Ministry of Higher Education and
Scientific Research
University of Baghdad
College of Science
Computer Science Department

Steganographic Techniqe Based on Wavelet Transform

A Dissertation Submitted to
The College of Science /University of Baghdad
In Partial Fulfillment of the Requirements
For the Degree of Master in
Computer Science

Done By

Inteasar Y. K. Al-Khzraji

B.SC In Computer Science 1997

February (2004)

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

أَقرَأْ بِاسْمِ رَبِّكَ الَّذِي خَلَقَ ﴿١﴾ خَلَقَ الْإِنسَانَ
مِـــنْ عَلَقٍ ﴿٢﴾ اقْرَأْ وَرَبُّكَ الْأَكْرَمُ ﴿٣﴾ الَّذِي عَلَّمَ
بِالْقَلَمِ ﴿٤﴾ عَلَّمَ الْإِنسَانَ مَا لَمْ يَعْلَمْ ﴿٥﴾

صدق الله العظيم

(سورة العلق)

Supervisor's Certification

I certify that the preparation of this project was made under my supervisions at the college of science, university of Baghdad in partial fulfillment of the requirements needed to word the degree of Master of Science in Computer ***(Steganographic Technique Based on Wavelet Transform)***.

Signature:
Advisor: Dr. Saleh M. Ali
Title: Professor
Date: 5/ 4 / 2004

Certification of the head of the department

In view of the available recommendation, I forward this dissertation for debate by the examination committee.

Signature:
Name: M. Sc Makia K. Hamad
Title: Assistant Professor
Address: Baghdad University
Date: ١٤/ 4 / 2004

Certification

We certified that, after reading this Project, and examining the student "Inteasar Y. K. Al-Khzraji", think, as an Examining Committee, it is adequate for the award of the degree of Master in Computer Science.

Signature:

Name: Prof. Saleh Mahdi Ali

Date: 5 / 4 / 2004

(Supervisor)

Signature: Loay

Name: Dr. Loay E. Jeorge

Date: 20 / 4 / 2004

(Member)

Signature:

Name: Dr. Lubna R. Hussain

Date: 5 / 4 / 2004

(Member)

Approved by the University.

Signature: Taleb

Name: Prof. A. M. Taleb

Title: The Dean of College of Science / University of Baghdad

Date: 21 / 4 / 2004

Dedication

To my mother …

Who supports me along my life

To my father …

Who encourage me to reach this level

To my brothers and sisters …

For their love and help

To all my friends …

To everyone who makes science the way that leads to the human's happiness.

Acknowledgement

Praise to Allah, Lord of the words. May the blessing and peace of Gad be upon the most honored prophet and upon his kind and pure folk.

No words can appreciate my family, without their help, patience, and support this work would not have been done.

I would like to express my gratitude and thankfulness to my supervisor Dr. Saleh Muhdi for his valuable advice and continuous encouragement throughout the work of this project.

Special thanks to the staff of the department of computer science, University of Baghdad, for their help and support.

I also wish to give special thanks to my friend Miss. Maysaa Hossam, and to my colleague Mr. Ibrahim nadear.

Abstract

Steganography is the art of hiding and transmitting data through apparently innocuous in an effort to conceal the existence of data. Image steganography is adopted in this work.

The proposed stego-system uses the transform domain in the steganography process to increase the robustness by inserting the low frequency component of the signature image in the high frequency component of the host image, using Haar-Wavelet Transform. For security purposes, the coefficients of the transformed signature image (LL subband) are normalized by dividing the LL coefficients of the signature image subband by certain value, the value by which the LL coefficients divided is tested to yield an acceptable PSNR in both stego and reconstructed image. Then the stego-key is used, in which the LL normalized coefficients were inserted in an inverse order at the HH location of the host image.

The imperceptibility of the resulted stego-image is assessed by using Peak-Signal-to-Noise Ratio (PSNR) measure. The stego-image, under certain parameters selection, has excellent quality (PSNR above 30 dB). In the other hand, the reconstructed image has an acceptable quality but not the same as of the stego-image because of the normalization process that is used in the embedding process. It should be noted that; the size of the signature image must be equal to or less than the size of the host image.

Contents

Chapter One: Introduction

Chapter Two: Information Hiding

Chapter Three: Discrete Image Transforms

Chapter Four: System Implementation

Chapter Five: Conclusion and Suggestion for Future Work

Chapter One

Introduction

Chapter One

Introduction

1.1 Introduction

It is often thought that communications may be secured by encrypting the traffic, but this has rarely been adequate in practice. Æneas the Tactician, and other classical writers, concentrated on methods for hiding messages rather than for enciphering them [1]; although modern cryptographic techniques started to develop during the Renaissance, we find in 1641 that Wilkins still preferred hiding over ciphering [2] because it arouses less suspicion. This preference persists in many operational contexts to this day. For example, an encrypted e-mail message between a known drug dealer and somebody not yet under suspicion, or between an employee of a defence contractor and the embassy of a hostile power, has obvious implications. So the study of communications security includes not just encryption but also traffic security, whose essence lies in hiding information. This discipline includes such technologies as: spread spectrum radio, which is widely used in tactical military systems to prevent transmitters being located; temporary mobile subscriber identifiers, used in digital phones to provide users with some measure of location privacy; and anonymous remailers, which conceal the identity of the sender of an e-mail message [3].

An important sub discipline of information hiding is steganography. While cryptography is about protecting the content of messages, Steganography is about concealing their very existence; it comes from Greek roots literally means "covered writing", and it is usually interpreted to mean hiding information in other information. Examples include sending a message to a spy by marking certain letters in a newspaper using invisible ink, and adding sub perceptible echo at certain places in an audio recording.

Until recently, information-hiding techniques received much less attention from the research community and from industry than cryptography, but this is changing rapidly (Table 1), and the first academic conference on the subject was organized in 1996 [4]. The main driving force is concern over copyright; as audio, video, and other works become available in digital form, the ease with which perfect copies can be made may lead to large-scale unauthorized copying, and this is of great concern to the music, film, book, and software publishing industries. There has been significant recent research into digital "watermarks" (hidden copyright messages) and "fingerprints" (hidden serial numbers); the idea is that the latter can help to identify copyright violators, and the former to prosecute them.

Table (1-1) Number of Publications on Digital Watermarking During the Past Few Years According to INSPEC, January 1999 (Courtesy of J.-L. Dugelay [5])

Year	**1992**	**1993**	**1994**	**1995**	**1996**	**1997**	**1998**
Publications	2	2	4	13	29	64	103

In another development, the DVD consortium has called for proposals for a copyright marking scheme to enforce serial copy management. The idea is that DVD players available to consumers would allow unlimited copying of home videos and time-shifted viewing of TV programs but could not easily be abused for commercial piracy. The proposal is that home videos would be unmarked, TV broadcasts marked "copy once only," and commercial videos marked "never copy"; compliant consumer equipment would act on these marks in the obvious way [6], [7].

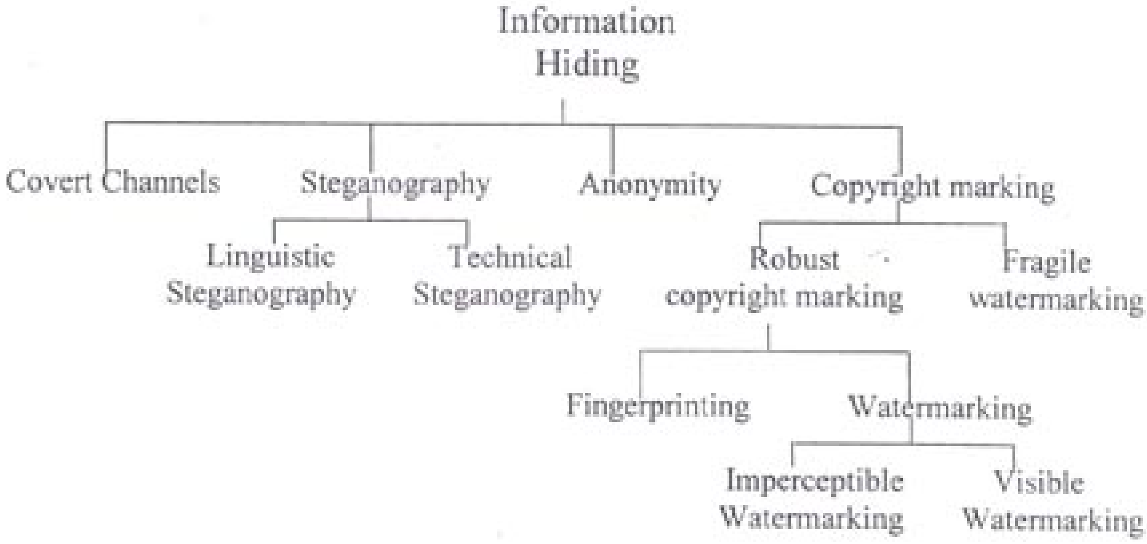


Figure (1-1): A classification of information-hiding Techniques based on [8].

There are a number of other applications driving interest in the subject of information hiding (Figure 1-1).

- Military and intelligence agencies require unobtrusive communications. Even if the content is encrypted, the detection of a signal on a modern battlefield may lead rapidly to an attack on the signaler. For this reason, military communications use techniques such as spread spectrum modulation or meteor scatter transmission to make signals hard for the enemy to detect or jam.
- Criminals also place great value on unobtrusive communications. Their preferred technologies include prepaid mobile phones, mobile phones which have been modified to change their identity frequently, and hacked corporate switchboards through which calls can be rerouted.

- Law enforcement and counter intelligence agencies are interested in understanding these technologies and their weaknesses, so as to detect and trace hidden messages.
- Recent attempts by some governments to limit online free speech and the civilian use of cryptography have spurred people concerned about liberties to develop techniques for anonymous communications on the Internet, including anonymous remailers and Web proxies.
- Schemes for digital elections and digital cash make use of anonymous communication techniques.
- Marketeers use e-mail forgery techniques to send out huge numbers of unsolicited messages while avoiding responses from angry users.

1.2 Methods for Hiding Information

The onset of computer technology and the Internet has given new life to steganography and the creative methods with which it is employed. Computer-based steganographic techniques introduce changes to digital carriers to embed information foreign to the native carriers. Since 1995, interest in steganogrphic methods and tools as applied to digital media has exploded.

Steganography encompasses methods of transmitting secret messages in such a manner that the existence of the embedded message is undetectable. Carriers of such messages may resemble innocent sounding text, disks and storage devices, network traffic and protocols, the way software or circuits are arranged, audio, images, video, or any other digitally represented code or transmission. These provide excellent carriers for hidden information and many different techniques have been introduced [9].

1.2.1 Hiding in Text

Documents may be modified to hide information by manipulating position of lines and words. HTML files can be use to carry information since adding spaces, tabs, " invisible " characters, and extra line breaks are ignored by web browsers. The "extra" spaces and lines are not perceptible until revealing the source of the web page.

1.2.2 Hiding in Disk Space

Other ways to hide information rely on finding unused space that is not readily apparent to an observer. Taking advantage of unused or reserved space to hold covert information provides a means of hiding information without perceptually degrading the carrier. The way operating systems store files typically results in unused spaces that appears to be allocated to files. This "allocated" but available space is known as slack space.

1.2.3 Hiding in Network Packets

Characteristics inherent in network protocols can be taken advantage of to hide information. An uncountable number of data packets are transmitted daily over the internet. Any of which can provide an excellent cover to communication channel.

1.2.4 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 the creator.

1.2.5 Hiding in Audio and Images

Many different methods for hiding information in audio and images exist. These methods may include hiding information in unused space in files headers to hold "extra" information. Embedding techniques can range from the placement of information in imperceptible levels (noise), manipulation of compression algorithms, to the modification of carrier properties. In audio small echoes or slight delays can be added or subtle signals can be masked by sounds of higher amplitude.

The messages can be transmitted in alossy DCT-based video compression scheme over an ISDN (Integrated Services Digital Network) line used for video conferencing. Up to 8 kilobits could be embedded without degrading the signal to the point that the secret communication becomes apparent.

In images, modifying properties such as luminance, contrast, or colors can be used. These methods hide information in audio and images with virtually no impact to the human sensory system [9].

1.3 Uses of Steganography

Steganography can be used anytime you want to hide data. There are many reasons to hide data but they all boil down to the desire to prevent unauthorized persons from becoming aware of the existence of a message. In the business world steganography can be used to hide a secret chemical formula or plans for a new invention. Steganography can also be used for corporate espionage by sending out trade secrets without anyone at the company being any the wiser. Steganography can also be used in the non-commercial sector to hide information that someone wants to keep private. Spies have used it since the time of the Greeks to pass messages undetected. Terrorists can also use steganography to keep their communications secret and to coordinate attacks [10].

1.4 Steganography and Wavelet Transform

Wavelet is mathematical functions that cutup data into different frequency components, and then study each component with a resolution matched into its scale. They have advantages over traditional Fourier methods in analyzing physical situation where the signal contains discontinuities and sharp spikes [11].

Wavelet were developed independently in the filed of mathematics, quantum physics, electrical engineering, and seismic geology. Interchanges between these fields during the last years have led to new wavelet applications such as image compression, turbulence, human vision, radar, and earthquake prediction [12].

Image compression based on wavelet transform was given more interest in the recent years by those who are working in data compression because of its improvement over the existing methods like high compression efficiency, the ability to handle large images, and progressive image transmission [13].

JPEG 2000, which is a new wavelet-based standard for the compression of still images, is one of the important attacks against image steganography because it gives little degradation on stego image at high compression ratios but at the same time it may make large damage on the embedded image [14].

Understanding the types of attacks that can be executed against steganography led to discovering countermeasures to those attacks. The purpose of the countermeasure is to thwart successful attacks. Such countermeasures are useful for creating more robust steganography [15].

Possible countermeasures to deter the effect of applying JPEG 2000 to the stego image may include the use of the wavelet transform itself to embed data in perceptually more significant part of a cover image to make the removal of the embedded data more difficult. In addition to this advantage, the multiresolution aspect of wavelets is helpful in managing a good distribution of the data in the cover in terms of robustness versus visibility [14].

At this point, it is expected for the next years that the wavelet transform may be the main tool in the image steganography that based on transform domain techniques.

1.5 Image Processing

Image processing is computer imaging where the application involves a human being in the visual loop. In other word, the images are to be examined and acted upon by people. For these types of applications, we require some understanding of how the human visual system operates. The major topics within the filed of image processing include *image restoration*, *image enhancement*, and *image compression*. Image analysis is often used as preliminary work in the development of image processing algorithms, but the primary distinction between computer vision and image processing is that the output image is to be used by a human being [16].

Image restoration is the process of taking an image with some known, or estimated, degradation, and restoring it to its original appearance. Image restoration is often used in the filed of photography or publishing where an image was somehow degraded but needs to be improved before it can be printed.

Image enhancement involves taking an image and improving it visually, typically by taking advantage of the human visual systems response. One of the simplest and often most dramatic enhancement techniques are to simply stretch the contrast of an image.

Image compression involves reducing the typically massive amount of data needed to represent an image. This is done by eliminating data that are visually unnecessary and by taking advantage of the redundancy that is inherent in most images.

1.6 Image Representation

The human visual system receives input images as a collection of spatially distributed light energy; this form is called an optical image. Optical images are the types we deal with everyday. We know that these optical images are represented as video information in the form of analog electrical signals and have seen how these are sampled to generate the digital image I(r,c).

The digital image types are [16]:

1- Binary images.

2- Gray-scale images.

3- Color images.

1.6.1 Binary images

Binary images are the simplest type of images and can take on two values, typically black and white, or '0' and '1'. A binary images is referred to as a 1-bit/pixel image because it takes only 1 binary digit to represent each pixel. These types of images are most frequently used in computer vision applications where the only information required for the task is general shape, or outline, information. For example, to position robotic gripper to grasp an object, to check a manufactured object for deformation, for facsimile (FAX) images, or in optical character recognition (OCR).

1.6.2 Gray-Scale Images

Gray scale images are referred to s monochrome, or one- color, images. They contain rightness information only, no color information. The number of bits used for each pixel determines the number of different brightness levels available. The typical image contains 8 bit/pixel data, which allows us to have 256(0-255) different brightness (gray) levels.

1.6.3 Color Images

Color images can be modeled as three-band monochrome image data, where each band of data corresponds to a different color. The actual information stored in the digital image data is the brightness information in each spectral band. When the image displayed, the corresponding brightness information is displayed on the screen by picture elements that emit light energy corresponding to the particular color. Typical or images are represented as red, green, and blue or RGB images. Using the 8-bit monochrome standard as a model, the corresponding color image would have 24 bits/pixel 8-bits for each of the three-color band (red, green, and blue) [16].

1.7 Literature Survey

- In 2002, A. M., Al-jashammi presents image in steganography system which embeds a gray scale image in another one, using wavelet transform. In this system the wavelet transform and the sorting process are used to cluster both the cover image and the embedded image according to their subbands energies to guarantee that the embedded image will be inserted in the low frequency component of the cover image in order to reduce the effect of the attacker [17].
- In 2000, L. Z. Avedissian presents image in image steganography system (denoted by IISS) which embeds a gray scale image into a gray or color image. The proposed system uses the substitution technique to embed image of size 100×120 in image of size 640×480 making the position of the embedded image pixels as a secret key [18].

- In 2000, N. K. Abdulaziz presents robust watermarking scheme based on wavelet transform. This watermarking system embeds the signature image, which is source coded using vector quantization, in the low band of the cover image. Channel coding is used to improve the system performance [19].
- In 2000, S. Areesponga presents a stegosystem using wavelet transform. In this system the data is embedded in the sign of the high frequency coefficients of the cover image in attempt to trade off between the robustness of the embedded data and the invisibility of the stegoimage [20].
- In 2001, U. I. Al-dilaimy presents text in image steganography system (denoted by TISS). She also uses the substitution technique to embed approximately 500 characters in gray scale image of size 640×480 [21].
- In 2001, H. H. Marza presents a stegosystem using transform domain techniques based on cosine transform to embed a text in gray scale image by swapping the middle frequency coefficients according to the embedding message. The stegosystem embeds"1" bit of the embedded message in "64" byte of the cover image [22].

1.8 The Aim of the Work

The aim of the present work is to design stegosystem. This stegosystem provides secret image hiding in a host image using transform techniques. Wavelet transform is used as the transform method. The hiding information is manipulated in such a way to keep a host image without any noticeable degradation.

1.9 Dissertation Outline

Beside chapter one , the Introduction, the Dissertation consist of another four chapters, these are:

- Chapter two which contain background a bout information hiding in general and its two areas Digital watermarking and steganography. It also describes types of steganogrphy systems, Steganographic techniques and finally it describes the Steganalysis.
- Chapter Three describe the Discrete Transform Domain and its equation in general, Fourier Transform, Cosine Transform, Walsh Hadamard Transform, and Wavelet Transform.
- Chapter four describe the implementation of the program and viewing the menus that are used in the proposed system in addtion to viewing four groups of images as a results of the system inplementation.
- Chapter five demonstrates the concluding remarks on the proposed stegosystem and presents suggestions for future work.

Chapter Two

Information Hiding

Chapter Two

Information Hiding

2.1 Introduction

Information-hiding techniques have recently become important in a number of application areas. Digital audio, video, and pictures are increasingly furnished with distinguishing but imperceptible marks, which may contain a hidden copyright notice or serial number or even help to prevent unauthorized copying directly.

With the rapid development of Internet technologies, the amount of information sent and received electronically is increasing greatly. As the technology of transmitting information on network in secure, the importance of information security came to be recognized widely.

Information hiding is a field of information security, and it includes methods creating covert channel where specification of transceiver is difficult, methods hiding the existence of information itself, and methods for digital watermarking. These technologies have lately attracted considerable attention as solution to copyright problems and the protecting method for communication privacy [23].

There are two area of research, which are generally referred to as "information hiding". Watermarking that is originated from the need for copyright protection of digital media, whereas Steganography studies methods to make communication invisible by hiding secrets in innocuous message [14].

2.1.1 Digital watermarking

The proliferation of digitized media (audio, image and video) is creating a pressing need for copyright enforcement schemes that protect copyright ownership. Conventional cryptographic systems permit only valid key holders access to encrypted data, but once such data is decrypted there is no way to track its reproduction and retransmission. Conventional cryptographic therefore provides little protection against data piracy, in which publisher is confronted with unauthorized reproduction of information.

A digital watermark is intended to complement cryptographic processes. It is a visible, or preferably invisible, identification code that is permanently embedded in the data, that is, it remains present within the data after any decryption process [24].

All watermarking methods show the same generic building blocks: a *Watermark Embedding System* and *Watermark Recovery System*. Figure (2-1) shows the generic watermarking process. The input to the scheme is the *Watermark*, the *Cover-Data* and an optional *public* or *secret key K*. The watermark can be any nature such as a number, text, or an image. The key may be used to enforce security. The output of the watermarking scheme is the *Watermarked Data*. The generic watermark recovery process is depicted in Figure (2-2). Input to the scheme are the *Distorted Data* (assuming that the watermarking system is attacked), the secret or public key, and, depending on the method, the original data and/or the original watermark. The output is either the recovered watermark or some kind of confidence measure indicating how likely it is for the given watermark at the input to be present in the distorted data under inspection [14].

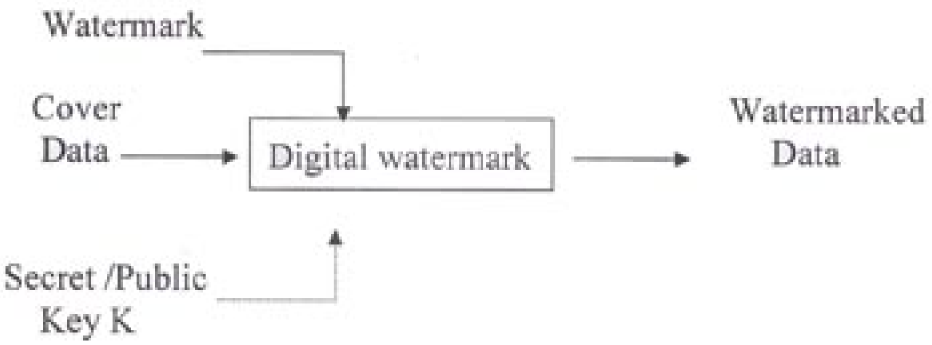


Figure (2-1) Generic Watermarking Scheme

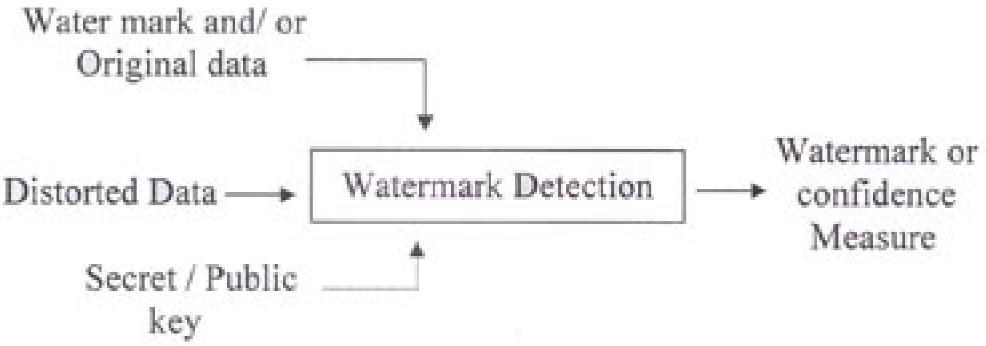

Water mark and/ or Original data
Distorted Data
Watermark Detection
Watermark or confidence Measure
Secret / Public key

Figure (2-2) Generic Watermark Recovery Scheme

Watermarking Requirements

- Imperceptibility :
  - The modifications caused by watermark embedding should be below the perceptible threshold.
- Robustness :
  - The ability of the watermark to resist distortion introduced by standard or malicious data processing.
- Security :
  - A watermark is secure if knowing the algorithms knowing for embedding and extracting does not help unauthorized party to detect or remove the watermark.
- Payload :
  - The amount of information that can be stored in a Watermark.

- Informed (nonoblivious , or private) Watermarking:
    - The original unwatermarked cover is required to perform the extraction process.
- Blind (oblivious, or public) Watermarking:
    - The original unwatermarked cover is not required to perform the extraction process [25].

2.1.2 Steganography

In conventional cryptography, even if the information contents are protected by encryption, the existence of the encrypted communications is known. In view of this, Steganography provides an alternative approach in which it conceals even the evidence of encrypted message. Generally, Steganography is defined as the art and science of communication in a cover fashion. It utilize the typical digital media such as text ,image ,audio, video and multimedia as a carrier (called host or cover signal) for hiding private information in such a way that the third parties (unauthorized person) cannot detect or even notice the presence of the communication[20].

Most applications of Steganography follow one general principle, illustrated in the Figure (2-3), *Alice*[1] , who wants to share a secret massage M to *Bob*, *randomly* chooses, using the private random source *r*, a harmless message, called *cover-object* C, which can be transmitted to Bob without raising suspicion, and embeds the secret message into C, probably by using a key, called *Stego-key* K. *Alice* therefore changes the cover C to the *Stego-object* S. This must be done in a very careful way, so that a third party, knowing only the apparently harmless message S, cannot detect the existence of the secret. In a "perfect" system a normal cover should not be distinguishable from the Stego-

[1] In the filed of the cryptography, communication protocols usually involve tow fictional characters named *Alice* and *Bob* or use a name whose first character matches the first letter of their role(e.g.*Wendy* the warden).

object, neither by a Human Visual System (HVS) nor by a computer looking for statistical pattern. *Alice* then transmits S over an insecure channel to *Bob* and hopes that *Wendy* will not notice the embedded message. *Bob* can reconstruct M since he knows the embedding methods used by *Alice* and has access to the key K used in the embedding process.

A third person watching the communication should not be able to decide whether the sender is active in the sense that he sends covers containing secret rather than covers without additional information. Thus, *the security of invisible communication mainly depends on the inability to distinguish cover-objects from stego-objects.*

Obviously a cover should never be used twice, since an attacker who has access to two versions of one cover can easily detect and possibly reconstruct the message. To avoid accidental reuse, both sender and receiver should destroy all covers they have already used for information transfer [14].

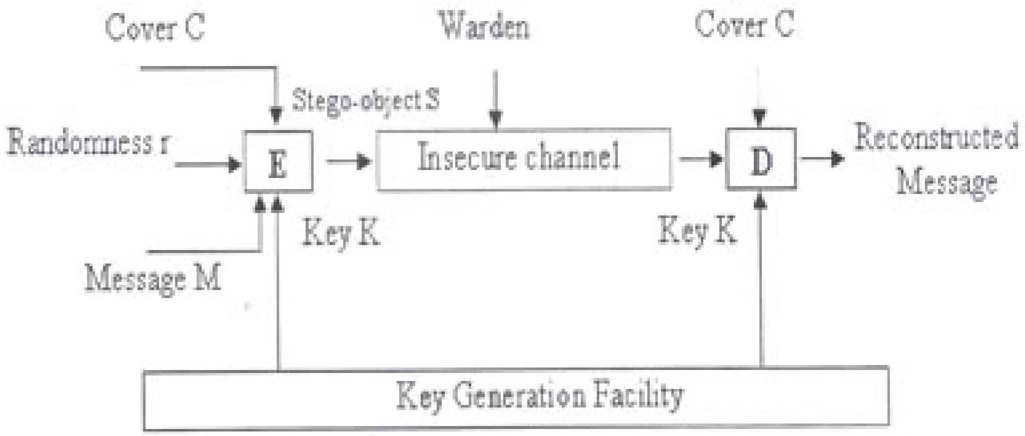


Figure (2-3)
Schematic Description of Steganogrphy

2.1.3 Watermarking Vs. Steganography

The purpose of both watermarking and steganography is to hide a message in a carrier signal, but the information hidden by a watermarking system is always associated to the digital object to be protected or to its owner while steganogrphic systems just hide any information. The robustness criteria are also different, since steganography is mainly concern with detection of the hidden message while watermarking concerns potential removal by a pirate.

Steganography communications are usually point to point (between sender and receiver) while watermarking techniques are usually one-to-many.

Furthermore, in watermarking the cover is the transmitted data and the hidden information just for authentication purposes, while in steganography the hidden information is the transmitted data and the cover just to hide it [14],[26].

2.2 Types of Steganography Systems

One could categorize the steg-system according to their stego-key used in the embedding process to three: *pure* steganography, secret key steganography and public key steganography.

2.2.1 Pure steganography

A secret key system which does not require the prior exchange of some secret information (like stego key) called pure steganography. Both the sender and receiver must have access to the embedding and extracting algorithm, but the algorithm should not be public [14].

In practice, the pure steganographic system is not secure enough because the security of the system depends on stego object imperceptibility and the algorithm secrecy so that violates *Kerckhoffs* principle[2] [27], so the stego-system based on key give a better performance form the securities viewpoint but of course not from complexity one.

2.2.2 Secret key steganography

A secret key steganogrphy system is similar to a symmetric cipher. The sender chooses a cover and embeds the secret message using a secret key. If the key used in the embedding process is known to the receiver, he can reverse the process and extract the secret massage. Anyone who dos not know the secret key, depending on the security of the key, should not be able to obtain evidence of the encoded information. Again, the cover and the stego-object should be perceptually similar [14].

As a price to this increase in the system security, the transmission of additional secret information subverts the original intention of the invisible communication. Furthermore, how to ensure that the same secret key is available to both the transmitter and receiver [28]. So to overcome these problems, a public key steganography is used.

2.2.3 Public Key Steganography

As in public key steganography [28], public key steganography dose not rely on the exchange of a secret key. Public key steganography systems require the use of two keys, one private and one public; the public key is used in the embedding process, the secret key is used to reconstruct the secret message.

One way to build a public key steganography utilized the fact that decoding function in a steganography system can be applied to any cover,

[2] In 1883, Augest Kerckhoffs put his principle which states that the method used to encipher data is known to the opponent, and that security must be lie in the choice of key.

whether or not it already contains a secret message. In the later case, a random element will be the result, so called "natural randomness" of the cover. If one assumes that this natural randomness is statistically indistinguishable from cipher text produce by some public key cryptosystem a secure steganogrphy system can be built by embedding cipher text rather than unencrypted message[29].

2.3 Steganographic Techniques:

Many different steganographic methods have been proposed during the last few years, most of them can be seen substitution system. Such methods try to substitute redundant part of the signal with a secret message; their main disadvantage is the relative weakness against cover modification. Recently, the development of new robust watermarking techniques led to advances in the construction of robust and secure steganography systems. Therefore, some of the methods are strongly related to the watermarking techniques [14].

There are several approaches in the classifying steganographic techniques. One of these approaches is to categorize them according to the cover modifications applied in the embedding process. Mainly, steganographic techniques may be grouped into five categories as follows [14]:

- ***Substitution Techniques:*** substitute redundant parts of a cover with a secret massage.
- ***Transform Domain Techniques***: Embed secret information in a transform space of the signal.
- ***Spread Spectrum Techniques:*** Adopt ideas from spread spectrum communication.

whether or not it already contains a secret message. In the later case, a random element will be the result, so called "natural randomness" of the cover. If one assumes that this natural randomness is statistically indistinguishable from cipher text produce by some public key cryptosystem a secure steganogrphy system can be built by embedding cipher text rather than unencrypted message[29].

2.3 Steganographic Techniques:

Many different steganographic methods have been proposed during the last few years, most of them can be seen substitution system. Such methods try to substitute redundant part of the signal with a secret message; their main disadvantage is the relative weakness against cover modification. Recently, the development of new robust watermarking techniques led to advances in the construction of robust and secure steganography systems. Therefore, some of the methods are strongly related to the watermarking techniques [14].

There are several approaches in the classifying steganographic techniques. One of these approaches is to categorize them according to the cover modifications applied in the embedding process. Mainly, steganographic techniques may be grouped into five categories as follows [14]:

- ***Substitution Techniques:*** substitute redundant parts of a cover with a secret massage.
- ***Transform Domain Techniques***: Embed secret information in a transform space of the signal.
- ***Spread Spectrum Techniques:*** Adopt ideas from spread spectrum communication.

- ***Statistical Techniques:*** Encode information by changing several statistical properties of cover image.
- ***Distortion Techniques:*** Store information by signal distortion and measure the deviation from the original cover in the decoding step.
- ***Cover Generation Techniques:*** Encode information in the way a cover is generated.

2.3.1 Substitution Techniques

Basic substitution systems try to encode secret information by substituting insignificant parts of the cover by secret message bits, the receiver can extract the information if he has Knowledge of the positions where secret information has been embedded. Since only minor modification is made in the embedding process, the sender assumes that they will not be noticed by an attacker.

2.3.1.1 Least Significant bit substitution:

The process consists of choosing a subset$\{j_1 , \ldots j_{l(m)} \}$, where $l(m)$ is the length of the message, of the cover elements and performing the substitution operation $C_{ji} \leftrightarrow m_i$ on them, which exchanges the LSB of the C_{ji} by m_i (m_i can be either be 1 or 0). In the extraction process, the LSB of the selected cover element are extracted and lined-up to reconstruct the secret message. In order to be able to decode the secret message, the receiver must have access to the sequence of element indices used in the embedding process [14].

2.3.1.2 Pseudorandom permutations:

If all cover bits can be access in the embedding process, the cover is a (*random access cover)*; the secret message bits can be distributed randomly over the whole cover. This technique further increases the complexity for the attacker, since it is not guaranteed that the subsequent message bits are embedded in the same order.

The embedding process starts with creating, using pseudorandom number generator, a sequence $j_{1,} \ldots, j_{l(m)}$ of element indices and store the k_{th} message bit in the element with the index j_k. Note that one index could be appearing more than once in the sequence, so collusion will be occurred. If the message is quit short compared with a number of cover element, the probability of collisions is negligible and that the corrupted bits could be reconstructed using error correcting code [14].

2.3.1.3 Image Downgrading:

Image downgrading is a special case of a substitution system in which images act both as secret messages and covers. Given a cover-image and a secret image of equal dimensions, the sender exchanges the four least significant bits of the cover's grayscale (or color) values with the four most significant bits of the secret message. The receiver extracts the four least significant bit out of the stego-image, thereby gaining access to the most significant bits of the secret image. While the degradation of the cover image is not visually noticeable in many cases, four bits are sufficient to transmit a rough approximation of the secret image [14].

2.3.1.4 Cover-Regions and Parity Bits:

By dividing the cover into several disjoint regions $R_{i,}$ it is possible to store one bit of information in a whole cover-region rather than in a single element. A parity bit of a region R can be calculated by:

$$P(R) = \sum_{j \in R} LSB(C_j) \bmod 2 \qquad (2\text{-}1)$$

In the embedding process step, *l(m)* disjoint cover-regions $R_i(1 \leq i \leq l(m))$are selected each encodes one secret bit m_i in the parity bit $P(R_i)$. If the parity bit of one cover region R_i does not match with the secret bit m_i to encode, one LSB of the value in R_i is flipped. This will result in $P(R_i)=m_i$. In the decoding process, the parity bits of all selected regions are calculated and lined up to reconstruct the message. Again, the cover-regions can be constructed pseudo randomly using stego-key.

2.3.1.5 Pallet-Based Images:

Generally, there are tow ways to encode information in pallet-based images; either the pallet or the image data can be manipulated. The LSB of the color vectors could be used for information transfer, just like the substitution methods. Alternatively, since the pallet dose not need to be sorted in any way, information can be encoded in the way the colors are sorted in the pallet. Since there is N! Different ways to sort the pallet, there is enough capacity to encode a small message however; all methods which use the order of the pallet to store information, are not robust, since an attacker can simply sort the entries in a different way and destroy the secret message without even modify the picture visibility [14].

2.3.1.6 Quantization Method

Quantization of digital images can be used for embedding secret information. A review of quantization in the context of predictive coding will be discussed first. In predictive coding, the intensity of each pixel is predicted based on the pixel values in a specific neighborhood; the prediction may be linear or nonlinear function of the surrounding pixel values. In its simplest form, the difference e_i between adjacent pixels x_i and x_{i+1} is calculated and fed into quantizer Q which outputs a discrete approximation Δ_i of the difference signal (i.e., Δ_i=Q(x_i- x_{i-1})). For highly correlated signals Δ_i is close to zero, so an entropy coder will be efficient. At the receiver side the difference signal is dequantized and added to the last signal sample in order to construct an estimate for a sequence x_i [14].

2.3.2 Transform Domain Techniques

The substitution modification techniques are easy ways to embed information, but they are highly vulnerable to even small cover modification. An attracter can simply apply signal processing techniques in order to destroy the secret information entirely.

It has been noted early 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 the same sort of transform domain [14].

Transform domain methods hide messages in the significant areas of the cover image which makes them more robust to attacks, such as adding noise, compression, filtering, cropping and some image processing, than the substitution approach. However, while they are more robust to various kinds of signal processing, they remain imperceptible which means that the HVS has sense that there exits a stego-image. Many transform domain variation exist, one method is to use the discrete cosine transform (DCT), and another would be the wavelet transformation [19],[24],[26]. Transformation can be applied over the entire image, to blocks throughout the image, or other variations.

One popular method of encoding of secret information in the frequency domain is modulating the relative size of two (or more) DCT coefficient within one image block.

During the encoding process, the sender splits the cover-image in 8×8 pixel block; each encodes exactly one secret message bit. The embedding process starts with selecting a pseudorandom block *bi* which will be used to code the i_{th} message bit. B_i=DCT (b_i) be the discrete cosine transformed image block.

Before the communication starts, both sender and receiver have to agree on location of two DCT coefficients, which will be used in the embedding process, say, (u_1, v_1) and (u_2, v_2). The two coefficients should correspond to cosine function with middle frequencies; this ensure that the information is stored in significant parts of signal (hence the embedded information will not be completely damaged by JPEG[3]). Furthermore, the embedding process will not be degenerated the cover heavily, because it is widely believed that the DCT coefficients of middle frequencies have similar magnitudes. Since the constructed system should be robust against JBEG compression, the DCT coefficients should be chosen in such a way that the quantization values associated with them in the JPEG compression algorithm are equal. One block encode a "1", if $B_i(u_1,v_1)>B_i(u_2,v_2)$, otherwise a "0". In the encoding step, the two coefficients are swapped if their relative size dose not matches with the bit to be encoded. The sender then performs an inverse DCT to map the coefficients back to the space domain.

[3] JPEG (Joint Photographic Export Group): one type of compression uses the DCT.

To decode the picture, all available blocks are DCT transformed. By comparing the two coefficients of every block, the information can be resorted[14].

2.3.3 Spread Spectrum Techniques

Spread spectrum (SS) is a mean of transmission in which the signal occupies a bandwidth in excess of the minimum necessary to send the information [30]. Although the power of the signal to be transmitted can be large, the signal to noise ratio in every frequency band will be small. Even if parts of the signal could be removed in the several frequency bands, enough information should be present in the other bands to recover the signal. Thus, SS makes its difficult to detect and / or remove the signal. The situation is very similar to a steganogrphy system which tried to spread a secret message over a cover in order to make it impossible to perceive. Since spreaded signals tend to be difficult to remove, embedding methods based on SS should provide a considerable level of robustness [14].

2.3.4 Statistical Techniques

Statistical steganography techniques utilize the existence of "1-bit" steganography schemes, which embed one bit of information in a digital carrier. This is done by modifying the cover in such a way that some statistical characteristic change significantly if a "1" is transmitted. Otherwise, the cover is left unchanged. So the receiver must be able to distinguish unmodified covers from modified ones.

In order to construct a *l(m)*-bit stego-system from multiple "1-bit" stego-systems, a cover is divided into *l(m)* disjoin block $B_1, \ldots, B_{l(m)}$. A secret bit, m_i, is inserted into the I_{th} block by placing a"1" into B_i if m_i=1. Otherwise, the block is not changed in the embedding process. The detection of a specific bit is done via a test function which distinguishes modified blocks from unmodified block [14].

2.3.5 Distortion techniques

In contrast to substitution system, distortion techniques require the knowledge of the cover in the decoding process. The sender applies a sequence of modification to a cover in order to get stego-object; he chooses this sequence in such a way that it corresponds a specific secret message he wants to transmit. The receiver measures the differences to the original cover in order to reconstruct the sequence of modification applied by the sender, which correspond to the message [14].

One of the main disadvantages of these techniques is the need of transmission additional information, *original cover* that needs another secure channel.

2.3.6 Cover Generation Techniques:

Encode information in the way a cover is generated

Example: Automated Generation of English Text

- Use a large dictionary of words categorized by different types, and a style source which describes how words of different types can be used to form a meaningful sentence.
- Transform message bits into sentences by selecting words out of the dictionary which conforms to a sentence structure given in the style source [25].

2.4 Steganalysis

A goal of steganography is to a void suspicion to the transmission of a hidden message. If the suspicion is raised, then this goal is defeated. *Steganalysis* is the art of discovering and rendering such covert message [26].

Analysis on hidden information may take several forms: detecting, extracting, confusing (counterfeiting or overwriting), and disabling.

The steganalyst or attacker is one who applies Steganalysis in an attempt to detect the existence of hidden information, extract and /or destroy it.

Somewhat parallel attacks are available to the steganalyst. There are *stego-only, known cover, known message, chosen stego, chosen message and known stego.* A stego-only attacks is similar to cipher text only attack where only the stego-object is available for analysis. If the original cover and stego-object are both available, then known message attack when the hidden message is revealed at some later date; an attacker may attempt to analyze the stego-object for future attacks. Even with the message, this may be very difficult and may be equivalent to the stego-only attack. The chosen stego attack is one where the steganography tool (algorithm) and the stego-object are known. A chosen message attacks is one where the steganalyst generate stego-object from some steganography tool or algorithm from a known message. The goal in this attack is to determine corresponding pattern in the stego-object that may point to the use of specific steganography algorithms or tools. Finally, when the attacker knows the steganography algorithm and both the original cover-object and stego-object are available, and then the attacker is called known stego attack [26].

On the other hand, the attacker (warden) may categorize according to their abilities to three main types:

- ***The passive attacker***: The attackers try to detect the existence of the hidden information [31].
- ***The active attacker***: the attacker are allowed to modify (slightly) the data being sent between the partner but he must modify data so much that innocent communication would be foiled [29].
- ***Malicious attacker***: the attacker can forge message, since the recipient is not able to verify the correctness of the sender identity [14].

Three parameters one should keep in his mind while designing a steganography system to give a certain level of resistance against the three types of attacker, that is, *imperceptibility, robustness*, and *security.*

The imperceptibility of the stego-object is required for all steganography system and for all types of attacks, not only the passive attack, because the main purpose of steganography is to make the available communication invisible and this ensure no conflicting with this purpose.

An active warden, who is not able to extract or the prove existence of secret message, thus try to destroy this information, so the practical requirement for a steganography system is avoid such type of attacks is robustness. A system is called robust if the embedded information can not be altered without making drastic changes to the stego-object. Many steganography systems are designed to be robust against a specific class of mappings (e.g. JPEG compression/decompression, filtering, addition of white noise, etc.) [14].

In the presence of malicious attacker, imperceptibility and robustness are not enough. If the embedding method is not dependent on some secret information shared by the sender and receiver, (i.e. in the case of pure or public key steganography), an attacker can forge message. Thus, to avoid the malicious attacks, the algorithm must be secure. The steganography algorithm has for requirements to be secure [14]:

- Messages are hidden using pubic algorithm and secret key.
- Only holder of the correct key can detect, extract and prove the existence of the hidden message.
- Even if the adversary knows (or is able to select) the. contents of one hidden message, he should have no chance of detecting others.
- It is computationally infeasible to detect the hidden message.

Chapter Three

Discrete Image Transform

Chapter Three

Discrete Image Transforms

3.1 Introduction

The concept of a transform is familiar to mathematicians and engineers. It is a standard mathematical tool used to solve problem in many areas of engineering and science, including computer imaging. The idea is to change a mathematical quantity to another form, where it may look unfamiliar but may exhibit useful feature [32].

Originally defined in their continuous forms, they are commonly used today in their discrete (sampled) forms. The discrete form of these transforms is created by sampling the continuous form of the functions on which these transforms are based, that is, the *basis function*. The functions used for these transforms are typically sinusoidal or rectangular, and the sampling process, for the one-dimensional case, provides us with basis vectors. When we extend these into two-dimensions, as we do for images, they are basis matrices or basis images.

The general form of the transformation equation, assuming an N×N image, is given by:

$$T(u,v)=\sum_{r=0}^{N-1}\sum_{c=0}^{N-1}I(r,c)B(r,c;u,v)$$

Where I(r, c) is the original image, T (u, v) are the transform coefficients, B(r, c; u, v) correspond to the basis images, r and c are the spatial domain variable and u and v are the frequency domain variable. The transform coefficients T (u, v) are the projections of I (r, c) onto each B (u, v). These coefficients tell how similar the image is to the basis image. By applying the inverse transform, one can obtain the image from the transform coefficients as follows:

$$I(r,c)=\sum_{u=0}^{N-1}\sum_{v=0}^{N-1}T(u,v)B^{-1}(r,c;u,v)$$

Here the B^{-1}(r, c; u, v) represents the inverse basis images. In many cases they are the same as the forward ones, but possibly weighted by a constant [16].

3.2 Fourier Transform

The Fourier transform is the most well Known, and the most widely used, transform. This transform allows for the decomposition of an image into a weighted sum of 2-D sinusoidal terms [16]. Assuming an N×N image, the equation for the 2-D discrete Fourier transform is:

$$F(u,v)=\frac{1}{N}\sum_{r=0}^{N-1}\sum_{c=0}^{N-1}I(r,c)e^{-j2\pi\frac{ur-vc}{N}}$$

The basis functions are sinusoidal in nature, as can be seen by Euler's identity: $e^{jx}=\cos x+j\sin x$

So we can also write the Fourier transform equation as:

$$F(u,v)=\frac{1}{N}\sum_{r=0}^{N-1}\sum_{c=0}^{N-1}I(r,c)[\cos(\frac{2\pi}{N}(ur+vc))+j\sin(\frac{2\pi}{N}(ur+vc))]$$

$F(u,v)=R(u,v)+jI(u,v)$ Where *R (u, v)* is the real part and *I (u, v)* is the imaginary part of complex spectrum, and j is the imaginary coordinate, then we define the magnitude and phase of a complex spectral component as:

$$MAGNTUDE=|F(u,v)|=\sqrt{[R(u,v)]^2+[I(u,v)]^2}$$

And $PHASE=\phi(u,v)=\tan^{-1}\left[\frac{I(u,v)}{R(u,v)}\right]$

The magnitude of a sinusoid is simply its peak value, and the phase determines where the origin is or where the sinusoid starts ,in other words, the phase data contain information a bout *where objects* are in an image and the magnitude gives their contrast [16],[33].

After we perform the transform, if we want to get our original image back, we need to apply the *inverse transform*. The inverse Fourier transform is given by:

$$F^{-1}[F(u,v)] = I(r,c) = \frac{1}{N}\sum_{u=0}^{N-1}\sum_{v=0}^{N-1} F(u,v)e^{j2\pi\frac{(ur-vc)}{N}}$$

3.3 Discrete Cosine Transform

The cosine transform, like the Fourier transform, uses sinusoidal basis functions. The difference is that the cosine basis functions are not complex; they use only cosine functions and not sine functions [32], [34]. Assuming an N×N image, the discrete cosine transform equation is given by:

$$C(u,v) = \alpha(u),\alpha(v)\sum_{r=0}^{N-1}\sum_{c=0}^{N-1} I(r,c)\cos\left[\frac{(2r+1)u\pi}{2N}\right]\cos\left[\frac{(2c+1)v\pi}{2N}\right]$$

Where $a(u),a(v) = \begin{cases} \sqrt{\frac{1}{N}} & u,v=0 \\ \sqrt{\frac{2}{N}} & u,v=1,2,\ldots,N-1 \end{cases}$

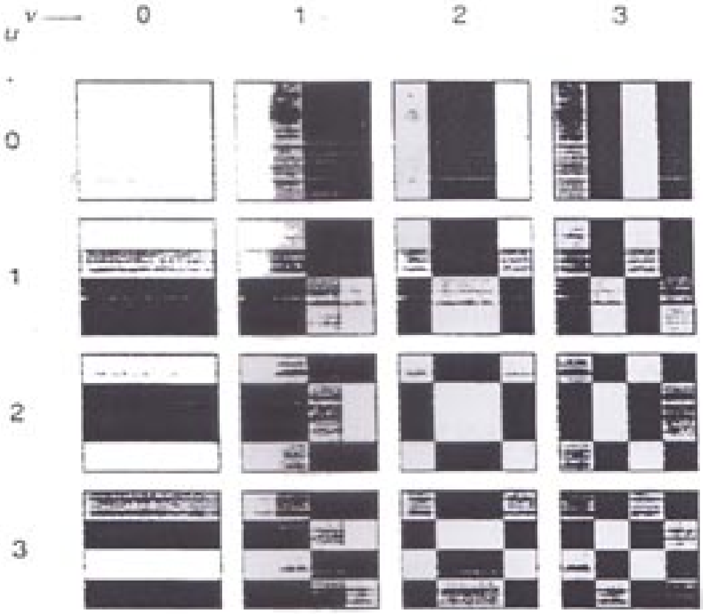


Figure (3-1) Discrete Cosine Transform Basis Image

Because the DCT transform is practically used for image compression purposes[1]; therefore, the DCT is applied not to the entire image but to the data units (blocks) to reduce the arithmetic operations and then speed the algorithm up [32]. Figure (1-3) shows the 2-D basis images for the cosine transform for 4×4 blocks of data, from these basis images and remembering that the transform coefficients are the projections of the original image onto each basis image, one can conclude the following:

- The origin coefficient represents the lowest frequency; in other word, the DC component of the entire image or subimage.
- The first row of the coefficients matrix increasingly shows the frequency component of the image rows and in the same manner the first column shows the frequency component of the image columns.
- The rest of the coefficients reflect the changes in the frequencies in both rows and columns that corresponding with each basis images.

Of course, there is no need to say that there exists a fast DCT algorithm as in FFT to efficiently compute the DCT coefficients.

The inverse cosine transform is given by:

$$C^{-1}[C(u,v)] = I(r,c) = \sum_{u=0}^{N-1}\sum_{v=0}^{N-1}\alpha(u)\alpha(v)C(u,v)\cos\left[\frac{(2r+1)u\pi}{2N}\right]\cos\left[\frac{(2c+1)v\pi}{2N}\right]$$

3.4 Walsh-Hadamard Transform

The Walsh-Hadamard transform differs from the Fourier transform and cosine transforms in that the basis are not sinusoids [16]. The basis functions are based on square or rectangular waves with peaks of ±1. Here the term rectangular wave refers to any function of this form, where the width of the pulse may vary. One primary advantage of a transform with these types of basis functions is that the computations are very simple. When we project the image onto the basis functions, all we need to do is multiply each pixel by ±1,

[1] The DCT is in particular used with JBEG image compression method.

as is seen is the Walsh-Hadamard transform equation (assuming an N×N image):

$$WH(u,v)=\frac{1}{N}\sum_{r=0}^{N-1}\sum_{c=0}^{N-1}I(r,c)(-1)^{\sum_{i=0}^{N-1}[b_i(r)p_i(u)+b_i(c)p_i(v)]}$$

Where N=2^n, the exponent on the (-1) is performed in modulo 2 arithmetic, and $b_i(r)$ is found by considering r as a binary number and finding the ith bit.

$P_i\,(u)$ is found as follows: $p_0(u)=b_{n-1}(u)$

$p_1(u)=b_{n-1}(u)+b_{n-2}(u)$

$p_2(u)=b_{n-2}(u)+b_{n-3}(u)$

.

.

.

$p_{n-1}(u)=b_1(u)+b_0(u)$

Strictly speaking we con not call the Walsh-Hadamard transform a frequency transform because the basis functions do not exhibit the frequency concept in the manner of sinusoidal functions. If we consider the number of zero crossings (or sign changes), we have a measure that is comparable to frequency, and we call this sequency [16].

The inverse Walsh-Hadamard transform equation is:

$$WH^{-1}[WH(u,v)]=I(r,c)=\frac{1}{N}\sum_{u=0}^{N-1}\sum_{v=0}^{N-1}WH(u,v)(-1)^{\sum_{i=0}^{n-1}[b_i(r)p_i(u)+b_i(c)p_i(v)]}$$

3.5 Wavelet Transform

Considerable interest has arisen in recent years regarding new transform techniques that specifically address the problem of image compression, edge and feature detection, and texture analysis. These techniques come under the heading of muliresolution analysis, time-frequency analysis; pyramid algorithms and wavelet transform [34].

The wavelet transform can be described as a transform that has basis functions that are shifted and expended versions of themselves. Because of this, the wavelet transform contains not just frequency information but spatial information as well. One of the most common models for a wavelet transform uses the Fourier transform and highpass and lowpass filters. To satisfy the conditions for a wavelet transform, the filters must be perfect reconstruction filters, which means that any distortion introduced by the forward transform will be canceled in the inverse transform (an example of these types of filters are quadrature mirror filters).

The wavelet transform breaks an image down into four sub-sampled, or decimated, images as shown in Figure (3-2). They are sub-sampled by keeping every other pixel. The results consist of one image that has been highpass filtered in both the horizontal and vertical directions, one that has been highpass filtered in the vertical and lowpass filtered in the horizontal, and one that has been lowpass filtered in the vertical and highpass in the horizontal, and one that has been lowpass filtered in both directions [16].

LOW/ LOW	LOW/ HIGH
HIGH/ LOW	HIGH/ HIGH

Location of frequency in a four-band wavelet Transformed image. Designation is row/column

Figure (3-2): Wavelet Transform Display

Wavelet transform have proven to be very efficient and effective in analyzing a very wide class of signal and phenomena because of their attractive feature that are [35]:

- Wavelet transform describe signals in terms of their local shifts. Thus, they provide a time-frequency representation.
- Wavelets are adjustable and adaptable. Because there is not just one wavelet, they can be designed to fit individual application.
- The size of wavelet expansion coefficient drop-off rapidly for a large class of signals.
- The generation of wavelets and a calculation of all wavelet expansions employing summation, not integrals, that is well matched to be implemented by digital computers.

3.5.1 Wavelet filters

Numerous filters can be used to implement the wavelet transform, and two of the commonly used ones, the Daubechies and the Haar. These are separable, so they can be used to implement a wavelet transform by first convolving them with the rows and then the columns. The Haar basis vectors are simple [16]:

$$LOWPASS: \quad \frac{1}{\sqrt{2}}[1 \quad 1]$$

$$HIGHPASS: \quad \frac{1}{\sqrt{2}}[1 \quad -1]$$

An example of Daubechies basis vectors follows:

$$LOWPASS: \quad \frac{1}{\sqrt[4]{2}}[1+\sqrt{3}, \quad 3+\sqrt{3}, \quad 3-\sqrt{3}, \quad 1-\sqrt{3}]$$

$$HIGHPASS: \quad \frac{1}{\sqrt[4]{2}}[1-\sqrt{3}, \quad \sqrt{3}-3, \quad 3+\sqrt{3}, \quad -1-\sqrt{3}]$$

The inverse wavelet filters for the Haar filter are identical to the forward filters, for the Daubechies example given, the inverse wavelet filters are:

$$LOWPASS_{inv} : \frac{1}{\sqrt[4]{2}}[3-\sqrt{3}, \quad 3+\sqrt{3}, \quad 1+\sqrt{3}, \quad 1-\sqrt{3}]$$

$$HIGPASS_{inv} : \frac{1}{\sqrt[4]{2}}[1-\sqrt{3}, \quad -1-\sqrt{3}, \quad 3+\sqrt{3}, \quad -3+\sqrt{3}]$$

3.5.2 Wavelet Coding

Wavelet coding, sometime, also called subband coding. The basic idea is split up the two dimensional frequency band images into sub-sampling channels which are encoded using techniques accurately matched to individual signal statistics and possibly to the properties of the human visual system in the individual subbands.

Practical image subband coding techniques mostly use separable decomposition, i.e., one-dimensional filters is used in order to separate the frequency bands both horizontally and vertically. The reason is that separable filter implementations of non-separable two dimensional filters. On the other hand, the gain in coding efficiency obtained by application of non-separable filters is usually small or negligible [36].

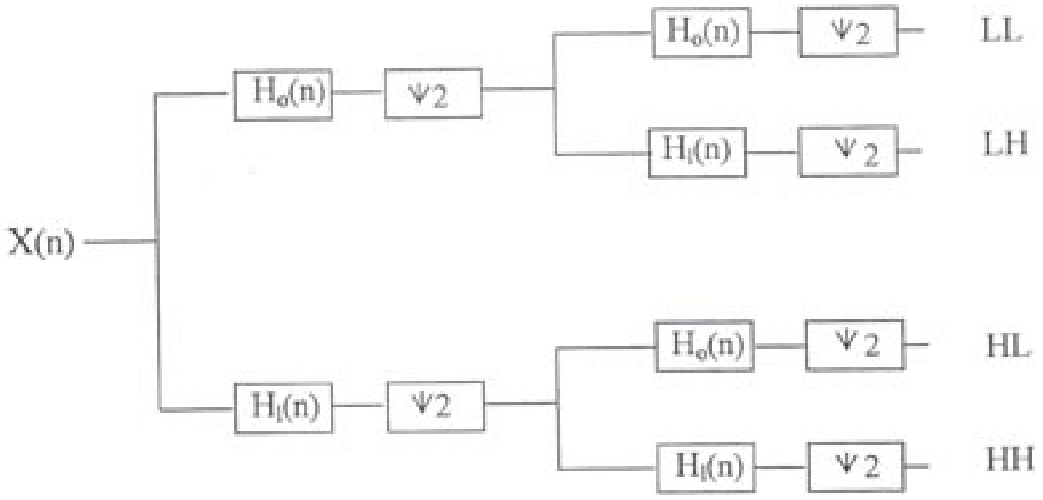


Figure (3-3) one stage of subbands decomposition With 2-D separable filters

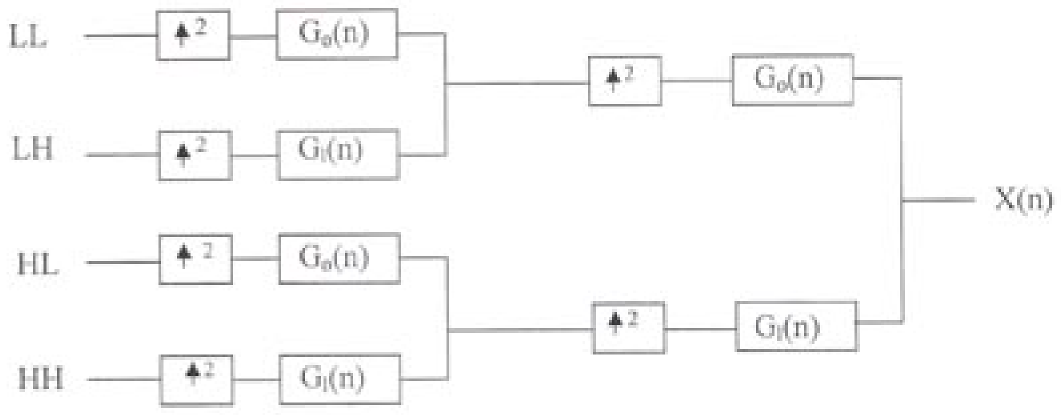


Figure (3-4) one stage of subbands reconstructing With 2-D separable filters

In the figure (3-3),↓ 2 denote down sampling by a factor of two, H_0 denotes a low-pass filter, and H_1 denotes a high pass-filter. The initial high and low-pass filters and down-sampling are applied to the rows of an image. The subsequent filters and down sampling is then applied to the resulting columns. Because there are only two filters. This is called a *two channels system*. The image is split into four bands LL, LH, HL and HH according to whether the rows and columns received the low or high frequency filtering. The reconstructing operation consists of an up-sampling operation followed by a synthesis filter bank, as shown in figure (3-4).

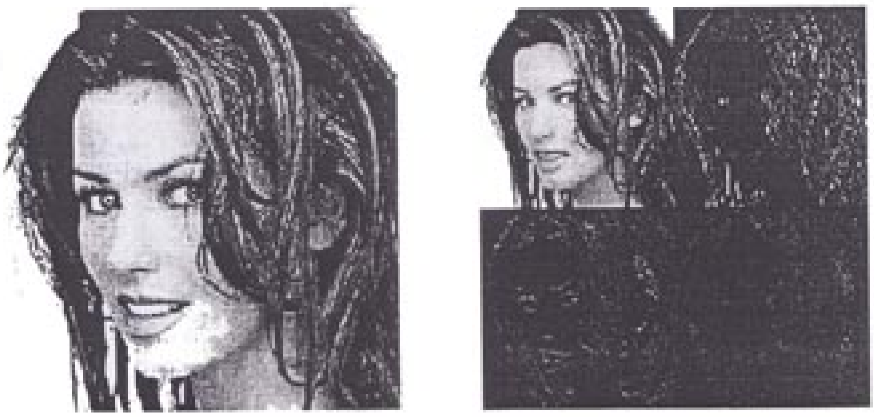
Subband decomposition is produced by an analysis filter bank followed by down sampling which produces subband decomposition. Therefore, the term "decomposition" refers to filtering and down sampling operation for as many stages as desired [37], [38].

The main purpose behind using the subband coding technique for video and digital image applications is the acquisition of a set of sub sampled frequency bands where each band contains various structural features of the original image.

The base band of the image presents a smaller replica of the original signal consist of all the low frequency components that are of major perceptual importance.

The neighboring picture elements of the base-band are highly correlated and this spatial redundancy needs to be exploited by an appropriate coding scheme [39]. Therefore, subband filtering provide a set of disjoint upper bands that are structurally different from the base band and to not display strong pixel to pixel intra-band correlation's [40]. However, the original image can be transformed into four sub-images, as shown in the figure (3-2), namely:

- LL sub image: Both horizontal and vertical directions have low frequency.
- LH sub image: the horizontal direction has low frequency and the vertical one have high frequencies.
- HL sub image: the horizontal direction has high frequencies and the vertical one has low frequencies.
- HH sub image: both horizontal and vertical directions have high frequencies [41].



a) Original image

b) Wavelet transform using Haar basis vector, four bands.

Figure (3-5) Wavelet Transform

Figure (3-5) shows the result of applying the wavelet transform to an image. We can see the lowpass-lowpass image in the upper-left corner, the lowpass-highpass images in the diagonals, and the highpass-highpass in the lower-right corner.

There are several types of wavelet transform, and depending on the application, one may be performed to the others. For a continuous input signal, the time and scale parameters can be continuous leading to the *Continuous Wavelet Transform* (CWT). They may as well be *Discrete Wavelet Transform* (DWT). Finally, the wavelet transform can be defined for discrete-time signals leading to a Discrete Time Wavelet Transform (DTWT) [42].

Chapter Four

System Implementation

Chapter Four

System Implementation

4-1 Introduction

Our presented stegosystem (*Information Hiding Using Wavelet Transform*) is used to embed a color or gray image in another one. We have utilized the transform domain techniques for robustness purposes.

The wavelet transform is applied to both the host and the signature images to guarantee that the low frequency components of the signature image will be inserted in the high frequency components of the host image. For security purposes, the low frequency components of the signature image has been quantized by dividing them on certain number, referred as (quantization value). Also the stego-key is used which is transmitted separately making the system type a secret key steganography system. The whole proposed stegosystem is illustrated in figure (4-1).

4.2 System Implementation:

The designed system implements *BMP* image file format. As illustrated in figure (4-2), the hiding process menu involves the following shown operations; ***Open Images, Wavelet Transform, Embedding Process, Save Image**, and **Extracting Process**.*

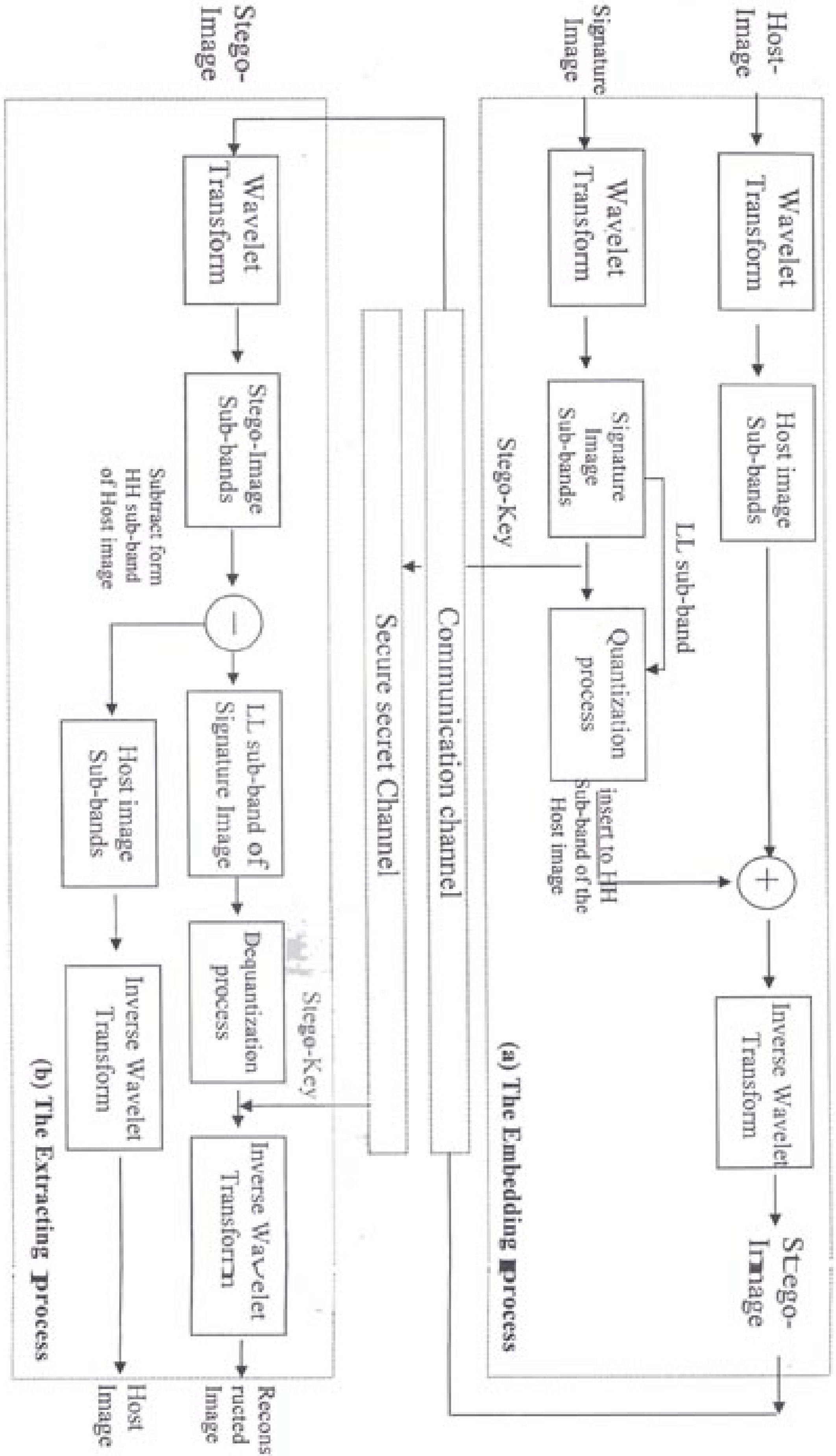


Figure (4-1) the proposed Stego-System

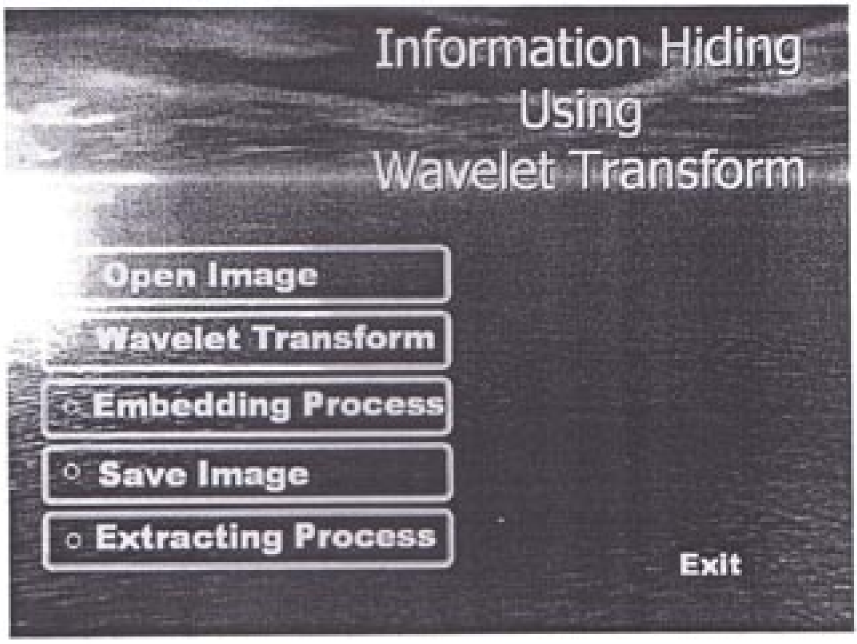


Figure (4-2) the Starting Menu

4.2.1 Open Images Menu

The Open Images Menu, as shown in fig.(4-3), involves ***Open Host Image*** and **Open Signature Image**.

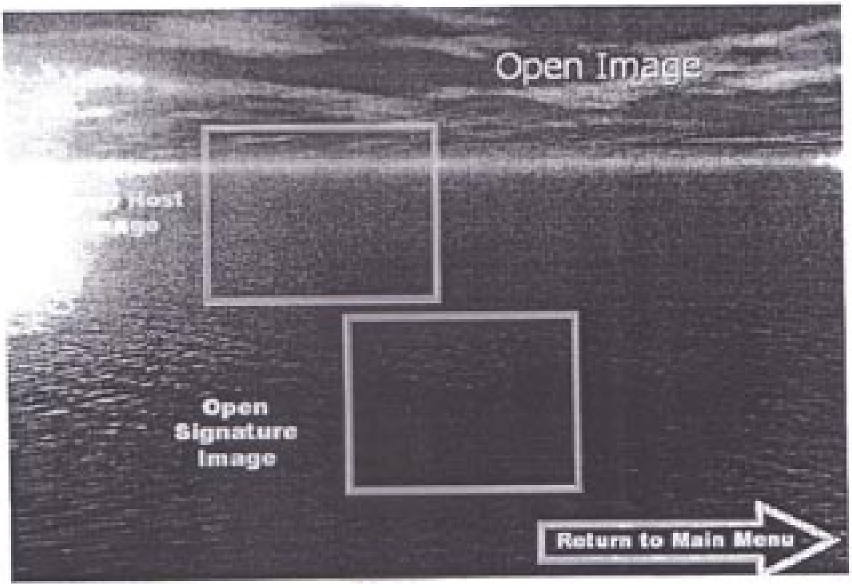


Figure (4-3) Open Image Menu

4.2.1.1 Open Host Image

This option is used to load the host (cover) image in which we embed the signature image. The user can load the host image from the open dialog form from any location of the program. Figure (4-4) shows the open dialog form. Notice, the user has only one choose; loading *BMP* file format.

4.2.1.2 Open Signature Image

This option is used to load the signature (hide) image, which will be embedded in the host image. The user can load the image that has the same or less size than the host image from the open dialog form. Figure (4-5) shows the open images.

4.2.1.3 Return to Main Menu

This option is used to return from the local choice (Open Images) to the starting menu's form.

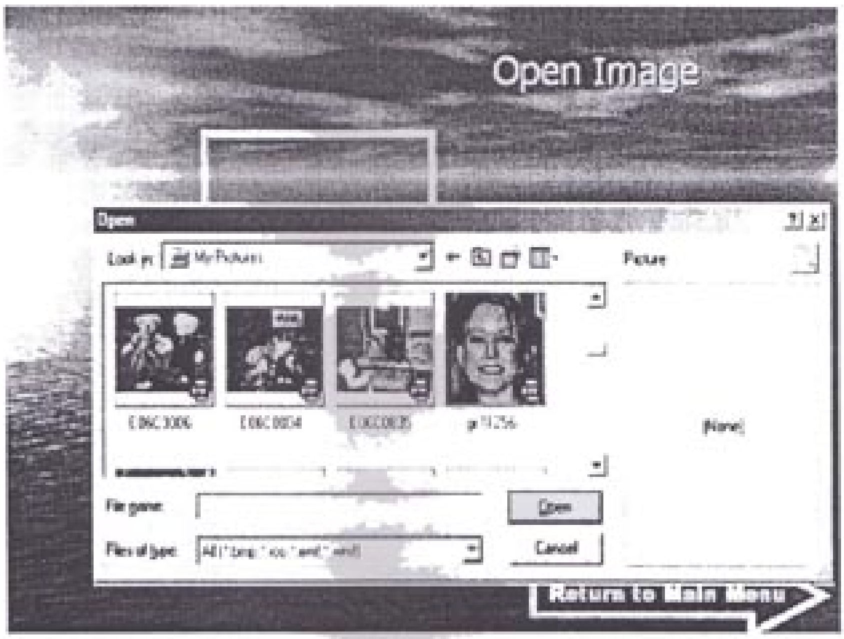


Figure (4-4) The Open Dialog form

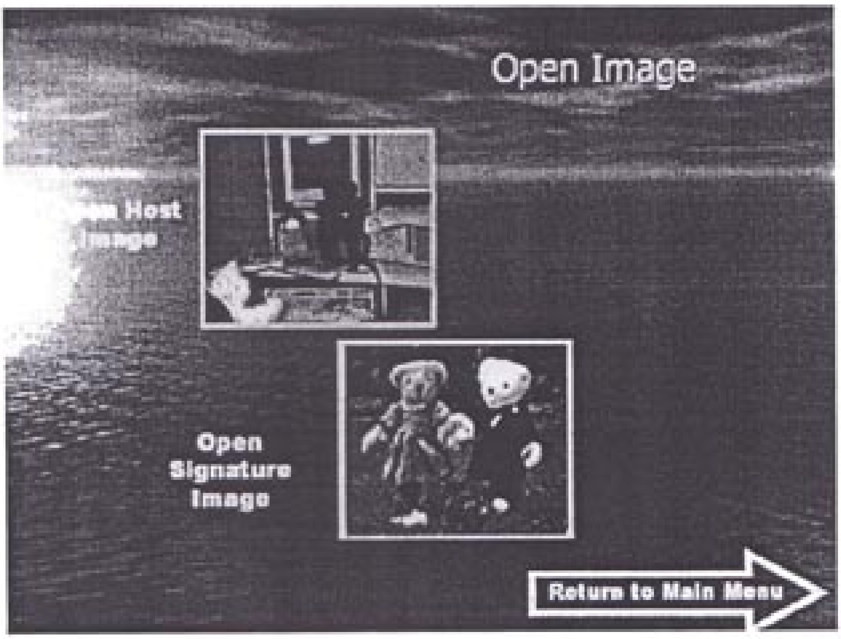


Figure (4-5) the Open Images

4.2.2 Wavelet Transform menu

This form, as illustrated in fig. (4-6), has four options: *Wavelet Transform on Host Image, Wavelet Transform on Signature Image, HH subband of Host Image* and *LL subband of signature Image*.

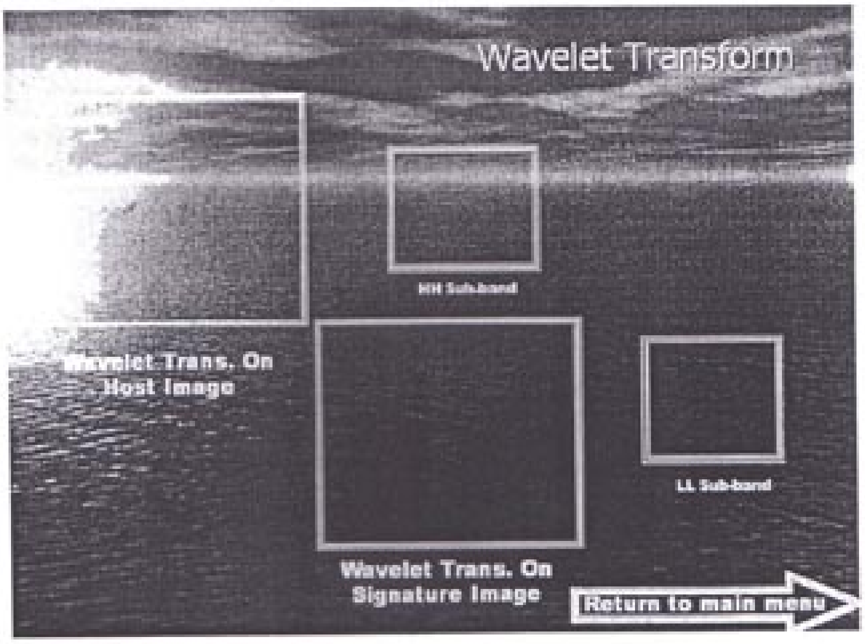

Wavelet Transform
HH Sub-band
Wavelet Trans. On Host Image
LL Sub-band
Wavelet Trans. On Signature Image
Return to main menu

Figure (4-6) Wavelet Transform Menu

4.2.2.1 Wavelet Transform of Both Host and Signature Images:

In these two options the wavelet transform can be applied to the host image as well as to the signature image. The main job of applying the wavelet transform to both the host image and the signature image in the proposed stego system is to partition these images into sub-bands; each sub-band has certain frequency information. Since most of the natural image's energy concentrates in the low frequency band, so that, in general, the high energy subband reflect their low frequency contents and vice versa[32]. The transform coefficients can be determined by the following steps that describe the adaptive Haar wavelet transformation procedure:

1- Applying the lowpass filter on the rows of the image pixels as fallows:

$$R_{(j,i)} = \frac{X_{(j,2i)} + X_{(j,2i+1)}}{\sqrt{2}}$$

Where j = {0, …, height-1} and i = {0, …, wid-1}

2- Applying the lowpass filter to the columns results from step (1) to producing the LL subband as fallows:

$$W_{(i,j)} = \frac{R_{(2i,j)} + R_{(2i+1,j)}}{\sqrt{2}}$$

Where i = {0, …, wid-1} and j = {0, …, hei-1}

3- Applying the highpass filter to the columns results from step (1) to producing the LH subband as fallows :

$$W_{(i+hei,j)} = \frac{R_{(2i,j)} - R_{(2i+1,j)}}{\sqrt{2}}$$

Where i = {0, …, wid-1} and j = {0, …, hei-1}

4- Applying the highpass filter to the rows of the original image as fallows:

$$R_{(j,j+wid)} = \frac{X_{(j,2i)} - X_{(j,2i+1)}}{\sqrt{2}}$$

Where i = {0, …, wid-1} and j = {0, …, height-1}

5- Applying the lowpass filter to the columns results from step (4) to producing the HL subband as fallows :

$$W_{(i,j+wid)} = \frac{R_{(2i,j)} + X_{(2i+1,j)}}{\sqrt{2}}$$

Where i = {0, …, hei-1} and j = {wid, …, width-1}

6- Applying the highpass filter to the columns results from step (4) to producing the HH subband as fallows:

$$W_{(i+hei,j+wid)} = \frac{X_{(2i,j)} - X_{(2i+1,j)}}{\sqrt{2}}$$

Where i = {0, …, hei-1} and j = {wid, …, width-1}

Where $X_{(i,j)}$ are the image pixel values, $W_{(i,j)}$ are the transformed coefficients, $R_{(j,i)}$ are temporarily assisted parameters, width is the image width, height is the image height, wid is the width divided by 2 and hei is the height divided by 2.

As a result of the transform, four smaller size images will be produced, referred as LL, LH, HL and HH. LL subband is the average of the pixels, and is the coefficients of the low resolution space, and the other three (LH, HL and HH) which are wavelet coefficients that allow as reconstructing the image. Figure (4-7) shows the wavelet transform implmentation.

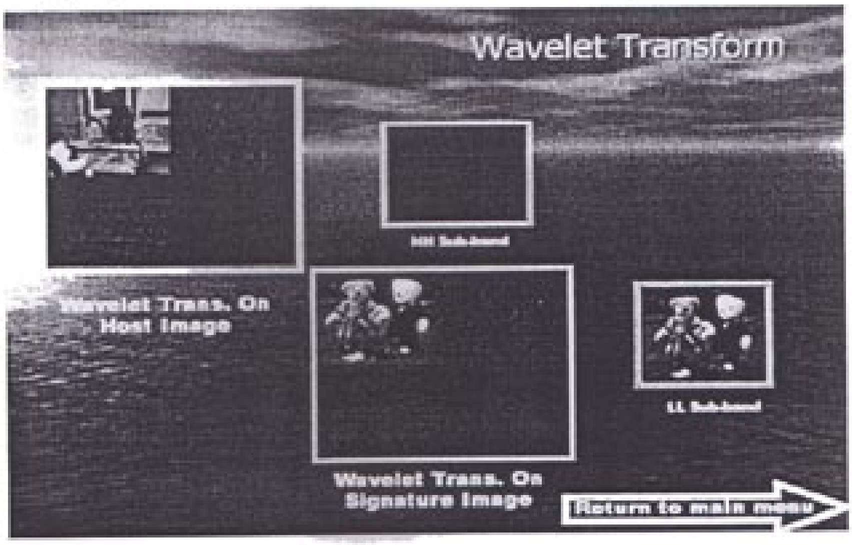

Wavelet Transform
HH Sub-band
Wavelet Trans. On Host Image
LL Sub-band
Wavelet Trans. On Signature Image
Return to main menu

Figure (4-7) Wavelet Transform Implementation

4.2.2.2 HH's Sub-band of the Host Image

This button is used to view the HH subband of the host image which represents the high frequency component of image that will be remved in the embedding process.

4.2.2.3 LL's Subband of the signature Image

This button is used to view the LL subband of the signature image which represents the low frequency component of the transformed image. In this subband the image energy is concentrated; therefore these coefficients should not be changed dramatically. In our present research the LL subband of the signature is inserted in the less significant position of the host transformed image; i.e. in the HH subband location.

4.2.3 Embedding Process Menu

The Whole process of insertion has been performed in this menu, illustrated in fig.(4-8). This menu has the following options: ***Quantization, stego key, Embedding process and the Inverse Wavelet Transform.***

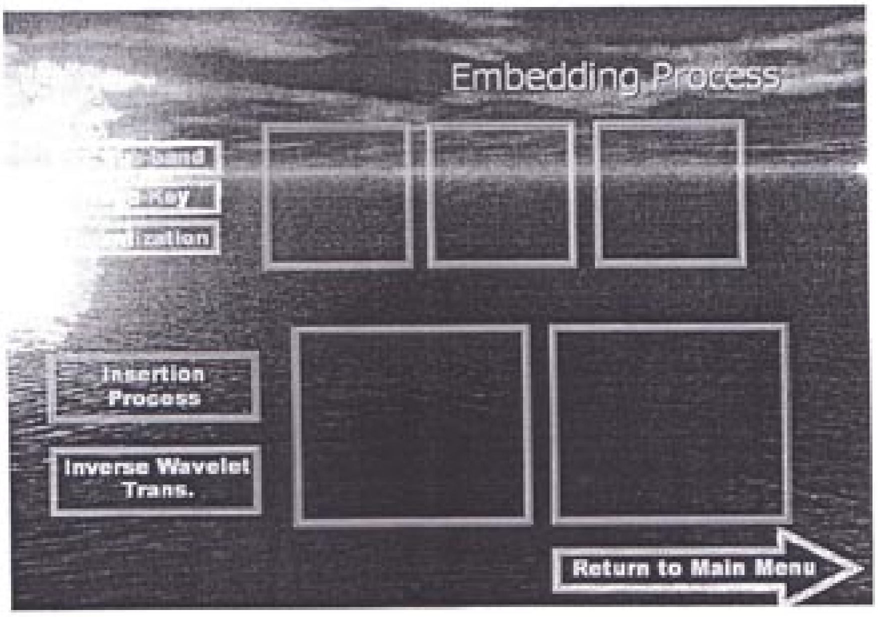


Figure (4-8) Embedding Process Menu

4.2.3.1 The Quantization (Normalization) Process

This process is considered as an important step in our designed stego-system. Quantization is, in fact, the mapping of the large set of the possible input (may be real values) into smaller set of possible output (integer). In this research, the quantization operation has been performed by normalizing (i.e. dividing) the transformed coefficients of the LL-Signature image by an integer number (in the related works the number 50 have been used as the quantization value).

4.2.3.2 Stego Key

This option is used to add some security to the stego image. The stego key used here is done by dividing the LL subband of the signature image into 32×32 blocks. The pixels of each block are drawn inversely, so that, the stego key is the way in which the pixels are arranged.

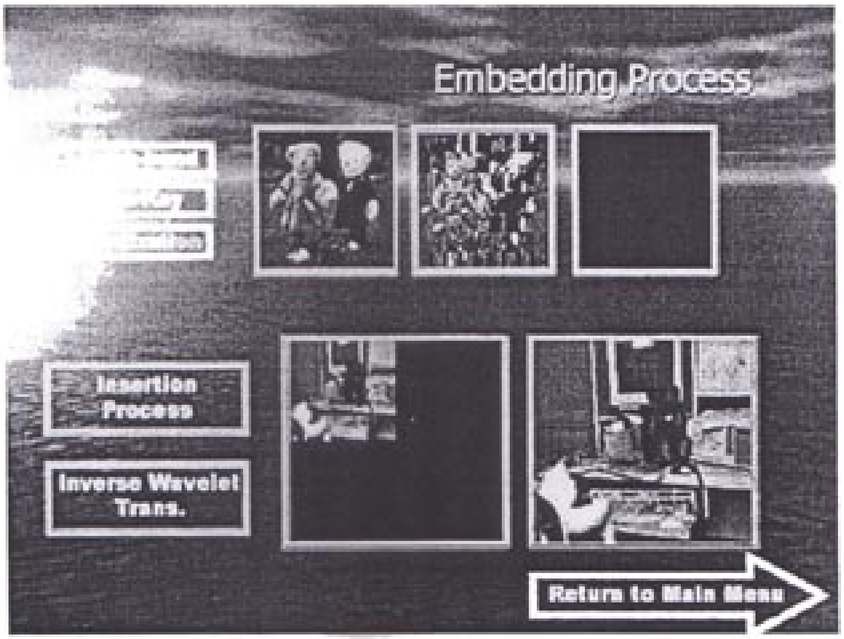


Figure (4-9) the Embedding Process

4.2.3.1 The Quantization (Normalization) Process

This process is considered as an important step in our designed stego-system. Quantization is, in fact, the mapping of the large set of the possible input (may be real values) into smaller set of possible output (integer). In this research, the quantization operation has been performed by normalizing (i.e. dividing) the transformed coefficients of the LL-Signature image by an integer number (in the related works the number 50 have been used as the quantization value).

4.2.3.2 Stego Key

This option is used to add some security to the stego image. The stego key used here is done by dividing the LL subband of the signature image into 32×32 blocks. The pixels of each block are drawn inversely, so that, the stego key is the way in which the pixels are arranged.

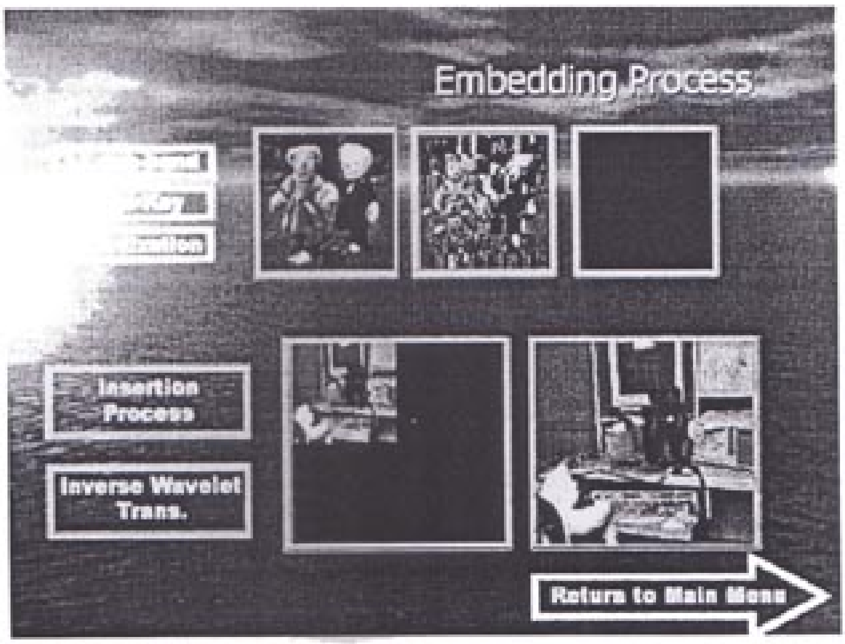


Figure (4-9) the Embedding Process

4.2.3.3 Embedding Process

This operation is one of the most important steps in the proposed stegosystem. Removing the HH subband of the host image is performed by this operation. The quantized coefficient of the LL subband of the signature image is inserted at the location of the removed subband of the host image, so that, the resulted image consist of the host image three subbands (LL, LH and HL) in addition to the LL subband of the signature image.

4.2.3.4 Inverse Wavelet Transform

After the embedding process, inverse wavelet transform is applied to transform the host image subbands into the spatial "image" domain. The resulted stego-image is same as the host image containing the LL subband of the signature image that is inserted on it. The following steps describe the inverse of Haar wavelet transformation procedure:

1- Applying the lowpass filter and highpass filter between the HL subband pixels and HH subband pixels to producing the H subband, using:

$$R_{(2i,j)} = \frac{W_{(i,j)} + W_{(i+hei,j)}}{\sqrt{2}} \qquad R_{(2i+1,j)} = \frac{W_{(i,j)} - W_{(i+hei,j)}}{\sqrt{2}}$$

Where i={0,…, hei-1}and j={wid,…, width-1}

2- Applying the lowpass filter and high pass filter between the LL subband pixels and LH subband pixels producing the L subband, using:

$$R_{(2i,j)} = \frac{W_{(i,j)} + W_{(i+hei,j)}}{\sqrt{2}} \qquad R_{(2i+1,j)} = \frac{W_{(i,j)} - W_{(i+hei,j)}}{\sqrt{2}}$$

Where i={0,…, hei-1}and j={0,…, wid-1}

3- Applying the lowpass filter and highpass filter between H subband pixels resulted from step (1) and the L subband pixels resulted from step (2) to producing the reconstructed image, using:

$$X_{(j,2i)} = \frac{R_{(j,i)} + R_{(j,i+wid)}}{\sqrt{2}} \qquad X_{(j,2i+1)} = \frac{R_{(j,i)} + R_{(j,i+wid)}}{\sqrt{2}}$$

Where i={0,…, wid-1}and j={0,…, height-1}

Where $W_{(i,j)}$ are the image transformed coefficients, $R_{(j,i)}$ are temporarily assisted parameters, $X_{(j,i)}$ are the reconstructed image pixels, width is the image width, height is the image height, wid is the width divided by 2 and hei is the height divided by 2.

4.2.4 Saving Image Menu

This menu mainly consists of three options: **Stego-Image, Save Image** and **Fidelity Criteria**, illustrated in fig. (4-10) shown below.

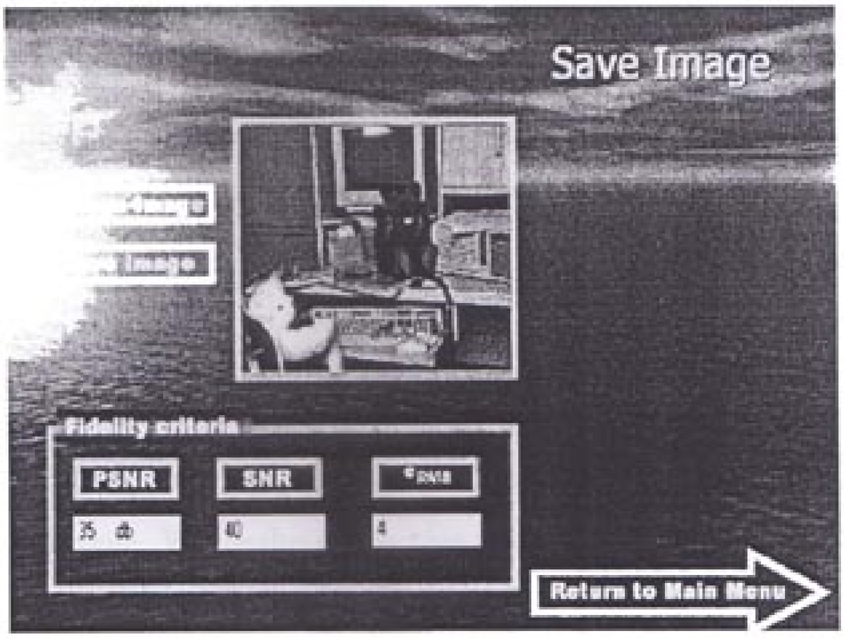


Figure (4-10) Save Image Menu

4.2.4.1 Viewing Stego-Image

This button is used to view the stego-image resulted from the embedding process to save it and in order to measure PSNR, SNR and e_{RMS}, shown in fig.(4-11).

4.2.4.2 Saving Image Menu

This option is used to save the resulted stego-image, the saving dialog appears and asking the user for the name and location that will be used to save the stego-image. Figure (4-11) shows the save dialog form.

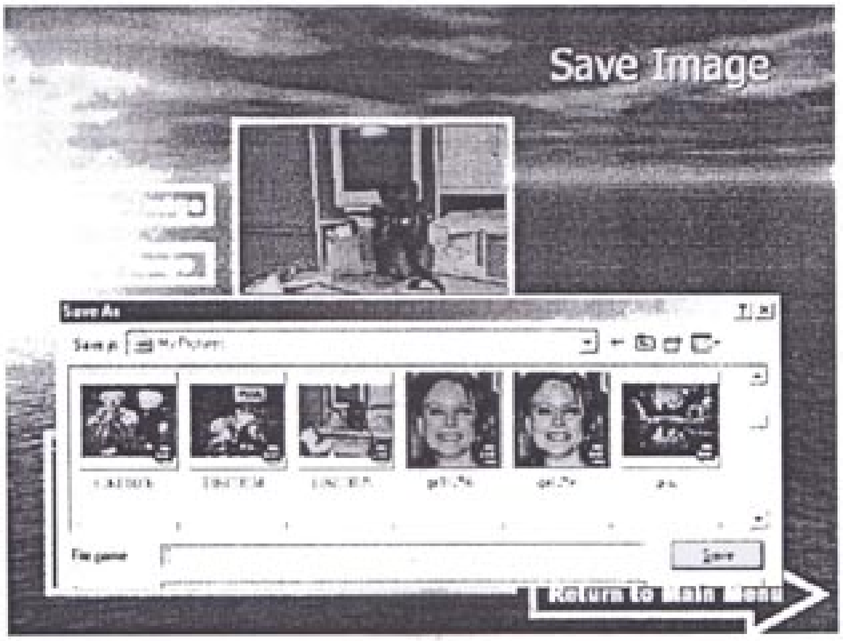


Figure (4-11) Save image dialog

4.2.4.3 Image Fidelity Criteria Measure Menu

Fidelity criteria can be divided into two classes: *Objective fidelity criteria* that provide us with quantitative tests to the amount of the error in the reconstructed image. While the *subjective fidelity criteria use* qualitative scale to assess image quality, and human judges carry this test.

In order to provide unbiased results, evaluation with subjective measure requires careful selection of the test subjects and carefully designed evaluation experiments. The objective criteria are useful as a relative measure in comparison different versions of the same image.

Commonly used objective measures are the root-mean-square error (E_{RMS}), the root-mean-square signal to noise ratio (SNR_{RMS}) and the peak signal-to-noise ratio (PSNR). Because related works have used these three measures [12], it will be used here for comparison purposes.

The e_{RMS} can be defined in an N×N reconstructed image as:

$$e_{RMS}=\sqrt{\frac{1}{N^2}\sum_{r=0}^{N-1}\sum_{c=0}^{N-1}[\hat{I}(r,c)-I(r,c)]^2}$$

And the SNR metrics consider the reconstructed image $\hat{I}(r,c)$ to be the "signal" and the error to be the noise. The SNR can be defined as:

$$SNR_{RMS}=\sqrt{\frac{\sum_{r=0}^{N-1}\sum_{c=0}^{N-1}[\hat{I}(r,c)]^2}{\sum_{r=0}^{N-1}\sum_{c=0}^{N-1}[\hat{I}(r,c)-I(r,c)]^2}}$$

The PSNR is usually measured in dB and can be defined as:

$$PSNR=10\log_{10}\frac{(L-1)^2}{\frac{1}{N^2}\sum_{r=0}^{N-1}\sum_{c=0}^{N-1}[\hat{I}(r,c)-I(r,c)]^2}$$

Where L is the number of the gray levels, $I(r,c)$ is the original image and $\hat{I}(r,c)$ is the stego-image.

If one considers the system as to be monitored by a human sense test, the subjective test must be used. However, subjective testing is performed by creating a database of image to be tested; i.e. gathering a group of people, and then having all the test subjects evaluate the images according to a predefined scoring criterion. The results are then analyzed statistically [16].

4.2.5 The Extracting Process Menu

Now, two objects must be transmitted to reconstruct the signature image. The stego-image that is transmitted via a public communication channel; that may be exposed to active attacks, and the stego-key which contain the way in which the pixels are arranged. These two objects are the input to the extracting process that approximately produces the signature image.

This menu consist of eight options; i.e. **Open Stego-Image**, **Wavelet Transform to Stego-Image, View HH subband, Dequantization Process, Stego-Key, Inverse Wavelet to Host Image, Inverse Wavelet to the Reconstructed (signature) Image**, and **Fidelity Criteria,** shown in fig.(4-12).

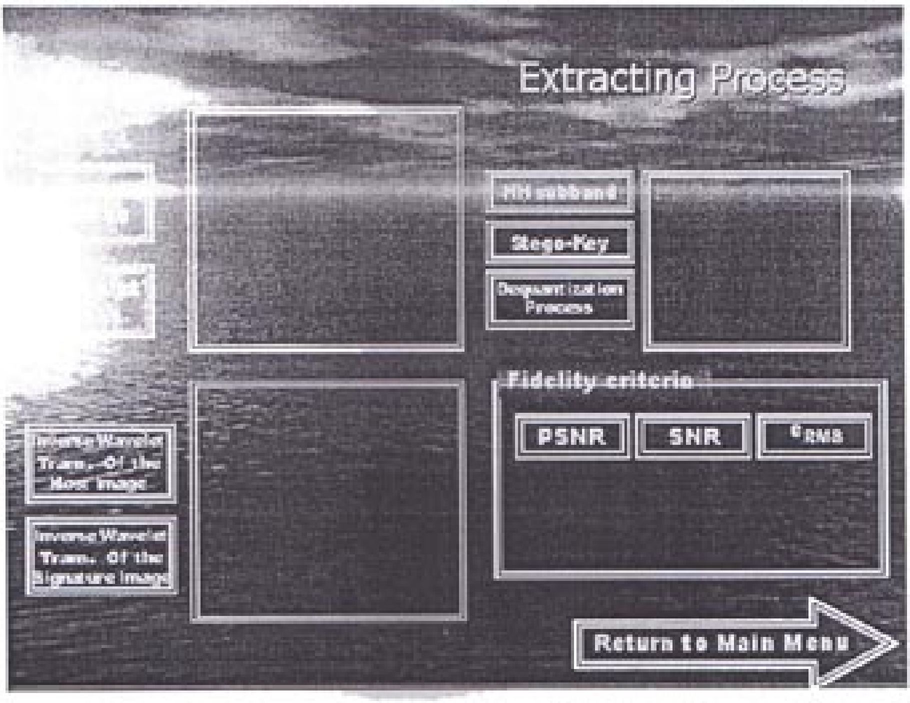


Figure (4-12) the Extracting Menu

4.2.5.1 Open Stego-Image

This button is used to load the stego-image. The users can also loading the stego-image from the open dialog form, and from any location in computer program.

4.2.5.2 Wavelet Transform on Stego-image

This option is used to apply the wavelet transform to the stego-image (see section 4.2.2.1), its subbands are produced. These subbands are the three host image subbands added to it the LL subband of the signature image. The inserted LL subband of the signature image is located in the HH subband of the stego-image subbands.

4.2.5.3 View HH subband

This option is used to view the HH subband of the stego-image. This subband is used to extract the LL subband of the signature image which is added to the host image subbands in the embedding process.

4.2.5.4 De-quantization process

This option is used to retrieve the original value of the extract LL sub-band. It is performed by multiplying the values of each image's pixels by the quantization (i.e. normalization) value that is used in the embedding process. Figure (4-13) show the relation between the quantization value and the PSR of both the steg-image and the reconstructed image.

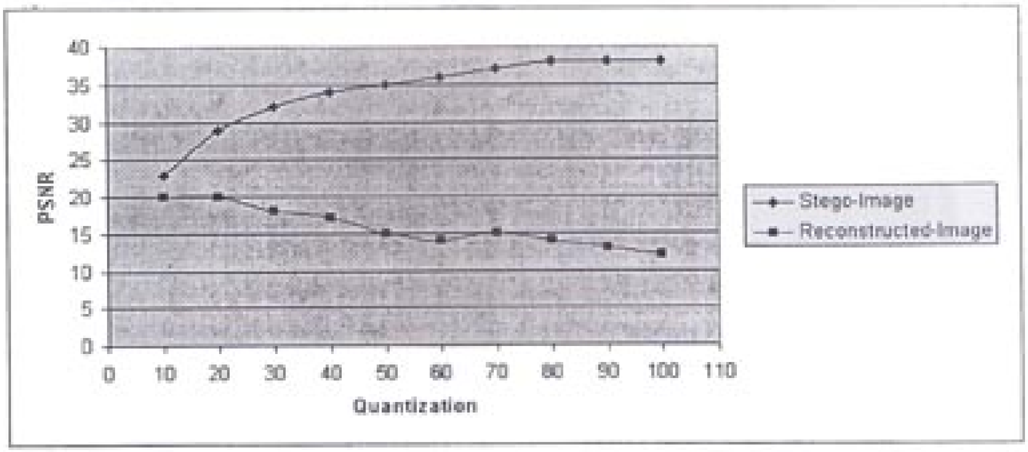


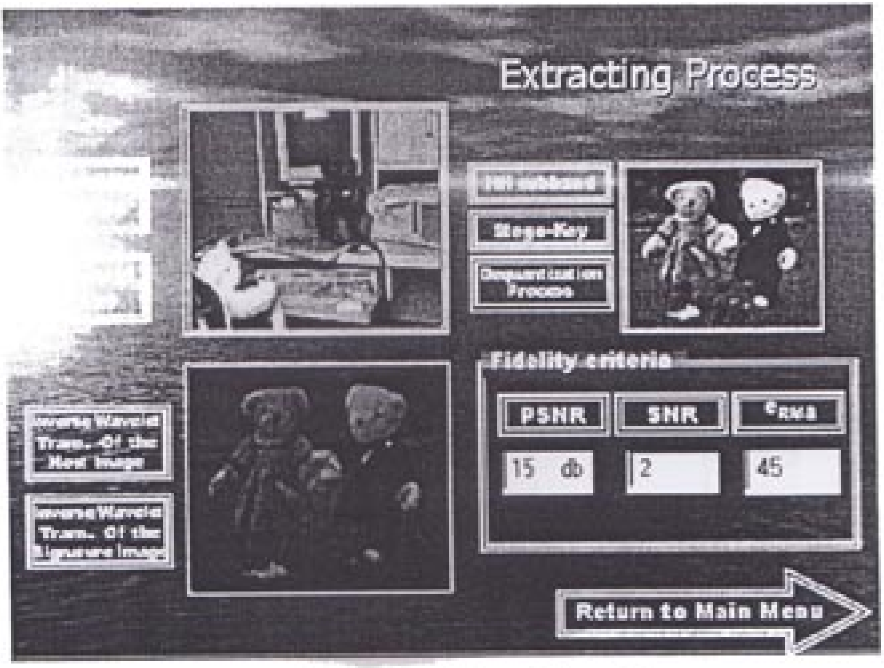
Figure (4-13) Shows the relation between the Quantization value and the output PSNR, of the Stego-Image And the *Reconstructed image*

4.2.5.5 Stego-Key

This option is used to return the LL subband pixels to its original arrangement. These pixels are drowning inversely in the embedding process, so that, return it to its position is done by dividing this subband to blocks of 32×32. And then the pixels of each block are drowning inversely.

4.2.5.6 Inverse Wavelet Transform on Host Image

This button is used to implement the inverse wavelet transform to the host image. After the extracting of the HH subband of the stego-image the three subbands (LL, LH and HL) remaining represent the host image without HH subband, so that, we assume that the HH subband pixels are equal to "0". Now the inverse wavelet Transform is applied to this four subbands in the same way that mention in section (4.2.2.1).



PSNR: 15 db
SNR: 2
e_{RMS}: 45

Figure (4-14) the Extracting Process

4.2.5.7 Inverse Wavelet Transform on Signature Image

This option is used to apply the inverse wavelet transform to the signature image. After the extracting process we have only the LL subband of the signature image. In order to reconstruct the signature image we assume that the other three subbands pixels equal to "0". And then the inverse wavelet transform is applied as mention in section (4.2.2.1).

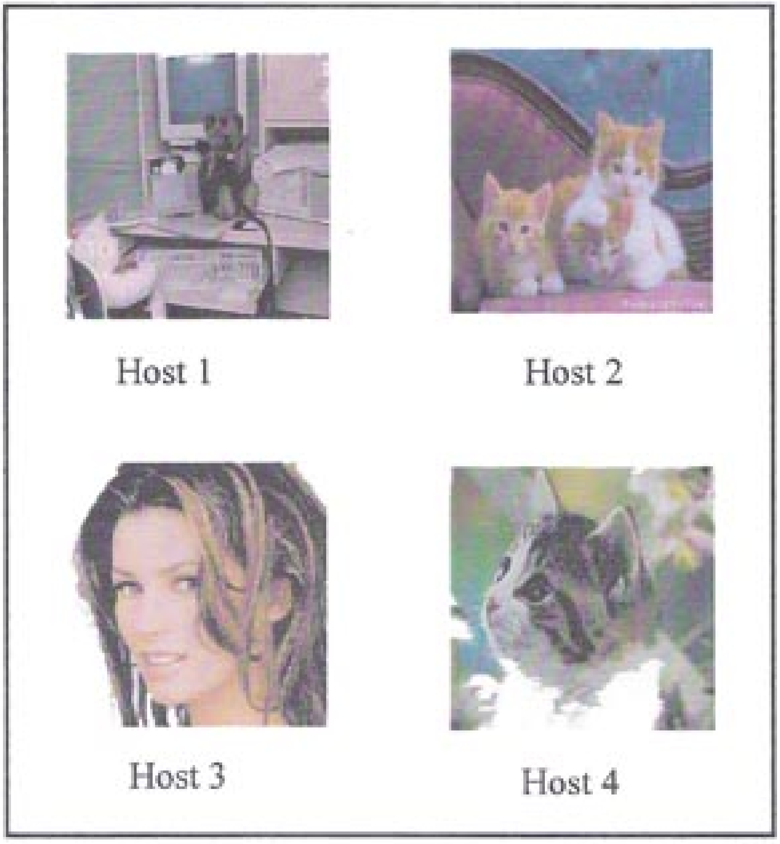
4.2.5.8 Fidelity Criteria Measure

This option is used to measure the **Objective fidelity criteria** (PSNR, SNR and e_{RMS}) to the reconstructed image. This operation is done between the reconstructed image and the original (signature) image in the same way that explains in section (4.2.4.3). For four groups (stego, reconstructed) images table (4-1) shows the Objective fidelity criteria (PSNR, SNR and e_{RMS}).

Table (4-1)

Objective fidelity criteria for Stego and Reconstructed images

Images	Stego-Image			Reconstructed Image		
	PSNR	SNR	e_{RMS}	PSNR	SNR	e_{RMS}
image1	35	40	4	15	2	45
Image2	34	28	5	13	2	59
Image3	30	15	8	14	3	53
Image4	28	12	10	18	5	31



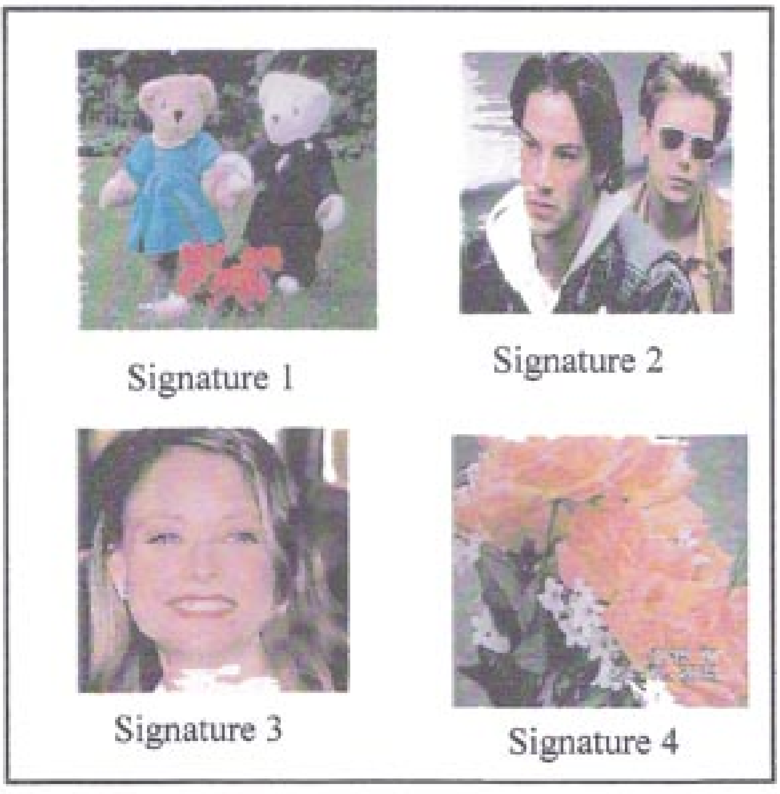
Host 1

Host 2

Host 3

Host 4

Figure (4-15): Samples of Host Images.



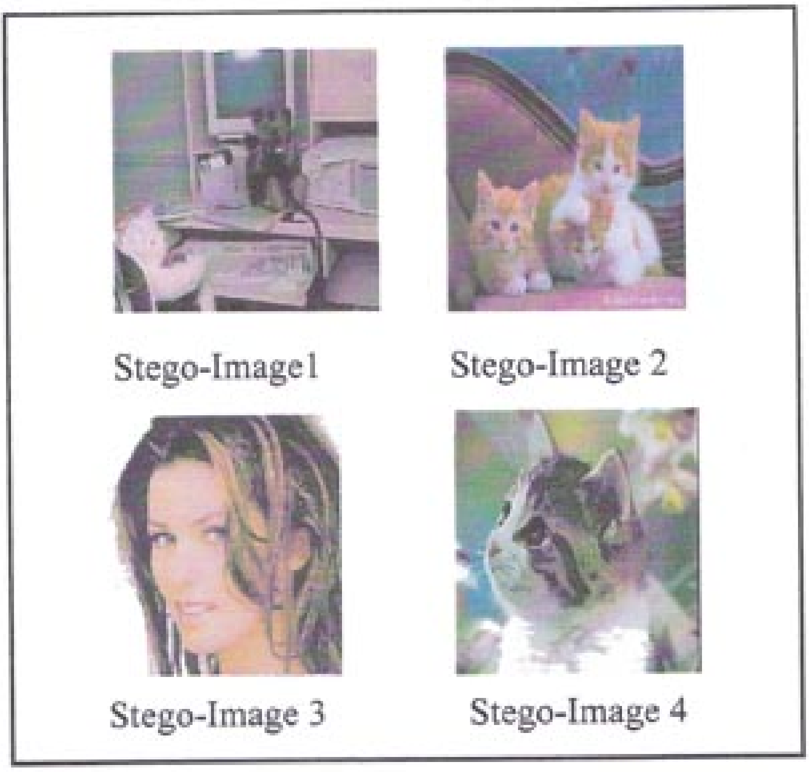
Signature 1

Signature 2

Signature 3

Signature 4

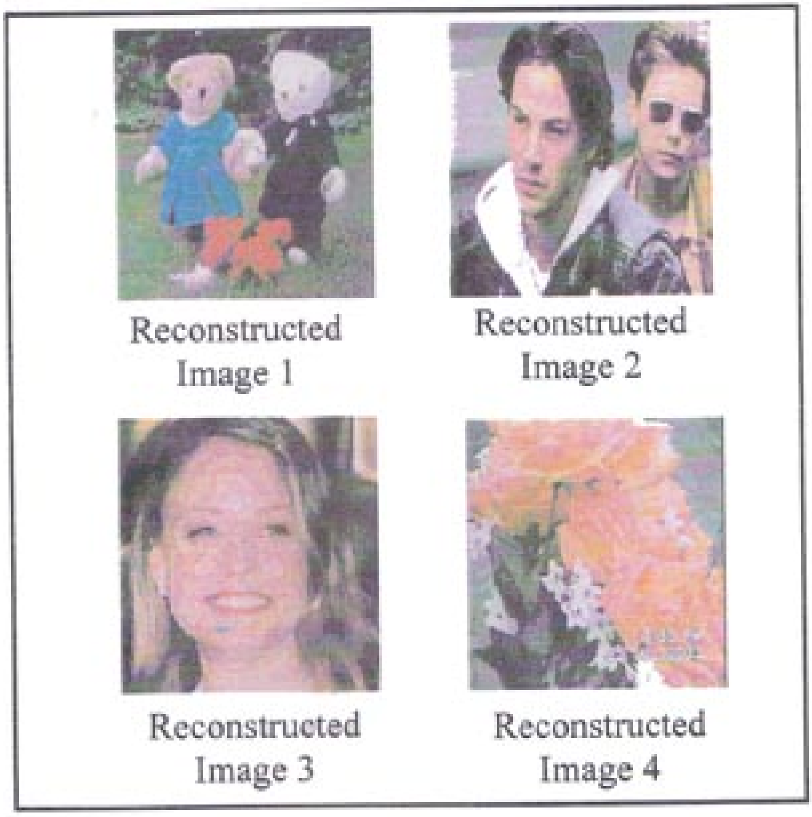
Figure (4-16): Samples of Signature Images.



Stego-Image1 Stego-Image 2

Stego-Image 3 Stego-Image 4

Figure (4-17): Samples of Stego-Images.



Reconstructed Image 1 Reconstructed Image 2

Reconstructed Image 3 Reconstructed Image 4

Figure (4-18): Samples of Reconstructed-Images.

Chapter Five

Conclusions

And Suggestions for Future Work

Chapter Five

Conclusions and Suggestions For Future Work

5-1 Concluding Remark

After studying the proposed stego-system, one can conclude the following:

1- It is easiest to embed a gray image in another gray image and a color image in color image. Otherwise, the reconstructed signature image will be deteriorated.

2- The quality of the stego-image and the reconstructed image, presented in terms of Peak-signal-to-noise ratio (PSNR) has been found to be quantization process dependent. This means that; increasing the normalization value would produce much degradation.

3- The quality of the reconstructed image is not the same as of the stego-image quality; therefore, a pre-enhancing process may be required to improve the image quality.

4- Using the wavelet transform yield an acceptable image quality from adopting only the LL subband. This, in turns, contributed in best hiding and acceptable reconstruction of the hided information.

5-2 Suggestions for Future Work

1- Applying attacks on the proposed system (e.g. image enhancement, linear and nonlinear filtering and/or data reduction) to demonstrate the stego system robustness against these attacks.

2- Design an error correcting code that takes into consideration much type of attacks and this, for sure, will improve the quality of the reconstructed image.

3- Another suggestion is to improve the reconstructed image quality by restoring or enhancing it, using special types of filters (spatial or frequency domain filters).

4- Applying the wavelet transform by utilizing two-levels to the signature image and using the subbands of the second level in the embedding process.

5- Using the Daubechies basis vectors instead of the Haar filter because of its ability to compact more image energy in the LL subband.

6- Applying another method of transform domain to the signature image and using the resulted coefficients of this transform in the embedding process.

References

1- A. Tacticus, *How to Survive Under Siege/Aineias the Tactician* (Clarendon Ancient History Series). Oxford, U.K.: Clarendon, 1990, pp. 84–90, 183–193.

2- J. Wilkins, *Mercury: Or the Secret and Swift Messenger: Shewing, How a Man May with Privacy and Speed Communicate His Thoughts to a Friend at Any Distance*, 2nd ed. London, U.K.: Rich Baldwin, 1694.

3- D. Chaum, "Untraceable electronic mail, return addresses and digital pseudonyms," *Commun. ACM*, vol. 24, no. 2, pp. 84–88, Feb. 1981.

4- R. J. Anderson, Ed., *Information Hiding: 1st Int. Workshop* (*Lecture Notes in Computer Science*), vol. 1174. Berlin, Germany: Springer-Verlag, 1996.

5- S. Roche and J.-L. Dugelay, "Image watermarking based on the fractal transform," in *Proc. Workshop Multimedia Signal Processing*, Los Angeles, CA, 1998, pp. 358–363.

6- J. P. M. G. Linnartz, "The "ticket" concept for copy control based on embedded signaling," in *Computer Security—5th Europ. Symp. Research in Computer Security, (ESORICS'98)* (*Lecture Notes in Computer Science*), vol. 1485, J.-J. Quisquater, Y. Deswarte, C. Meadows, and D. Gollmann, Eds. Berlin, Germany: Springer, 1998, pp. 257–274.

7- M. L. Miller, I. J. Cox, and J. A. Bloom, "Watermarking in the real world: An application to DVD," in *Multimedia and Security—Workshop at ACM Multimedia'98* (*GMD Report*), vol. 41, J. Dittmann, P. Wohlmacher, P. Horster, and R. Steinmetz, Eds. Bristol, U.K.: ACM, GMD—Forschungszentrum Information stechnik GmbH, 1998, pp. 71–76.

8- F. L. Bauer, *Decrypted Secrets—Methods and Maxims of Cryptology.* Berlin, Heidelberg, Germany: Springer-Verlag, 1997.

9- N. F. Johnosn, Z. Durie and S. Jajodia, *"Information Hiding: Steganography and Watermarking – Attacks and Countermeasures".* KLUWER ACADEMIC PUBLISHERS, 2001.

10- F. Queirolo, "*Steganography in Images*", Final Communications Report, 2002.

11- A. Graps, "*An Introduction to Wavelet*" IEEE computational Science and engineering, Vol.2, Pt.II, pp. 1-18, 1995.

12- M. Vetterli and J. Kovacevic, "*Wavelet and subband coding*", Englewood Cliffs, New Jersey: Prentice Hall, 1995.

13- J. L. Strack, F. Murtagh, and A. Bijaoui, " *Image processing and Data Analysis, the Multiscale Approach* " COMBRIDGE UNIVERSITY PRESS 1998.

14- S. Katzenbeisser and F. A. P. Petitcolas, *"Information Hiding Techniques for Steganography and Digital watermarking"* Artech House, London 2000.

15- N. F. Johnson, Z Duric, and S. Jajodia, "*Information Hiding: Steganography and watermarking",* KLUWER ACADEMIC PUBLISHERS 2001.

16- S. U. Umbaugh, *"Computer Vision and Image Processing",* Prentice Hall, 1998.

17- A. M. Al-jashammi, *"Image Steganography using Wavelet Transform Techniques*", B.Sc. thesis, Electronic and communication Engineering dept. College of Engineering, University of Baghdad, Baghdad, Iraq ,2002.

18- L. Z. Adedissian, *"Image in Image Steganography*", Ph.D. thesis, computer science dept. College of Science, University of Technology, Baghdad, Iraq, 2000.

19- N. K. Abdulaziz and K. K. Pang, *"Robust Data Hiding for Images"*, Proc. IEEE, pp.380-383, 2000.

20- S. Areeposga, Y. F. Syed, N. Kawkamnerd, and K. R. Rao, *"Steganogrphy for a Low Bit-Rate Wavelet Image Coder"*, http://issu.gmu.edu/~njohnson/steganography

21- U. I. Ibrahim, *"Text in Image Steganography"*, M.Sc. thesis, computer science dept., College of Science, University of Technology, Baghdad, Iraq, 2001.

22- H. H. Marza, *"Text in Image Steganography Techniques"*, M.Sc. thesis, computer science dept., College of Science, University of Baghdad, Baghdad, Iraq, 2001.

23- F. A. P. Petitcolas, R. J. Anderson and M. G.Kuhn, *"Information Hiding_ A survey"*. Proceedings of the IEEE, Vol. 87, No. 7, July 1999.

24- J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "A *Secure, Robust watermarking for multimedia*", Information Hiding: First International workshop, proceedings, Vol. 1174 of Lecture Notes in computer Science, Springer, 1996, pp 185-25.

25- M. Al-Mualla and H. Al-Ahmad "*Information Hiding: steganography and watermarking*". Multimedia communication and signal Processing (MCSP) Research Group, Etisalat College of engineering, Sharjah, UAE.

26- N. F. Johnson and S. Jajodia, *"Steganalysis of Images Created Using Current Steganography software*", Information Hiding: Second International workshop, proceedings, Vol. 1525 of Lecture Notes in computer Science, Springer, 1998, pp 273-289.

27- R. J. Anderson and F. A. P. Petitcolas, "*On the Limits of steganogrphy* ", IEEE Journal of selected Areas in communications, 16(4): 474-481, May 1998.

28- J. C. A. Lubbe, "*Basic Method of Cryptography* ", Cambridge University press, 1998.

29- S. Craver, "*On Public Key Steganogrphy*", Information Hiding: Second International workshop, proceedings, Vol. 1525 of Lecture Notes in computer Science, Springer, 1998, pp 355-368.

30- R. L. Pickholtz, D. L. Schilling, and L. B. Milstein, "*Theory of spread Spectrum communication –A Tutorial*", IEEE Trans. Communications, Vol. 30, Pt. I, pp. 855-884, May 1982.

31- J. M. Ettinger, "*Steganalysis and Game Equilibria*", Information Hiding: Second International workshop, proceedings, Vol. 1525 of Lecture Notes in computer Science, Springer, 1998, pp 319-330.

32- D. Salomon, "*Data Compression, the Complete Reference*", Spriger-Verlag. New York, Inc. 2000.

33- R. C. Gonzalez and R. E. Woods, *"Digital Image processing"*, ADDISON-WESLEY PUBLISHIN COMPANY, 1992.

34- K. R. Castleman, "*Digital Image Processing*", Prentice Hall 1998.

35- S. Burrus, R. Gopinath, and H. Guo, "*Introduction to Wavelets and Wavelet Transform*", Upper Saddle, New Jersey: Prentice Hall, 1998.

36- Woods J.W and Ed. *Subband Image Coding*, Boston: Kluwer, 1991.

37- Gomes G.P., Member, IEEE, Robert M.G., Fellow, IEEE, and Martin V., Fellow, IEEE, "*Vector Quantization of Image Subband: A Survey*", IEEE Trans. On Image Processing, Vol. 5, No. 2, Feb. 1996.

38- Vetterli M. and Herley C. "*Wavelet and Filter Banks: Theory And Design* " IEEE Trans. Signal Processing, Vol.40, No.9; PP.2202-2232, Sept. 1992.

39- Mohsenian N. and N. M. Nasserabadi, "*Edge-Based Subband VQ Technique for Image and Video* ", IEEE Trans. And system for video Technology, vol.4, No. 1, Feb. 1994.

40- Kim Y.H. and Modestion J. W. "*Adaptive Entropy coded Subband Coding of Image* ", IEEE Trans. Image Processing, Vol. IP-1, No. 1, PP.31-48, Jan. 1992.

41- Punya T. S. "*SAR Image Classification by Wavelet Based Texture Analysis*" 2nd International Symposium on Operationalization of Remote Sensing, Enschede, The Netherlands, 16-20 August. 1999.

42- O. Rioul and M. Vetterli, "*Wavelets and Signal processing*" IEEE Signal Processing Magazine, pp. 14-38, October 1991.

تقنية إخفاء المعلومات بالاعتماد على تحويل المويجة

الخلاصة

الكتابة الخفية هو فن اخفاء وارسال المعلومات خلال حاملات مشاعة ظاهرياً في محاولة لتخبئة وجود هذه المعاملات. تم تبني إخفاء صورة في صورة في هذا العمل.

نظام الإخفاء المقترح يستعمل التحويلات الرياضية (Mathematical Transform) في عملية الإخفاء لزيادة متانة النظام وذلك بوضع مركبات الترددات الواطئة للصورة المخفية (Signature Image) في مركبات الترددات العالية للصورة الغطاء (Host Image) بإستخدام تحويل المويجة (Haar-Wavelet Transform). وللإغراض الأمنية تعيير معاملات الصورة المخفية المحولة (مركبات التردد الواطىء) بالقسمة على قيمة معينة، هذه القيمة اختبرت لتعطي PSNR مقبولة للصورتين الناتجة (Stego-Image) والمسترجعة (Reconstructed Image) .بعد ذلك نستخدم المفتاح الخفي(Stego-Key) الذي من خلاله تحشر مركبات التردد الواطئ المعيرة للصورة المخفية (Signature Image) بترتيب معكوس في مواقع مركبات التردد العالي للصورة الغطاء (Host Image).

قيّمت اللاإقابلية على إدراك الصورة الناتجة باستخدام مقياس نسبة الذروة للإشارة مقابل الضوضاء (PSNR). تمتلك الصورة الناتجة، باختيار عوامل معينة، لاقابلية على الإدراك ممتازة عندما تكون نسبة الضوضاء إلى الأشارة بحدود ٣٠ ديسبل إو أكثر. من جهة اخرى الصورة المسترجعة تمتلك جودة جيدة ولكن ليس بنفس جودة الصورة الناتجة ويعزى ذلك لعملية التكميم أو التعيير التي رافقت عملية الإخفاء. ولابد من الإشارة إلى أن حجم الصورة المخفية في هذا العمل هو بنفس حجم أو أقل من حجم الصورة الغطاء.

وزارة التعليم العالي والبحث العلمي
جامعة بغداد
كلية العلوم
قسم علوم الحاسبات

تقنية إخفاء المعلومات بالاعتماد على تحويل المويجة

رسالة مقدمة
إلى كلية العلوم / جامعة بغداد
كجزء من متطلبات نيل شهادة الماجستير
في علوم الحاسبات

مقدم من قبل
انتصار ياسين خضير

بإشراف
الاستاذ الدكتور صالح مهدي

2004