اختيار الغطاء الملائم لاخفاء معلومات في الصور

Selection of the Appropriate Cover to Hide Information in Images

Prepared by:

Rema F. Farhat

Supervised by:

Dr. Feras Al-Mashakba

A Thesis Submitted in Partial Fulfillment of the

Requirements for Master Degree in Computer

Science

College of Computer Sciences and Informatics

Amman Arab University

2013

Authorization

I, Rema F. Farhat, authorize Amman Arab University to provide copies of my thesis to libraries, institutions or any one requesting a copy.

Name: Rema F. Farhat

Signature: .....

Date: 24/7/2013

Name: Rema F. Farhat

Degree: Master of Computer Science.

Title of thesis in Arabic:

اختيار الغطاء الملائم لإخفاء معلومات في الصور

Title of thesis in English:

Selection of the appropriate cover to hide information in the images

Examining committee	Signature
Dr. Feras Al- Mashakba	17/7/2013
Dr. Alaa Al-Hamami	Alahamami 17/7/2013
Dr. Moayyed Abd Al-Razzaq Fadil	17/7/2013

Dedication

To My husband,

My parents,

My children,

My friends,

For their care and support

Also great thanks and gratitude for my supervisor and Dr. Mohammed Nassar for their guidance and support

List of Abbreviations

BMP	Bitmap Format
CD	Compact Disk
dB	Decibel
DCT	Discrete Sine Transform
DVD	Digital Video Disk
FBS	Feature Based Steganalysis
FLD	Fisher Linear Discriminant
GIF	Graphics Interchange Format
HVS	Human Visual System
IP	Internet Protocol
JPEG	Joint Photographic Experts Group
LSB	Least Significant Bit
MB	Model Based
PNG	Portable Network Graphics
PSNR	Peak Signal-to-Noise Ratio
QMFs	Quadrature Mirror Filters
SSIS	Spread Spectrum Image Steganography
SVM	Support Vector Machine
TCP	Transmission Control Protocol
WWW	World Wide Web

List of Figures

Table of Contents

Abstract

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. In steganography the freedom to choose a cover that result in the least detectable stego image is an advantage that can be maximized. In this thesis, we proposed a new cover selection approach with four versions then we compared between them based on their ability to minimize the detectability of the resulting stego image while keeping the host image distortion as minimum as possible. Our cover selection technique versions are created by dividing the cover images and the secret image into blocks of size 4x4 and each block is divided into sub-blocks of different sizes (1x4, 4x1, 2x4, and 4x2); for each block we calculated the block texture and neighborhood information to measure the similarity of 256 blocks for the secret image as a one unit with the 4096 blocks for each cover image divided in 16 groups. Finally; the best similar cover for each version is chosen to hide the secret image using the least significant bit (LSB) technique. Our proposed methods were examined with wavelet based domain (WBS) and Fisher Linear Discriminator (FLD) to prove their robustness against detectability of the resulting stego image, also we examined the Peak signal-to-noise ratio(PSNR) to prove the ability of the four versions in maintaining minimum distortion in the host image. The results show that (1×4) blocking gives the best security and the best minimum distortion, (2×4) was the fastest version, and (1×4, 4×1, 2×4 and 4×2) were simple. Experimental results are carried out on image processing ToolBox in Matlab under windows 7, and images are randomly selected from Washington University image database by using method of the class random sample.

الملخص

إخفاء المعلومات هو فن وعلم كتابة الرسائل المخفية بطريقة أن لا أحد وبصرف النظر عن المرسل والمتلقي، يشتبه بوجود رسالة. في إخفاء المعلومات حرية اختيار غطاء التي تؤدي في الصورة stego الأقل كشفها هي ميزة يمكن تعظيمها. في هذه الأطروحة اقترحنا نهج جديد لاختيار الغطاء مع أربعة إصدارات ثم قارنا بينهما على أساس قدرتها على تقليل الكشف لـ صورة stego الناتجة مع الحفاظ على تشويش صورة المضيف إلى أدنى حد ممكن. يتم إنشاء إصدارات تقنية اختيار الغطاء عن طريق تقسيم الصورالغطاء والصورة السرية إلى كتل بحجم 4×4 و كل كتلة تقسم إلى كتل فرعية ذات أحجام مختلفة (1×4,4×2,1×4,4×2)؛ لكل كتلة حسبنا نسيج كتلة ومعلومات الجوار من الأربع جهات المجاورة للكتلة لقياس التشابه لـ 256 كتلة للصورة سرية كوحدة واحدة مع 4096 كتلة لكل صورة الغلاف مقسمة إلى 16 مجموعة. وأخيرا؛ يتم اختيار أفضل غطاء مماثل لكل إصدار لإخفاء الصورة السرية باستخدام تقنية بت الأقل أهمية (LSB). تم فحصنا طرقنا المقترحة مع مجال الموجة (WBS) و فيشر الخطي الممي (FLD) لإثبات متانتها ضد الكشف لصورة stego الناتجة ، أيضا فحصنا ذروة الإشارة إلى نسبة الضوضاء (PSNR) لإثبات قدرة الإصدارات الأربعة في الحفاظ على الحد الأدنى من التشويش في الصورة المضيفة. النتائج تبين أن طريقة التقسيم (1 × 4) يعطي أفضل أمن ، (2 × 4) كانت الإصدار الأسرع ، و(1 × 4 و 4 × 1، 2 × 4 و 4 × 2) كانت بسيطة . تتم النتائج التجريبية من على مربع الأدوات معالج الصور في Matlab تحت ويندوز 7، الصور تم اختيارها عشوائيا من قاعدة البيانات صورة جامعة واشنطن باستخدام طريقة العينة العشوائية الطبقية.

Chapter One

Introduction

Chapter One

Introduction

1.1. Introduction

Today's Internet world is full of data thieves and hackers. There is a strong need to design a system that enables the internet users to exchange their secret and private data safely.

Cryptography can achieve goal, but cryptography just transforms the sensitive data into another form which could not be understood by everyone, so that only the intended recipients with a key can unlock the data back to the original form. Therefore, the transformed cryptic data is visible to everyone, and thus may create curiosity among cyber criminals to break into the meaning of the cryptic data, though it is not that easier.

Steganography is yet another powerful tool that achieves the goal of transferring sensitive data secretly across the web.

Steganography is one of the types of information hiding, as shown in Figure 1.1.

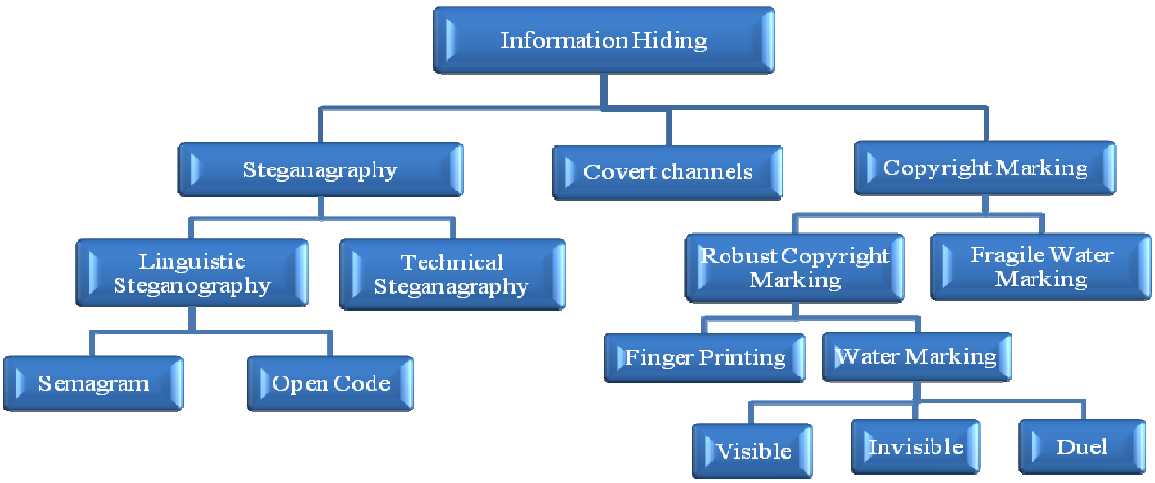

Figure 1.1: Information Hiding Hierarchy [1]

1.2. What is steganography?

Steganography is one of the most important sub disciplines of information hiding. Steganography is defined as the art and science of invisible communication. It hides information in other information (text, image, audio, video), thus hiding the existence of the communicated information [2].

The word steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning, “writing”, defining it as “covered writing”.

The primary goal of steganography techniques has been to maximize embedding rate while minimizing the delectability of the resulting stego against steganalysis techniques. However, one particular advantage of steganography, as opposed to other information hiding techniques, is that the embedder has the freedom to choose a cover that result in the least detectable stego.

1.2.1. Steganography and cryptography

Steganography differs from cryptography in the sense that cryptography focuses on keeping the contents of a message secret, but steganography focuses on keeping the existence of a message secret [3].

The existence of an encrypted message shows that someone is communicating secret information and this is the reason, why nowadays Steganography is used combined with cryptography. By this way the existence of a secret communication is erased.

1.2.2. Steganography and information hiding techniques

Steganography is one of the information hiding techniques, but Steganography unlike other information hiding techniques, the cover object in steganography acts only as a transporter for the secret data. Therefore, the embedder is allowed to choose any cover object from a database using a cover selection approach [1].

There is a difference between Steganography and watermarking, in Steganography the message is important, any alteration to the message will make it unreadable. In watermarking it is important that at least one watermark is preserved during and attack, it doesn't matter if the other marks are destroyed.

1.3. The structure of Steganography

The basic structure of Steganography is made up of three components: the cover, the message, and the key.

Message: It is the object that will hide it into cover. The message can be a text, an image, an audio, a video.

Key: is used to encode/decode the hidden message. This can be anything from a password, a pattern, random generator, hashing method, … etc.

Cover: It is defined as original media which required information is embedded and it is also called carrier. The cover (or carrier) can be a text, an mage, an audio file, a video file, even a protocol (like TCP/IP packet).

Type of object to be concealed influence in the choice of the cover, for example, if the object was a picture or video is difficult concealed within the text as if the text can be concealed inside a photo or video, as well as the audio can not be concealed within the text while can be concealed inside the audio or video.

The type of cover influence in the choice of embedding algorithm, for example, if the cover image can be used LSB or transform domain techniques or ... etc, But if the cover was audio can be use of spread spectrum or echo data hiding or ….. etc, and so on for each type its algorithms, In Section 1.6 explained types of the covers and its algorithms.

1.4. Properties of steganography

When a Steganography algorithm is evaluated the following are taken into consideration [4]:

- Capacity - the amount of information that can be hidden without altering the cover medium in such way that will attract suspicion

- Security - the difficulty of detecting the hidden information. Usually security relates to capacity - if we hide a large amount of information in a cover medium it will be easier to detect.

- Robustness - the amount of modification that the cover medium can endure before the hidden information will be destroyed.

1.5. Uses of steganography

According to Wayner [5] steganography can be used for:

- Enhanced Data Structures: hide extra information with the standard medium such as hiding information about a photo (like the year and place it was taken) in the photo itself, this way the information will "travel" along with the photo.

- Strong watermarks: used mostly for copyright of digital content such as books, movies and audio files. Some watermarks are meant to be visible such as a word in the background of a document and others are not. The invisible watermarks are used for identification purposes mostly to know how originated the document, who bought that file and distributed illegally. Watermarking technology has been embedded into DVDs and DVDs/CDs, nowadays if a DVD/CD bears a DO NOT COPY watermark, some DVD/CD writers might refuse to create a copy.

- Document-Tracking tools -the hidden information inside of a document can identify the legitimate owner of the document or the person the document was issued to - this type of identification is used mostly in digital libraries who generate a watermark barring the users id, if the file is posted over the Internet it can be tracked to the person who illegally published it.

- File Authentication -the hidden information embedded into a file can certify file authenticity.

- Private Communications - Steganography can be used for private communications by embedded information into a harmless cover.

1.6. Different kinds of Steganography

There are different kinds of Steganography which are going to be briefly described for information purposes. Due to the message topic, the emphasis will be on Steganography in images; the other domains will be briefly mentioned.

1.6.1. Steganography in Audio

This type of steganography is very difficult because the human auditory system is perceptible to background noises. The weakness of the human auditory system is that it can't differentiate between the sounds high and low sounds. It is clear that this weakness must be exploited when hiding data into audio files.

There are several methods of data hiding in audio files:

1- Low bit encoding which is somewhat similar to LSB that is generally used in images. The problem with this technique is that the human ear can notice it[6].

2-Spread Spectrum this method addsrandom noises to the signal and the information is concealed inside acarrier and spread across the frequency spectrum [6].

3- Echo data hiding this method uses the echoes in sound files in order to try and hide information [6].

1.6.2. Steganography in Video

The most commonly used method for hiding information inside a video is DCT (Discrete Cosine Transform). DCT works by slightly changing the each of the images in the video, only so much though so the human eye can't notice [6]. Steganography in Video works like the steganography in images, the difference is that the data is hidden in video frames.

Stfeld and Wolf have described a method for data hiding in a video conferencing system [7]. Because of the bandwidth necessities the videoconference systems have a special transmission system. Because of bandwidth necessities the videoconferences systems transmit only the differences between successive frames. If the information is hidden when these differences are transmitted it is very hard to detect because there is no "whole" image to compare only frames differences.

1.6.3. Steganography in text

There are several methods of hiding data into text or documents, sometimes called linguistic Steganography. The most common methods are:

- Open text methods like intersentence spacing, end of line spacing, interword spacing. The problem with these methods is that they can be easily removed from the text by a simple reformatting.

- Syntactic method - manipulates the punctuation to hide information.

- Semantic method - this method uses synonyms for primary and secondary value. For example, the word "beautiful" could be considered primary and "exhilarating" secondary. Whether a word has primary or secondary value

bears no relevance to how often it will be used, but primary words will be read as ones, secondary words as zeros when decoding [8].

- New file generation - new files are generated in order to create the message.

This latest method described is the best way to hide information inside documents because it doesn't use o cover document, but rather creates one. A popular program that can do that is: spam mimic [9].

If we encode the following text "hidden message" we obtain the following spam message:

We notice that the generated message is actually a "normal" spam message that mostly will be ignored. The advantage of this technique is that the generated spam can be send to millions of users and it will be quite impossible to know to whom that message was addressed.

1.6.4. Steganography in networks

Usually the Steganography in networks can be divided into the following categories [9]:

- Hiding in an attachment - is the basic form of sending Steganography files to another person. The message contains an attachment, a file, which has a secret message hidden inside it. The file can be an image, a audio file, video file, a document. The best transmission methods are via email, ftp, website posting.

- Hiding in a transmission - it uses special programs that hide the data into a file and then transmit the message. The previous method needed two steps: first hide the data into the cover file, and then transmit the data.

- Hiding in an overt protocol - involves camouflaging data like so it looks like something else. For example, the data transmitted can be masked so it looks like normal web traffic, even though is not.

- Hiding in network headers - it uses the headers of the TCP/IP protocol to hide data. The IP protocol header contains the necessary information for packets to be routed where is needed, so when we insert or change the data into the header we must do so we do not affect communication.

Some fields in the IP header must contain specific values such: header length version number. If we change those numbers the communication will fail. One field in the IP header thatcan be changed without affecting the communication is the IP identification number. Usually, this number is incremented by one when large packets are sent (the large packets are broken down into smaller one). A different number can be used as long as the order of the packages is respected and the protocol will work properly.

1.6.5. Steganography in Images

Images are the most popular carriers for Steganography. The techniques of hiding messages into images can be divided into Image Domain and Transform Domain [10]. The Image Domain (or spatial domain) techniques embed the message directly into the image, while the Transform domain the image is first transformed and then the message is embed into the file.

A digital image is represented as a collection of numbers that makeup different light intensities in different areas of the image [11]. The digital images may be 2D or 3D, where 2D and 3D refer to the actual dimensions in a computer's workspace. 2D is 'flat', using the X & Y (horizontal and vertical) axis', the image has only two dimensions and if turned to the side becomes a line. 3D adds the 'Z' dimension. This third dimension allows for rotation and depth. It's essentially the difference between a painting and a sculpture. The steganography in 3D images provide high capacity.

The selection of the cover image is very important. It is advisable not to use well known images because the hidden message can be found very easily .The best cover images are the ones with many details, which don't have large portion with the same color.

size of cover image that must be bigger than secret message, Where increasing security whenever the difference between the size of the message and the cover was large.

The security is decreasing whenever cover had low texture such as sky, desert, sea, ….. etc. It must be clear that changing a bit in an image might represent switching form a color pixel to another color one (like red to blue). Such a change will be immediately detected in the cover picture, imagine a red pixel in the middle of the sky.

Another thing we must be aware when we select the cover image is the image compression and how the image is going to be transmitted. There are two types of images compression "lossless" and "lossy". The difference between them is that "lossless" data compression is a type of algorithm that allows the

exact original data to be reconstructed from the original data contrast to lossy algorithm which only allows an approximation of the original data to be reconstructed. he "jpeg" images uses lossy compression while "bmp", "gif" uses the lossless compression.

Due to the fact that the transmission medium for the Steganography is mostly the Internet, the preferred compression algorithm is the lossy compression because it offers bigger compression rates.

1.6.5.1. Image steganography algorithms

This category of steganography algorithms tries to hide a message within an image cover. The most important factor of the cover image in such algorithms is the fact that how many bits of noise (parts of secret message) can be injected without perceptually deteriorating the image quality, while a noisy image would arise the interceptors' suspicion [11].

Common existing approaches of hiding information in digital images include :

- Least Significant Bit insertion (LSB): this simple approach tries to hide information within the least significant bits of pixel colors of an image (some algorithms also modify the second least significant bits). The secret may be embedded within 24-bit or 8-bit BMP or GIF images. The main disadvantage of this method is its ulnerability to even slight image manipulations. Image conversions to lossy formats can also destroy the hidden message.[12]
- Masking and filtering: these techniques usually restricted to 24-bit and gray-scale images, hide information by marking an image, similar to

paper watermarks. Since watermarking techniques are more integrated into the image, they can be applied in applications involving lossy compression. These techniques can also be applied into other multimedia (audio/video) applications.[12]

- Algorithms and transforming: unlike LSB which is vulnerable to data manipulation, these techniques can be applied on lossy compression formats like JPEG images. These approaches may help protect against image processing manipulations such as cropping and rotating. The selection of such algorithms should be accomplished according to the system mission and the environment. For example a BMP steganography algorithm may not be appropriate for Internet communication, on which JPEG images are the most popular formats because of their high quality-low size attribute. Using such an algorithm may be a hint for the opponent entities.[12]

1.6.5.2. Applications of Image ssteganography

There are many applications of Image Steganography, especially in today's modern, high-tech world. Privacy and anonymity is a concern for most people on the internet. Image Steganography allows for two parties to communicate secretly and covertly. It allows for some morally-conscious people to safely whistle blow on internal actions; it allows for copyright protection on digital files using the message as a digital watermark. One of the other main uses for Image Steganography is for the transportation of high-level or top-secret documents between international governments. While Image Steganography has many legitimate uses, it can also be quite nefarious. It can be used by hackers to send viruses and trojans to

compromise machines, and also by terrorists and other organizations that rely on covert operations to communicate secretly and safely [4].

1.7. The statement of the problem

Choosing the cover is important process in steganography, because random selection may lead to selection of inappropriate cover whose may maximize detectability and time of process , also the size may be not suitable , additionally may not meet requirements of the user needs. So the proposed method take different dividing formats (1x4, 4x1, 2x4, 4x2 and mix) in order to improve Steganography in terms of security, complexity and time.

1.8. Methodology

The proposed work includes:

- Selecting a secret image

Here, the user will insert a secret image that he/she wants hide .

- Dividing to blocks

The system will divide a secret image and cover images to blocks.

- Extracting features

The system will extract statistics for each block and neighbors at four sides of a block.

- Finding similarities

The system will compare features of a secret image and features of cover images to find the best host image (the most similarity).

- Hiding the secret image

After finding the best host image, the system will hide the secret image into the best host image by using LSB.

- Steganalysis and measuring of quality of the image.

The system is measuring of quality of the image by use PSNR and evaluating the security of the method by using WBS/FLD.

1.9. Thesis Organization

This thesis includes five chapters. Chapter one is an introduction. Chapter two that describes several studies and literately work done on steganography and techniques used for improving steganography. Chapter three includes image steganography and steganalysis. Chapter four describes the proposed technique, experimental and presents results of method, and comments about the results after each table. Finally, chapter five presents some conclusions and a number of recommendations for future work.

Chapter Two

Literature Reviews

Chapter Two

Literature Reviews

2.1. Introduction

Image steganography is used to embed covert information in image. The intent is to transmit hidden information. Steganalysis is the process used to detect hidden messages in images. Although steganography is not a new discipline, it has become increasingly important in today's digital world where information is often and easily exchanged through the Internet, email, and other means using computers. The need for better methods and techniques which can be used to embed hidden information in images . Since the last century many research and studies were conducted for introducing a steganography technique that provides security, capacity, and robustness. Some research and studies were selected and based on the similarity , other based on correlation characteristic, there studies use contourlet transform to introduce secure steganography, there methods were based on complexity of a cover image, and …..etc, also their some methods use spatial domain, another methods use frequency domain techniques, and …etc. In this chapter, the related literatures review is discussed.

2.2. Literature reviews

Z. Kermani[13] developed an algorithm for providing a high level of capacity, robustness and also similarity, while maintaining the minimum distortion in the host image(s). The main idea is based on dividing the secret image into blocks of size 4*4. Each block in secret image is taken

as a texture pattern for which the most similar block is found among the blocks of the host image. The embedding procedure is carried on by replacing these small blocks of the secret image with blocks in host image in such a way that least distortion would be imposed on it. They used Gabor filter to measure the similarity between texture patterns. The location addresses of blocks in host image which are replaced by blocks of secret image are saved. This data is converted to a bit string and then modified by Hamming code. This bit string is embedded in DCT coefficients of the modified host image using a key which is the seed of a random number generator.

The experimental results showed a high level of capacity, robustness and minimum distortion on standard images to achieve more capacity and also decrease host image distortion. They introduced the idea of embedding the secret image into more than one host image. Therefore, an image database using which the most suitable host images were found.

Kharrazi [14] investigated in problem of cover selection by three scenarios in which the embedder has either no knowledge, partial knowledge, or full knowledge of the steganalysis technique. Experimentation illustrated how a number of simple measures could improve the chances of undetectability by the steganalyzer, and investigated the performance due to the use of each measure, as observed that common distortion measures like MSE and prediction error are not necessarily good measures in quantifying the steganographic embedding distortion. That is a decrease in distortion measured between the cover-stego pair does not increase the chances of raising a false alarm. The reverse holds true as well. The increased distortion, introduced to the

cover image, results with a less accurate estimate of the cover, and correspondingly the classifiers ability to distinguish between cover and stego images diminishes. For the no knowledge case, the results indicate that minimizing the number of changes made to the cover image serves as a reliable measure. On the other hand, in the partial knowledge case, despite their simplicity, MSE and the number of changeable coefficients seem to be more effective measures in selecting a less detectable cover image. The superiority of these measures over perceptual measures, like SSIM and Watson's metric, also indicates that steganographic embedding distortion has to be quantified in a statistical (rather than perceptual) manner. In addition, as the partial knowledge , in terms of the size of test stego set, increases from 10 to 100 the cover selection method becomes more effective , and the improvement due to increase to 500 is rather marginal.

Hedieh [15] proposed the blocks of secret image are compared with blocks of a set of cover images and the image with most similar blocks to those of the secret image is selected as the best candidate to carry the secret image, and hiding only blocks indices (location addresses) in DCT coefficients of host image.

This method uses statistical features of image blocks and their neighborhood. Using the block neighborhood information and consequently, prevent appearing virtual edges in the sides and corners of the replaced blocks.

The main achievements of the proposed steganography method are: (i) reduction of the host image distortion, and (ii) increased security.

Yifeng [16] introduced a method for cover selection is based on the correlation characteristic in cover data, and they find that the covers whose data have smaller correlation characteristic are "better".

This work shows that the point of view is obtained from Gauss-Markov cover model and spread spectrum embedding model. Note that Gauss-Markov cover model still has a gap with the practical multimedia data, for example digital image. The effect of the gap on the security of steganography is still a question. But in the experiments, for image spatial domain steganography, the images that have smaller correlation parameters are more difficult in discriminating cover with stego than the images that have larger correlation parameters.

Sajedi [17] introduced method is based on embedding the secret data in contourlet coefficients via an iterative embedding procedure to reduce the stego image distortion.

The proposed steganography method primarily decomposes the cover image by contourlet transform. Every bit of secret data is embedded by increasing or decreasing the value of one coefficient in a block of a contourlet subband. Contourlet coefficients are manipulated relative to their magnitudes to hide the secret data adaptively. This work investigates the effect of cover selection on steganography embedding and steganalysis results.

The proposed cover selection measures illustrated through the experimentation that applying improve the undetectability of stego images by the steganalyzers. Image complexity criterions are very fast measures to select a proper cover image from the database, but they are not very

precise. In contrast, exact measures are slow but introduce the best cover image with respect to the secret data. The results indicate that the amount of changes and visual quality measures are reliable criterions for cover selection. Finally, the results show that by using cover selection one can embed much more bits in a suitable cover image.

Chapter Three

Image Steganography and Steganalysis

Chapter Three
Image Steganography and Steganalysis

3.1. Introduction of images

An image is defined as an arrangement of numbers and such numbers usually stand for different light intensities in different parts of the image [11]. The numeric description takes the form of a lattice where the individual points given the name 'pixels'. Pixels are displayed horizontally, row by row. In a color scheme, the number of bits is known as the bit depth and this basically refers to the number of bits assigned to each pixel [18]. Moreover, the smallest bit depth in the color scheme is 8, i.e., 8 bits are utilized to represent the color of each pixel. The gray scale images usually utilize 8 bits for each pixel and such bits are capable of displaying up to 256 different colors or shades of gray. One more point to add is that digital color images are known for being saved in 24-bit files and for utilizing the RGB color model. Almost all the color variations for the pixels of a 24-bit image are derived from three basic color terms: red, green, and blue, and each of these colors is represented by 8 bits [11].

The most prominent image formats, exclusively on the internet, are the Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPEG) format, and to a lesser degree, the Portable Network Graphics (PNG) format. The important issue to touch here is that most of the steganographic techniques attempt to exploit the structure of these formats. However, some literary contributions use the bitmap format (BMP) simply because of its simple and uncomplicated data structure [19, 22].

3.2. Image steganography

Images are considered as the most popular file formats used in steganography. They are known for constituting a non-causal medium, due to the possibility to access any pixel of the image at random. In addition, the hidden information could remain invisible to the eye. However, the image steganography techniques will exploit "holes" in the Human Visual System (HVS).

The JPEG file format is the most common image file format on the internet owing to the small size of resultant images obtained by using it.

3.2.1. Image Steganographic Techniques

There are quite a lot of approaches in classifying steganographic techniques. According [21] these approaches can be classified according both the methods that modify the image file format as following:

- Spatial domain
- Transform domain
- Spread spectrum
- Statistical methods
- Distortion techniques

Spatial Domain Technique

Spatial domain steganographic techniques, also known as substitution techniques which are a group of relatively simple techniques that create a covert channel in the parts of the cover image in which changes are likely to be a bit scant when compared to the human visual system (HVS).One of the ways to do so is to hide information in the least significant bit (LSB) of the image data [21].

This embedding method is basically based on the fact that the least significant bits in an image can be thought of as random noise, and consequently they become not responsive to any changes on the image [22].

In computer science, the term Least Significant Bit (LSB) refers to the smallest (right-most) bit of a binary sequence. The structure of binary is such that each integer may only be either a 0 or a 1, often thought of as off and on respectively. Starting from the right, the value (if on) denotes a 1. The value to its left (if on) denotes a 2, and so on where the values double each time. Now let us consider the following 8-bit binary sequence:

1 0 1 1 0 0 1 1

If we now think of each 8-bit binary sequence as a means of expressing the color of a pixel for an image, it should be clear to see that changing the LSB value from a 0 to a 1 will only change the color by +1 - a change that is unlikely to be noticed with the naked eye[23].

The advantages of LSB techniques are:

- Popularity
- Easy to understand and comprehend
- High perceptual transparency.
- Low degradation in the image quality
- It has good embedding capacity and the change is usually visually undetectable to the human eye

LSB Algorithm

From [11] algorithm for LSB Based embedding and extracting process is given as:

- **A LSB-based Embedding Algorithm**

Input -: cover C

for i = 1 to Length(c), do

S□ ← Cj

for i = 1 to Length(m), do

Compute index j□ where to store the i message bit of m

S□□ ← LSB(C□□) = m□

End for

Output -: Stego image S

- **A LSB-based Extracting Algorithm**

Input -: Secret image s

for i = 1 to Length (m), do

Compute index j□ where to store the i message bit of m

m□□ ← LSB(C□□)

End for

In the extraction process, the embedded messages can be readily extracted without referring to the original cover-image from the given stego-image S. The set of pixels storing the secret message bits are selected from the stego-image, using the same sequence as in the embedding process. The n LSBs of the selected pixels are extracted and lined up to reconstruct the secret message bits [11].

3.2.1.1. Transform Domain Techniques

The process of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain[24].

The major JPEG steganographic methods can be described as follows:

- **JSteg/JPHide**. Jsteg and JPHide are two classic JPEG steganographic tools that employ the LSB embedding technique [24]. JSteg functions to hide the secret data in a cover image by simply exchanging the LSBs of non-zero quantized DCT coefficients with secret message bits. The quantized DCT coefficients, already used to conceal secret message bits in JPHide, are selected randomly by a pseudo-random number generator[3].
- **F5**. The F5 steganographic algorithm was introduced by Westfeld [25]. The absolute value of the coefficient is reduced by the F5 algorithm by one if it needs modification. Due to the author's argument, the use the chi-square attack can never detect this type of embedding [26]. In addition to embedding message bits into randomly chosen DCT coefficients, the F5 algorithm employs matrix embedding that reduces the number of changes necessary for hiding a message of a certain length[27].
- **OutGuess**. OutGuess is provided by Provos as a UNIX source code[28]. There are two stages representing the embedding process of OutGuess. The first one is that OutGuess embeds secret message bits along a random walk into the LSBs of the quantized DCT coefficients while skipping 0s and 1s.Soon after modifications are made to the coefficients, they already left during embedding to make the global DCT histogram of the stego image match that of the cover image. OutGuess cannot be subjected to a chi-square attack [27, 26].

- **MB**. Model-based steganography (MB) can be defined as a general framework for conducting both steganography and steganalysis by simply using a statistical model of the cover media [29]. The MB method for JPEG images is capable of having high message capacity while remaining secure against many first-order statistical attacks [27].

3.2.1.2. Spread Spectrum Technique

Spread spectrum either deals with the cover image as noise or tries to add pseudo-noise to the cover image.

- **Cover image as noise**

  A system that treats the cover image as noise can add a single value to that cover image. This value must be transmitted below that noise level. This means that the channel capacity of the image changes significantly. Thus, while this value can be a real number, in practice, the difficulty in recovering a real number decreases the value to a single bit. To permit the transmission of more than one bit, the cover image has to be broken into sub images [21]. When these sub cover images are tiles, the technique is referred to as direct-sequence spread spectrum steganography. When the sub cover images consist of separate points distributed over the cover image, the technique is referred to as frequency-hopping spread-spectrum steganography[26].

- **Pseudo-noise**

  This technique shows that the hidden data is spread throughout the cover image and that is why it becomes difficult to detect. Spread Spectrum Image Steganography (SSIS) described by Marvel et al.,

combined spread spectrum communication, error control coding, and image processing to hide information in images, is an example of this technique [21].

In SSIS, the process goes like this: the message is hidden in noise and then it is combined with the cover image to reach into a stego image. Since the power of the embedded signal is much lower than the power of the cover image, the embedded image becomes imperceptible[24].

3.2.1.3. Statistical Methods

Also known as model-based techniques, these techniques tend to modulate or modify the statistical properties of an image in addition to preserving them in the embedding process. This modification is typically small, and it is thereby able to take advantage of the human weakness in detecting luminance variation [22].

Statistical steganographic techniques exploit the existence of a "1-bit", where nearly a bit of data is embedded in a digital carrier. This process is done by simply modifying the cover image to make a sort of significant change in the statistical characteristics if a "1" is transmitted, otherwise it is left unchanged[30]. To send multiple bits, an image is broken into sub-images, each corresponding to a single bit of the message [21].

Another technique, called data masking, has been proposed in [31].

3.2.1.4. Distortion Techniques

Distortion techniques require knowledge of the original cover image during the decoding process where the decoder functions to check for differences between the original cover image and the distorted cover image in order to restore the secret message. On the other hand the

encoder adds a sequence of changes to the cover image[31]. So, information is described as being stored by signal distortion [32].

Using this technique, a stego-object is created by applying a sequence of modifications to the cover image. This sequence of modifications is selected to match the secret message required to transmit [30]. However, the need for sending the cover image limits the benefits of this technique. As in any steganographic technique, the cover image should never be used more than once. If an attacker tampers with the stego-image by cropping, rotating, or scaling, the receiver can easily detect the modification[21].

3.2.2. Performance measure of steganography

As a performance measure for image distortion due to embedding, the well-known peak-signal-tonoise ratio (PSNR), which is categorized under difference distortion metrics, can be applied to stego images [15][2]. It is defined as:

$$\mathbf{PSNR = 10\ log_{10}\frac{L}{MSE}} \qquad \textbf{(3.1) ….. [15]}$$

$$\mathbf{MSE = \frac{1}{N}\sum_{i=1}^{N}(X_i - \overline{X}_i)^2} \qquad \textbf{(3.2) ….. [15]}$$

Where:

L: The maximum gray level value

X□: The intensity value of the pixel in the cover image.

$\overline{X}_i$: The intensity value of the pixel in the stego image.

N: Size of an Image.

3.3. Steganalysis

Steganalysis is the art and science of detecting messages hidden using steganography. . The art of steganalysis plays a major role in the selection of features or characteristics a typical stego message might exhibit while the science helps in reliably testing the selected features for the presence of hidden information.

Steganalysis can be classified into two broad categories:

3.3.1. Target steganalysis

Specific/Targeted Steganalysis: Specific steganalysis also sometimes knows as targeted steganalysis is designed to attack one particular type of steganography algorithm. The steganalyst is aware of the embedding methods and statistical trends of the stego image if embedded with that targeted algorithm. This attack method is very effective when tested on images with the known embedding techniques whereas it might fail considerably if the algorithm is unknown to the steganalyst. For example, Fridrich et al. broke the F5 algorithm by estimating an approximation of cover image using the stego image [34]. Bohme and Westfeld broke the model-based steganography [29] using analysis of the Cauchy probability distribution [35]. Jsteg , which simply changes the LSB of a coefficient to the value desired for the next embedded data bit, can be detected by the effect it has of equalizing adjacent pairs of coefficient values [26].

3.3.2. Blind/Generic/Universal Steganalysis:

Blind steganalysis also known as universal staganlysis is the modern and powerful approach to attack a stego media since this method does not depend on knowing any particular embedding technique. This method can

detect different types of steganography content even if the algorithm is not known. However, this method cannot detect the exact algorithm used to embed data if the training set is not trained with that particular stego algorithm. The method is based on designing a classifier which depends on the features or correlations existing in the natural cover images. The most current and popular methods include extracting statistical characteristics (also known as features) from the images to differentiate between cover and stego images. A pattern recognition classifier is then used to differentiate between a cover images and a stego image.

Each steganalyzer is composed of feature extraction and feature classification components.

3.3.2.1. Feature extraction

The first step in steganalysis is used to find and calculate features which are able to capture statistical changes introduced in the image after the embedding process. To find the features of an image there are many methods:

3.3.2.1.1. Wavelet Based Steganalysis (WBS)

The decomposition employed here is based on separable quadrature mirror filters (QMFs). As illustrated in Fig. 3.1, this decomposition splits the frequency space into multiple scales and orientations. This is accomplished by applying separable lowpass and highpass filters along the image axes generating a vertical, horizontal, diagonal and lowpass subband. Subsequent scales are created by recursively filtering the lowpass subband. The vertical, horizontal, and diagonal subbands at scale i = 1; …; n are denoted as V□(x; y), H□(x; y), and D□(x; y), respectively [36].

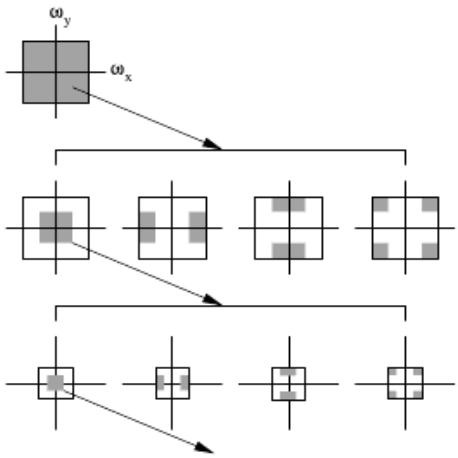

Figure 3.1: An idealized multi-scale and orientation decomposition of frequency space.Shown, from top to bottom, are levels 0, 1, and 2, and from left to right, are the lowpass, vertical, horizontal, and diagonal subbands.[36].

The statistical model is composed of the mean, variance, skewness and kurtosis of the subband coefficients at each orientation and at scales i = 1; .. ; n-1. These statistics characterize the basic coefficient distributions. The second set of statistics is based on the errors in an optimal linear predictor of coefficient magnitude.

In[16] the subband coefficients are correlated to their spatial, orientation and scale neighbors, as illustrated in Fig. 3.2.

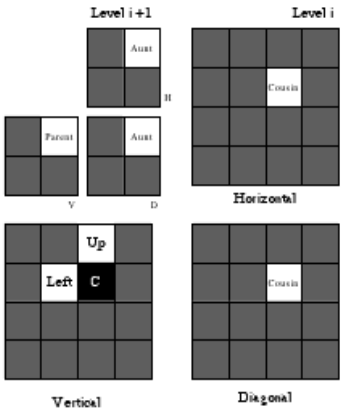

Figure 3.2: Subset of wavelet coefficients surrounding a given coefficient (C), that are potentially suitable for conditioning [37].

For purposes of illustration, consider first a vertical band, V□ (x; y), at scale i. A linear predictor for the magnitude of these coefficients in a subset of all possible neighbors 1 is given by[36]:

$$V\square(x; y) = w1Vi(x - 1; y) + w2Vi(x + 1; y) + w3Vi(x; y - 1) + w4Vi(x; y + 1) + w5Vi+1(x=2; y=2) + w6Di(x; y) + w7Di+1(x=2; y=2); \quad (3.3)$$

Where wk denotes scalar weighting values. This linear relationship is expressed more compactly in matrix form as:

$$V = Qw; \quad (3.4)$$

where the column vector w = (w1 : : : w7)T , the vector V contains the coefficient magnitudes of Vi(x; y) strung out into a column vector, and the columns of the matrix Q contain the neighboring coefficient magnitudes as specified in Equation (1) also strung out into column vectors. The coefficients are determined by minimizing the quadratic error function:

$$E(w) = [V - Qw]. \quad (3.5)$$

This error function is minimized by diferentiating with respect to w:

$$dE(w)=dw = 2QT [V - Qw]; \quad (3.6)$$

setting the result equal to zero, and solving for w to yield:

$$w = (Q\square Q)^{-1}Q\square V \quad (3.7)$$

The log error in the linear predictor is then given by:

$$E = \log2(V) - \log2(\lvert Qw \rvert) \quad (3.8)$$

It is from this error that additional statistics are collected namely the mean, variance, skewness, and kurtosis. This process is repeated for

each vertical subband at scales i = 1; …. ; n - 1, where at each scale a new linear predictor is estimated. A similar process is repeated for the horizontal and diagonal subbands. The linear predictor for the horizontal subbands is of the form:

$$Hi(x; y) = w_1 Hi(x - 1; y) + w2Hi(x + 1; y) + w3Hi(x; y - 1) + 4Hi(x;y + 1) + w5Hi+1(x=2; y=2) + w6Di(x; y) + w7Di+1(x=2; y=2); \quad (3.9)$$

And for the diagonal subbands:

$$Di(x; y) = w1Di(xi\ 1; y) + w2Di(x + 1; y) + w3Di(x; yi\ 1) + w4Di(x; y + 1) + w5Di+1(x=2; y=2) + w6Hi(x; y) + w7Vi(x; y), \quad (3.10)$$

The same error metric, Equation (6), and error statistics computed for the vertical subbands, are computed for the horizontal and diagonal bands, for a total of 12(n-1) error statistics. Combining these statistics with the 12(n-1) coefficient statistics yields a total of 24(n - 1) statistics that form a feature vector which is used to discriminate between images that contain hidden messages and those that do not [36].

3.3.2.1.2. Feature Fased Steganalysis (FBS)

Calibrated Features:

Two types of features were used in analysis – first order features & second order features. All features were constructed in the following manner. A vector functional *F* is applied to the stego JPEG image *J1*. This functional could be global DCT

coefficient histogram, a cocurrence matrix, spatial blockiness. The stego image *J1* is decompressed to the spatial domain, cropped by 4 pixels in each direction and then recompressed with the same quantization as *J1* to obtain *J2*. The same vector functional *F* is then applied to *J2*. The final feature *f* is obtained as an *L1* norm of the difference

$$f = \| F(J1) - F(J2) \|$$

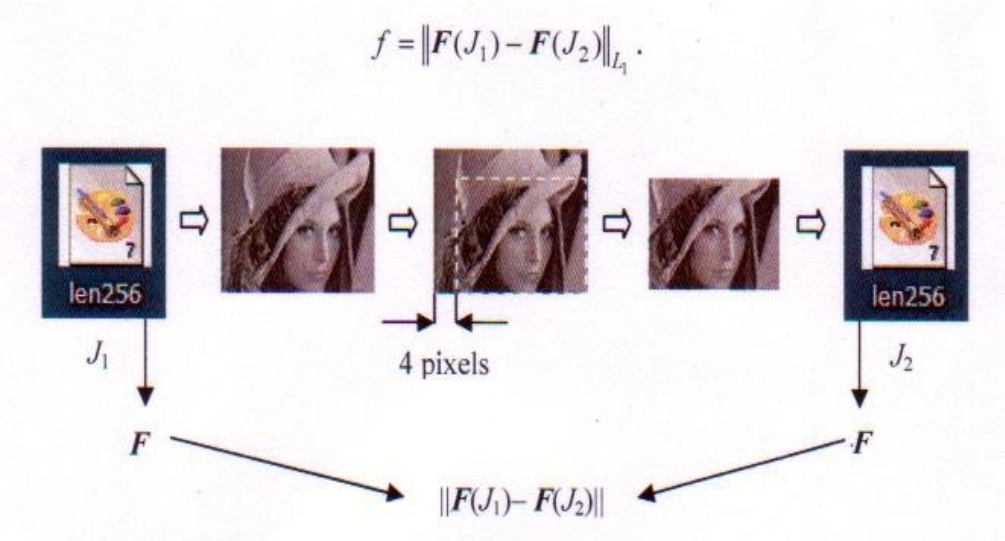

Figure 3.3: Constructed Features Manner[38]

3.3.2.2. Classification

The second component of a steganalyzer is classification, and is done based on some inherent "features" of typical natural images which can get violated when an image undergoes some embedding process.

Classifier is defined as "a mechanism or algorithm which takes an unknown variable and gives a prediction of the class of that variable as an output. Before a classifier can be used, it has to be

trained with a given data set which includes variable from different classes [39]". And below explain two of classifiers:

3.3.2.2.1. Support Vector Machine (SVM)

SVM is using to determine whether a test image contains a message, from the measured statistics of a training set of images with and without hidden messages [36].

Support vector machines separate the deferent classes of data by a hyperplane, where SVM approach seeks to find the optimal separating hyperplane between classes by focusing on the training cases. These training cases are called support vectors. Training cases other than support vectors are discarded. This way, not only is an optimal hyperplane fitted, but also less training samples are effectively used; thus high classification accuracy is achieved with small training sets (Mercier and Lennon 2003). This feature is very advantageous [40][41].

There are three classes of SVM:

a) Linear Separable SVM
b) Linear Non-Separable SVM
c) Non-Linear SVM

3.3.2.2.2. Fisher's Linear Discriminant (FLD)

Fisher's linear discriminant (FLD), is also known as Linear discriminant analysis (LDA), after its inventor, Ronald A. Fisher, who published it in The Use of Multiple Measures in Taxonomic Problems (1936)[42].

Fisher's linear discriminant is a classification method that projects high-dimensional data onto a line and performs classification in this one-dimensional space. The projection maximizes the distance between the

means of the two classes while minimizing the variance within each class [43].

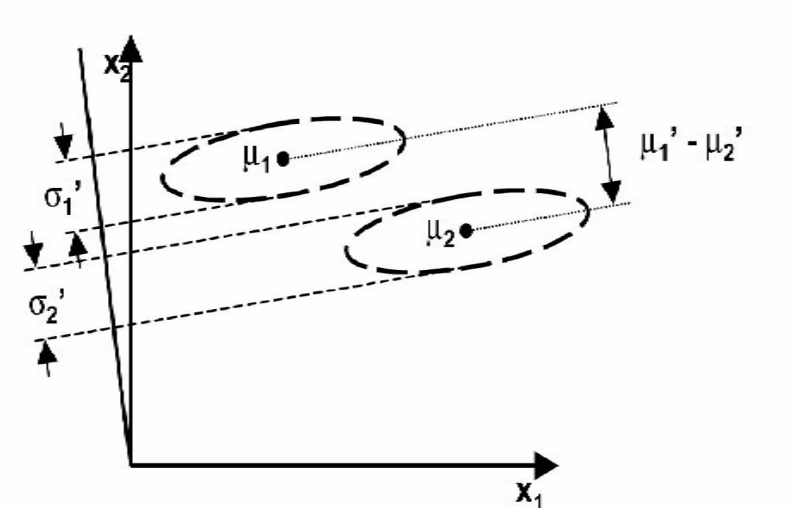

Figure 3.4: Fisher Linear Discriminant Maximizes the Distance between two Classes while Minimizing the Variance within each Class [42]

Fisher's Linear Discriminant: Algorithm

1. Estimate class means m_j and covariance matrices S_j , and prior probabilities, p_j.

2. Compute pooled covariance matrix,W.

3. Invert matrix W (using some standard matrix inversion procedure).

4. Compute the discriminant vector, α.

5. Apply the discriminant using equation y= α□x.[43].

Chapter Four

System Implementation

Chapter four
System Implementation

4.1. Introduction

This chapter includes the proposed method, experimental and results of a proposed steganography technique. The main idea is based on dividing the cover images and secret image into blocks of size 4×4, and then we have used five formats to divide the blocks into sub-blocks. we have used block texture combined with neighborhood information to measure the similarity of blocks, and LSB algorithm to embed the blocks of secret image into the most similar blocks in the best host image. Our experimental results showed a high level of capacity, minimum time of embedding process and maximum a security. In this way, we present a method for image hiding that uses the concept of block similarity between host and secret images. The stego and restored secret images have low quality and we verified that, using recent powerful blind steganalyzer.

4.2. Tools

This section describes methods and tools used in this thesis which are:

1. Using image processing ToolBox in Matlab under windows 7.
2. Using image database contained 330 JPEG images as covers images of size 256×256, and 110 images as secret images of size 64×64. The images are randomly selected from Washington University image database[44].
3. Using LSB for embedding and extracting the secret image.
4. Using PSNR to examine the proposed method.

5. Using blind steganalysis to evaluate the security of the proposed algorithm that use features constructed in wavelet domain (WBS), and a Fisher Linear Discriminator (FLD) for training and testing..

4.3. Working Process

Work process follows the following stages:

4.3.1. Feature extraction

Image texture would be used to categorize the images. All the images are divided into blocks of size 4×4, and each block is divided to sub-blocks. There are five methods (1x4, 4x1, 2x4, 4x2 and mix) to divide the blocks to sub-blocks. The figures 4.1, 4.2, 4.3, 4.4 show the dividing formats:

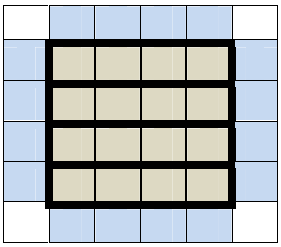

Figure.4.1: Dividing the Block into Sub-blocks of Size 1x4

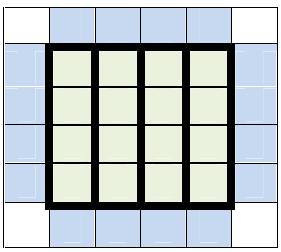

Figure 4.2: Dividing the Block into Sub-blocks of Size 4x1

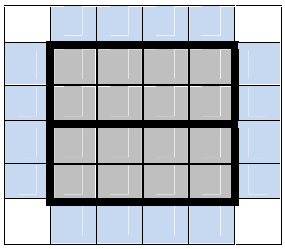

Figure 4.3: Dividing the Block into Sub-blocks of Size 2x4

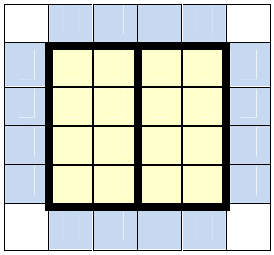

Figure 4.4:. Dividing the Block into Sub-blocks of Size 4x2

The fifth format is mix of the previous formats.

4.3.2. Finding the similarity

The similarity between secret and cover images blocks would be computed through measuring of image texture that was statistical values (mean, variance, and skewness) of sub- blocks and, the neighborhood information of four pixels that are adjacent to each side of a 4×4 block. The measure of neighborhood would be the mean of 4 sides. In 2 cases (1x4 and 4x1) sub-block, a 16 dimensional feature vector is obtained (12 statistical values and 4 neighborhood mean values). And other 2 cases (2x4 and 4x2) sub-block a 10 dimensional feature vector is obtained (6 statistical values and 4 neighborhood mean values). By searching a host image from image database, the image which provides the best similarity to the secret image will be selected.

4.3.3. Finding the best cover image and Hiding

Due to the cover image has 4096 blocks (feature vectors) and the secret image has 256 blocks (feature vectors). Therefore, the feature vectors of a cover image could be divided to 16 groups and each group has 256 feature

vectors. For finding a best cover and similar to a secret image the feature vectors extracted from the secret image is compared to each group, then computation the average of similarity of the groups. Euclidean distance is applied to measure the closeness of cover images in database to a secret image. This procedure is carried on for all cover images in database and finally, the image that has most similarity is chosen to be the host image. After cover image selection, secret image is embedding to the selected cover image. The used algorithm for that is a Least Significant Bit (LSB).

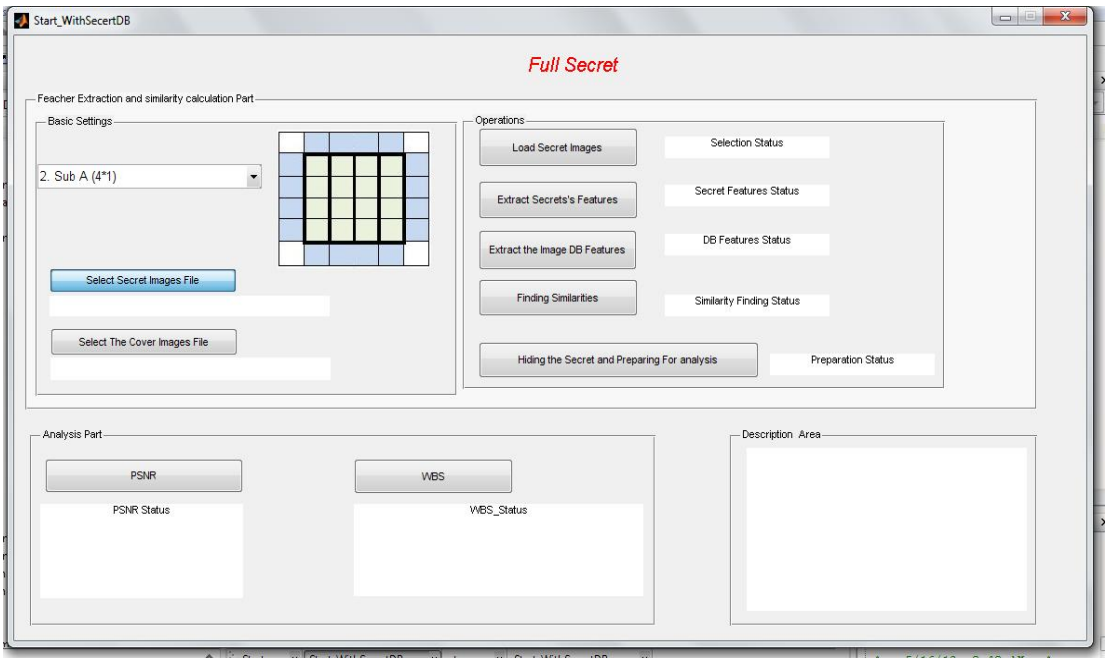

Figure 4.5: The Stages of Working Process

The 4.5 is divided to 4 parts. These parts will show how the system will operate:

1. The Basic settings

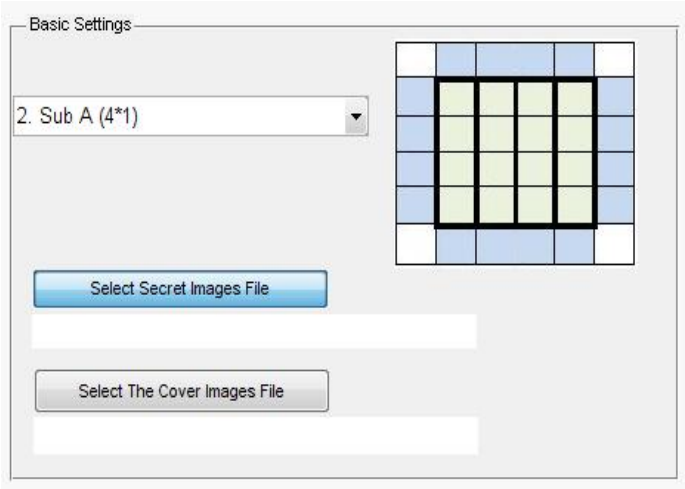

Figure 4.6: Basic Settings

In this part the user will be select the following:

1.1. Dividing format of the blocks of both secret and cover images.

1.2. Directory of the secret images.

1.3. Directory of the cover images.

2. The operations in this system

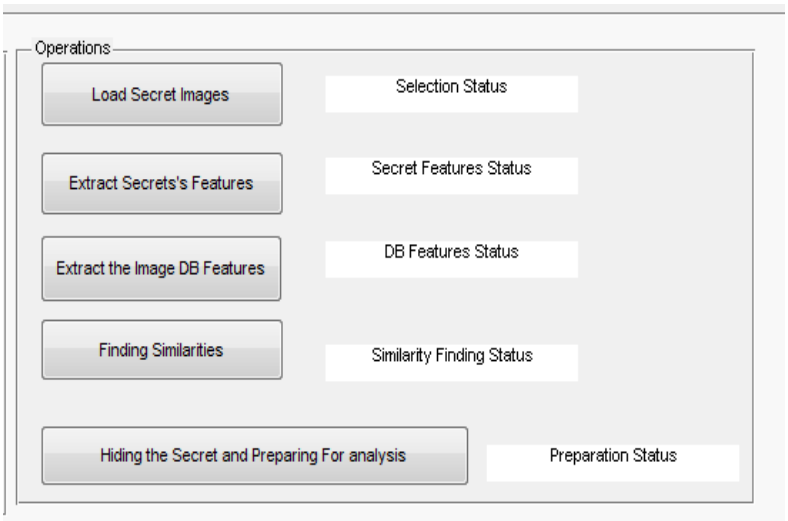

Figure 4.7: System Operations

In this part the user will be process steps of a method to embed the secret images in cover images, these steps as following:

2.1. Load secret images

In this step the system will be load the secret images from a selected folder in a past part, and resolution a size of all secret images 64x64.

2.2. Extract secret's features

Here the system will be divide all secret images into blocks, each image has 256 blocks and then extract features (statistics) for each block.

2.3. Extract the image database features

The system will be divide all cover images into blocks, each cover has 4096 blocks, and then extract features (statistics) for each block. Thus each cover image has 4096 feature vectors.

2.4. Finding similarities

In this step the system compare all feature vectors of each secret image with all feature vectors of all cover images, and the cover that has large number from similar blocks will be chosen as a best cover to embed a secret image into it.

3. Analysis part

Figure 4.8: Analysis Window

In this part the system will be analysis the proposed method by using wavelet based steganalysis (WBS) and fisher linear discriminant (FLD),

also in this part evaluation of a method by using peak signal to noise ratio (PSNR). And it will be show the results.

4. Description Area

Figure 4.9: Description Area

In this part the operations of a proposed method is descript.

4.4. Experiments

Different experiments were done to examine the proposed method

4.4.1. Peak signal-to-noise ratio(PSNR)

It is the measure of quality of the image by comparing the cover image with the stego image, i.e., it measures the statistical difference between the cover and stego image, is calculated using Equation 1, 2.

$$\text{PSNR} = 10 \log_{10} \frac{L}{\text{MSE}} \qquad \textbf{(1) ……. [15]}$$

$$\text{MSE} = \frac{1}{N} \sum_{i=1}^{N} (X_1 - \bar{X}_1)^2 \qquad \textbf{(2) ……. [15]}$$

4.4.2. Steganalysis

In this section, we evaluate the security of the proposed algorithm using blind steganalyzer that use features constructed in wavelet domain (WBS). A Fisher Linear Discriminator (FLD) is trained to discriminate clean and stego images.

Experimental Results

4.4.3. Results by using PSNR

This section presents results of using the PSNR to examine the proposed method (measure of quality of the image). And following table show of stego and restored secret image PSNR for a proposed method.

	Average Stego Image PSNR	**Average Restored Secret Image PSNR**
Proposed method	37.11	22.43

Table 4.1: Comparison of Stego and Restored Secret Image PSNR Between a Previous Method and a Proposed Method

This table shows that the average of PSNR of our proposed method, where are 37.11 for stego image and 22.43 for restored secret image.

4.4.4. Results by using steganalysis technique

In this section the WBS is firstly used to calculate features in wavelet domain, and then the FLD is trained and tested for classification of the images. The detection accuracy is shown in Table 4.2.

	Steganalyzer	False Positives	True Positives	Detection Accuracy	Time	Complexity
Proposed method(1×4)	WBS(FLD)	73.51%	26.49%	26.49%	1:50:64	Simple
Proposed method(4×1)		31.8%	68.19%	68.19%	1:50:69	Simple
Proposed method(2×4)		62.92%	37.07%	37.07%	1:48:55	Simple
Proposed method(4×2)		42.72%	57.28%	57.28%	1:48:57	Simple
Proposed method(mix)		35.32%	64.68%	64.68%	1:52:67	complex

Table 4.2: Blind Steganalyzer Detection Accuracy.

Table 4.2 shows that the proposed method cannot be reliably detected by WBS (FLD) steganalyzer.

The Detection in the proposed method is bad , where detection accuracy of dividing formats (1×4, 4×1, 2×4, 4×2 and mix) are (26.49%, 68.19%, 37.07%, 57.28%, 64.68%) respectively.

While the time in the proposed method is good, where the time of all dividing formats are (1:50:64,1:50:69,1:48:55,1:48:57,1:52:67) with (1×4,4×1,2×4, 4×2 and mix) dividing formats respectively.

All dividing formats in the proposed method are simple except (mix) dividing format is complex.

When the user wants to hide a secret message, the priority can be recognized, if the priority of the user is the security then (1×4) format is

the best dividing format, while the priority is the time then the best format is (2×4) dividing format, and if he/she wants simplicity then all dividing formats is appropriate except (mix) dividing format.

Chapter Five

Conclusion and Recommendations for Future Works

Chapter five

Conclusion and Future Work

5.1. Introduction

Image steganography systems can be considered secure if it is impossible for attackers to detect the presence of a hidden message in the stego image by using any accessible means. Therefore, the hidden message must be invisible both perceptually and statistically in order to avoid any suspicions of attackers. Moreover, a steganography system is perfectly secure if the statistics of the cover image and the stego image are identical. However, a steganography system fails if an attacker is able to prove the existence of a secret message or if the embedding technique arouses suspicions of attackers. In addition to the security, steganography capacity is important issue in the evaluation of the steganography, and where Steganographic capacity is the maximum number of bits that can be embedded in a given cover image with a negligible probability of detection by an adversary, while the embedding capacity is the maximum number of bits that can be embedded in a given cover image, therefor each steganography methods is seeking to increase the steganographic capacity and enhance security.

5.2. Conclusion

The primary goal of steganography techniques is to maximize embedding rate while minimizing the detectability of the resulting stego against steganalysis techniques, and minimizing time of embedding process .

Comparing previous method with the dividing formats of proposed method (1×4, 4×1, 2×4, 4×2 and mix); results showed that (1×4) provided the best security, (2×4) was the fastest, and with regard to a complexity all the formats were simple except (mix) dividing format.

Also if the priority of user is the speed then (2×4) is the most appropriate, and if the user is wanted the most secure method (1×4) is the most suitable, but if he is not want complex method then he must choose any dividing format except (mix).

the experimental of a proposed method proved high level of security and minimize time of the process, but it had disadvantage; the quality of the reconstructed secret image was somewhat low.

5.3. Future Works

Multiple contributions are advised to be followed for future work such as:

- Using another technique to embed a secret image into a cover image such as transform domain techniques or spread spectrum technique or statistical methods or ….. etc.
- Using another similarity measure to find the best host image such as Gabor filter or cross-correlation coefficient or ….. etc .
- Using another steganalyzer to evaluate the security such as FBS for feature extraction and SVM for classification.

References:

[1].Indradip Banerjee, Souvik Bhattacharyya and Gautam Sanyal. An Approach of Quantum Steganography through Special SSCE Code. EBSC.2011.

[2]. T. Morkel, J.H.P. Eloff, and M.S. Oliver. "An overview of image steganography." in Proc. ISSA, pp. 1-11, 2005.

[3]. Abbas Cheddad and others. "Digital image steganography: survey and analysis of current methods". Signal Processing Journal. 90(3), pp. 727-752, 2010.

[4]. Abbas Westfeld and Gritta Wolf, "Steganography in a Video Conferencing System, Information Hiding", LNCS - Lecture Notes in Computer Science, Vols. 1525/1998;32-47, 1998.

[5]. Peter Wayner, Dissappearing Cryptography: Information hiding: Steganography & watermarking, chapter one, p 11-12, 2009.

[6] Aelphaeis Mangarae. Steganography FAQ. March 2006.

[7] Andreas Westfeld and Gritta Wolf. Steganography in a video conferencing system, information hiding, LNCS - Lecture Notes in Computer science. Springer Link,Vols. 1525/1998;32-47.1998.

[8]. Gregory Kipper,Investigator's guide to Steganography, Auerbach Publications, 2004.

[9]. Eric Cole, "Hiding in plain site: Steganography and the Art of Covert Communication". Indianapolis, Indiana, Wiley Publishing Inc, chapter 7, 2003.

[10]. Sarita Dhawale. Secure Connectivity using Image Steganography. International Journal of Pharma and Bio Sciences. 2011.

[11]. Neil Johnson and Sushil Jajodia. "Exploring Steganography: Seeing the Unseen,"Computer Journal IEEE, 1998.

[12].Gary C. Kesslet, "An Overview of Steganography for the Computer Forensics Examiner,"Forensic Science Communications, 2004.

[13]. Z. Kermani, and M. Jamzad. "Arobbust steganography algorithm based on texture similarity using gabor filter.2005.

[14].Kharrazi, M. Cover Selection for Steganographic Embedding. IEEE. 2008.

[15].Hedieh Sajedi and Mansour Jamzad. Cover Selection Steganography Method Based on Similarity of Image Blocks. IEEE 8th International Conference on Computer and Information Technology Workshops.2008.

[16]. Yifeng Sun and Fenlin Liu. "Selecting Cover for Image Steganography by Correlation Coefficient". Second International Workshop on Education Technology and Computer Science. 2010.

[17]. Hedieh Sajedi and Mansour Jamzad. Using contourlet transform and cover selection for secure steganography. Int. J. Inf. Secur. 2010.

[18]. T. Morkel, J.H.P. Eloff, and M.S. Oliver. "An overview of image steganography." in Proc. ISSA, pp. 1-11, 2005.

[19]. Abbas Cheddad and others. "Digital image steganography: survey and analysis of current methods". Signal Processing Journal. 90(3), pp. 727-752, 2010.

[20].Matteo Fortrini. "Steganography and digital watermarking: A global view." University of California, Davis.

[21].P. Kruus, C. Scace, M. Heyman, and M. Mundy. "A survey of steganography techniques for image files." Advanced Security Research Journal. 2003.

[22]. Mehdi Kharazi, Husrev Sencar, and Nasir Memon.. "Image steganography: Concepts and practice". Apr 2004.

[23]. Phil Sallee. Model-based steganography. In Proc. Of the 2nd international work shop on digital watermarking, pages 254–260.12. 2004.

[24].Neil Johnson and Stefan. Katzenbeisser. "A Survey of steganographic techniques." in Information Hiding Techniques for Steganography and Digital Watermarking:chapter three, pp. 43-78, 2000.

[25]. Andreas Westfeld. "F5-A steganographic algorithm: high capacity despite better steganalysis." in Proc. of the 4th Information Hiding Workshop. pp: 289-302, 2001.

[26]. Andreas Westfeld and Andreas Pfitzmann. "Attacks on steganographic systems" . Lecture notes in computer science,pages 61–76, 2000.

[27]. Bin Li and others. "A survey on image steganography and steganalysis". Journal of Information Hiding and Multimedia Signal Processing. 2(2), pp. 142-172, April, 2011.

[28].Neils Provos. "Defending against statistical steganalysis." in Proc. of the 10th USENIX Security Symposium, pp. 323-325, 2001.

[29]. Phil Sallee. Model-based steganography. In Proc. Of the 2nd international work shop on digital watermarking, pages 254–260.12. 2004.

[30].Stefan Katzenbeisser and Fabien. Petitcolas,. "Principles of steganography. " in Information Hiding Techniques for Steganography and Digital Watermarking, , pp. 43-78, 2000.

[31]. Regunathan Radhakrishnan, Kulesh Shanmugasundaram, and Nasir Memon. "Data masking: a secure-covert channel paradigm." in IEEE Workshop on Multimedia Signal Processing, pp 339-342, 2002.

[32]. H.S. Majunatha Reddy and K.B. Raja. “High capacity and security steganography using discrete wavelet transform.” International Journal of Computer Science and Security. 3(6), pp 462-472, 2009.

[33]. Abbas Shaddad, and others. “Biometric inspired digital image steganography.” In Proc. of the 15th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems, Pp. 159-168. 2008.

[34]. Jessica Fridrich, Miroslav Goljan, and Dorin Hogea. Steganalysis of JPEG images: Breaking the F5 algorithm.Lecture Notes in Computer Science, pages 310–323, 2003.

[35]. Rainer Bohme and Andress Westfeld. Breaking Cauchy model-based JPEG steganography with first order statistics.Computer Security–ESORICS, pages 125–140, 2004.

[36]. Siwei Lyu and Hany Farid “Detecting hidden messages using higher-order statistics and support vector machines,” in Proc. 5th Int. Workshop on Information Hiding 2002.

[37]. R.W. Buccigrossi and E.P. Simoncelli. Image compression via joint statistical characterization in the wavelet domain. IEEE Transactions on Image Processing, 8(12):1688{1701, 1999.

[38]. Jessica Fridrich. Feature-Based Steganalysis for JPEG Images and its Implications for Future Design of Steganographic Schemes. 2005.

[39]. Wei Huang, Yao Zhao, and Rong-Rong Ni. Block-Based Adaptive Image Steganography Using LSB Matching Revisited. Journal of electronic science and technology, VOL 9, NO. 4, December 2011.

[40]. Angelos Tzotsos. A Support vector machine approach for object based image analysis. Laboratory of Remote Sensing, Department of Surveying, School of Rural and Surveying Engineering, National Technical University of Athens, Greece.

[41]. Alexandros Karatzoglou, David Meyer, and Kurt Hornik. "Support Vector Machines in R". JSS Journal of Statistical Software. Volume 15, Issue 9, April 2006.

[42]. http://www.classification-society.org/csna/mda-sw/M2/expose-discr-new.pdf.

[43]. http://www.lsv.uni-saarland.de/dsp_ss05_chap11.pdf.

[44]. http://www.cs.washington.edu/research/imagedatabase/groundtruth/