet Transform (DWT).

```
clc
clear all
tic
index=[];
wname='haar';
depth=1;
Lenc=0;
len_speech=30000; %%% length of speech signal
%%%% read the cover speech signal
fid=fopen('sound6.wav','rb');
%fseek(fid,20,0);
[x]=fread(fid,len_speech,'int16');
origdata=x(250:end);
origdata(length(origdata)+1:2*length(origdata))=x(250:end);

% read the image
x_i=imread('Dock.jpg');
y_i=rgb2gray(x_i);
[rr cc]= size(y_i);
y_i_v=reshape(y_i,1,rr*cc);% vector of the image

y_i_b=dec2bin(y_i_v) ;% binary
[a1 a2]=size(y_i_b);
im=reshape(y_i_b,1,a1*a2);
imr=im;
len_speech=length(origdata);
len_frame=10;
nf=floor(len_speech/len_frame); % no. of frames required
index=1;
% nf=1;
for tt=0:nf-1
    %%% framing into blocks of length =len_frame
```

```
xf=origdata(1+tt*len_frame:len_frame+tt*len_frame);  
[c,l] = wavedec(xf,depth,wname);
```

```
Wout=c;  
sum=l(1);
```

```

%sum=0;
%Wa=c(1:l(1));
for kk=1:length(c) % take only detail of information
    yd=c(kk);
    sign_yd=sign(yd);

    xb=dec2bin(abs(yd),16);
    if index < (a1*a2)
        xb(16)=im(index) ; % hid information in the LSB
        index=index+1;
    end

    xd=bin2dec(xb);

Wout(kk) =xd*sign_yd;

end

% extracting image from sound files
xr=waverec(Wout,l,wname);
[cr,l] = wavedec(xr,depth,wname);

for kk=1:length(index)
    yd=c(kk);
    xb=dec2bin(abs(yd),16);
    imr(kk)=xb(16);
end

for k1=1:length(xf)
rS(k1+tt*len_frame)=xr(k1);
end

end

```



```
imr2=reshape(imr,a1,a2);  
imr2b=bin2dec(imr2) ;% binary  
im_r=reshape(imr2b,rr,cc);% reconstructed image  
%%  
% y_i original image
```

```
% im_r extracting image

subplot(2,1,1)
imshow(y_i);
subplot(2,1,2)
imshow(im_r/256)

origdata=origdata(1:length(rS));

rS = rS';%(1:length(origdata));
```

الخلاصة

الكتابة الخفيه (Steganography) هو فن اخفاء المعلومات بطرق معينه بحيث يصعب اكتشافها. الرساله المشفره تؤدي الى الشك بينما الرساله الغير مرئيه لا تؤدي الى الشك. في فن الكتابة الخفيه الرقيه تستخدم رساله او بيانات معينه تعرف بالحاويه (Container) او الغطاء (Cover) لاختفاء بيانات او رسائل اخرى تسمى بالسريه (Secret) داخله.

النظام المقترح في هذه الاطروحه هو نظام اخفاء صوره داخل صوت. ثم تنفيذها في النظام المقترح (الاخفاء في البت الاخير LSB) في مجال الوقت وفي مجال التحويل الموجه ومجال الجيب تمام.

طريقة (LSB) نفذت في مجال الوقت حيث ان البيانات السريه تم اخفاؤها مباشرة في بيانات الغطاء ونفذت في مجال التردد الذي نتج باستخدام التحويل الموجه (DWT) حيث هن البيانات السريه يتم اخفاؤها في معاملات التحويل الموجه لبيانات الغطاء.

النظام المقترح يتم اختباره باستخدام مقاييس معوليه قياسييه هي متوسط الخطأ المربع (MSE) ومتوسط جذر الخطأ المربع (NRMSE) ونسبة الاشاره الى الضوضاء (PSNR) والارتباط (COR). كل المقاييس المعوليه التي استخدمت في اختبار النظام المقترح أظهرت قيم جيده ل (PSNR). اما البيانات المسترجعه فكانت بالضبط هي نفسها البيانات السريه التي تم اخفاؤها اذا كانت طريقه الاخفاء بالبت الاخير (LSB) في مجال التحويل الموجه هي المستخدمه بينما يظهر بعض الاختلاف غير المحسوس اذا كانت طريقه الاخفاء في البت الاخير (LSB) في مجال الوقت هي المستخدمه.

شكر وتقدير

تتقدم الباحثه بالشكر والامتنان للأستاذ المساعد الدكتور رجاء الدين عبد خالد لما بذله من جهود قيمه تمثلت بالمتابعة والتوجيهات الدقيقة طوال فترة العمل, والتي كان لها الدور في إظهار البحث بالصورة التي ظهر بها.

كما تود الباحثه أن يتقدم بالشكر والامتنان لكل من ساهم بتسهيل إنجاز هذا العمل في قسم الهندسة الالكترونية والاتصالات وخاصة السيد رئيس القسم الدكتور جابر سلمان عزيز والسيد مقرر الدراسات العليا الدكتور قصي لطفي عباس.

كما وتشكر الباحثه السيد عميد كلية الهندسة في جامعة النهريين الأستاذ الدكتور محسن جبر جويج على جهوده القيمة التي بذلها في إنجاز مسيرته الدراسية خلال سني الدراسة الاولى والعليا.

وأخيرا تشكر الباحثه المهندس فاضل صاحب في كلية الهندسة الجامعة المستنصرية على تقديمه المساعدة القيمة في إكمال البحث.

الباحثه

ريام مجيد زعال

نظام إخفاء المعلومات الصوتي المبني على معالجة الاشارة الرقمية

رسالة

مقدمه إلى كلية الهندسة في جامعة النهريين
وهي جزء من متطلبات نيل درجة ماجستير علوم في
الهندسة الالكترونية والاتصالات/الدوائر والمنظومات الالكترونية

من قبل

ريام مجيد زعال

(بكالوريوس علوم في الهندسة الالكترونية والاتصالات 2005)

1430

2009

ربيع الاول

اذار