Ministry of Higher Education & Scientific

Research University of Babylon

Science College for Women

Computer Science Department

Information Hiding Based on Image Edges

Research presented to College of Science for Girls
In Fulfillment of the Requirement For the
Degree of B.SC. Of Science in Computer

BY

BANEN MOSA

Supervised by

Dr. Suhad Ahmad Ali

هجري **1444** **2024** م

بسم لله الرحمن الرحيم

إنّا فتحنا لك فتحاً مبينا (1) ليغفر لك الله ما تقدم
من ذنبك وما تأخر ويتمَّ نعمته عليك ويهديك
سراطاً مستقيما (2) وينصرك الله نصرا عزيزا(3)
هو الذي أنزل السكينة في قلوب المؤمنين ليزدادوا
إيمانا مع إيمانهم ولله جنود السموات والأرض
وكان الله عليما حكيما (4) ليدخل المؤمنين
والمؤمنات جنات تجري من تحتها الأنهار خالدين
فيها ويكفر عنهم سيئاتهم وكان ذلك عند الله فوزا
عظيما (5)

صدق الله العلي العظيم

شكر وتقدير

من علمني حرفا ،،، ملكني عبداً

أحمد الله عز وجل وأشكره على كل نعمه التي منَ بها عليَّ فهو المنعم المعطي ،،

كما وأتقدم بأجمل عبارات الشكر والتقدير الى كل من قدم لي العلم

وأخص بالشكر الجزيل أولاً :

أستاذتي التي تحملت مني الكثير الدكتورة الطيبة "سهاد احمد علي "

الاهداء

اليك دون غيرك ...... يابن فاطمة البتول
لا لشيء .... الا لأنك قران تنير العقول
و لأنك ياحسين..... إمام تواصل بعد الرسول
إليك يامن استمطرت من نحره:
آيات السماء
وقيم وإباء
و همم وعطاء
حينها.... نعم حينها كان ختام النزول
إليك يا أمة الشموخ.... من عبد عاشق خجول
يسعى بكل جوارحه يريد اليك الوصول
لا لشيء .... الا لأنك قران تنير العقول،،

......
والى مولاي بقية الله الأعظم
ولي نعمتي سيدي الحجة بن الحسن العسكري "عجل الله فرجه الشريف"

......
والى من لازلت تتعامل معي كبنتها الصغيرة وتعبت معي كثيرا
كي اصل الى مكانة مرموقة في المجتمع...أمي الطيبة
.

Abstract

Steganography is a branch of data-hiding science which aims to reach a desirable level of security in the exchange of private military and commercial data which is not clear. In this project, a study was made of hiding text data in gray scale image which is called the cover image . The system have two main Participants which are the sender and reciever. Sender will apply embedding method, this method consist of many stages. To obtain the sego image, the edges in the cover image have been used to embed messages. At the reciever side, the extracting method will be applied in order to extract the secret message. This method consist of the same stags in the embedding method but it applied inversly.

المحتويات

Chapter One
General Introduction

1.1 Introduction

The word steganography is derived from the Greek words stegos meaning cover and grafia meaning writing defining it as covered writing. In image steganography the information is hidden exclusively in images. Steganography is the art and science of secret communication .It is the practice of encoding / embedding secret information in a manner such that the existence of the information is invisible. The original files can be referred to as cover text, cover image, or cover audio. After inserting the secret message it is referred to as stego-medium. A stego-key is used for hiding/encoding process to restrict detection or extraction of the embedded data. The various applications of steganography include secure military communications, multimedia watermarking and fingerprinting applications for authentication purposed to curb the problem of digital piracy.

The Related Works 1.2

In the last few years, a large number of schemes have been proposed for hiding information in digital picture, video, audio and anther multimedia objects. We describe some contenders that have appeared in the search literature.

The substitution method has to be performed cautiously as overloading the cover image may lead to visible changes leaking the presence of the secret information [1].

With the LSB method as the baseline, a number of related methods have been proposed. For example, a slight variation in converting the secret message into binary codes is undertaken in [2].

In [3], another version of the LSB method is used for RGB images. The cover image is in 3 channels and they are bit sliced. The secret message is embedded in all the three planes in the 2:2:4 ratios for R, G and B planes.

A combination of cryptography and steganography is utilized where the LSB of the cover image is replaced with the most significant bits of the secret image [4].

In 2020, Wang and et.al. a "hybrid steganography" technique based on the replacement of the "least significant bit (LSB)" and "Hamming code (HLAH)" was introduced. Two different methods of steganography are often used to improve information security. Since sharp areas in an image can withstand more changes than smooth areas, more confidential messages are included in the edge areas of the image and a small amount of information is embedded in them [5].

In 2020, Delmi *and et.al.* Presented steganography, The method was used with Less Important Bit Matching (LSBMR) review. The embedding area was at the edge of the digital images to ensure that the message in the image was not detected by the image. The method used for edge area detection using Canny Edge Detection [6].

1.3 problem statement

Image steganography is an engineering term defining a different and significant discipline for information hiding. Security of any steganography technique depends on the selection of pixels for embedding. Pixels in noisy and textured area are better choice for embedding because they are difficult to model.It can be seen that the modified pixels in the smoother parts are clearly noticeable, whereas it is hard to detect these distortions in the high texture parts. In this project, a steganography technique is applied which can hide the secret message only in the edges of the cover image.This project proposes the algorithm for embedding and extracting the secret message embedded behind the cover gray scale image. Also, the analysis of performance measurement methods such as Peak signal to noise ratio (PSNR) and Mean square error (MSE), gives us the experimental summary for four different cases where each case spans different sizes of cover and secret image, comparing the cover image and stego image at the sender"s side and embedded secret and extracted secret at the receiver"s side.

1.4 Project Layouts

This research is organized as follows:

Chapter Two (Theoretical Background)

The overall objective of this chapter is to present fundamentals details, and characteristics of all approaches which have been used steganography method, where the chapter starts with short introduction to image steganography, then it gives an explanation about the methods have been used.

Chapter Three(The Proposed Method):

This chapter presents the designed steps of the entire system's stages and the description of all algorithms that have been used to implement the system.

Chapter Four (Experiential Results and Discussions)

This chapter displays the implementation results, and a discussion on obtained results. The derived conclusions from the proposed system and some suggestions to enhance the proposed system have been presented in this chapter.

Chapter two

Theoretical Background

2.1 Introduction

Steganography is an art of secure transmission of messages from a sender to a receiver. It should ensure that no one can reliably conclude on the secret communication between the sender and the receiver. To achieve such secrecy, the message is hidden in some cover media which may not raise any suspicion on the possibility of carrying the secret message to the third party. Embedding introduces distortion in the cover medium. The embedding distortion in visual and statistical properties of the cover medium may lead steganographic detectability. The objective of any steganographic technique is to preserve these properties while embedding the message in the cover media.

Images are preferred medium for the current steganography techniques. Content adaptability, visual resilience, and smaller size of images make them good carrier to transmit secret messages over the internet.

2.2 Image definition:

An image is a picture that has been created or copied and stored in electronic form. An image can be described in terms of vector graphics or raster graphics. An image stored in raster form is sometimes called a bitmap. An image map is a file containing information that associates different locations on a specified image with hypertext links. An image is a collection of numbers that constitute different light intensities in different areas of the image. This numeric representation forms a grid and the individual points are referred to as pixels (picture element). Grey scale images use 8 bits for each pixel and are able to display 256 different colors or shades of grey. Digital color images are typically stored in 24-bit files and use the RGB color model, also known as true color. All color variations for the pixels of a 24-bit image are derived from three primary colors: red, green and blue, and each primary color are represented by 8 bits. Thus in one given pixel, there can be 256 different quantities of red, green and blue [7].

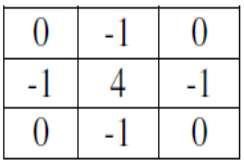
2.3 Edge Detection

Edge is the basic feature of image[8]. Border pixels connecting two separate regions are known as edge. Edges can be defined as image pixels changes. Edges distinguish boundaries and is therefore a major problem in image processing [9].

Edge detection lets users look those features of an image where there's a more or less sudden alteration in gray level or texture refer the top of 1 region at the image and therefore the beginning of another[10]. Edge detection within image processing is a well-developed self-domain. You can extract key features from the image edges, greatly reducing the amount of data to process while maintaining the significant structural properties of the image [9].

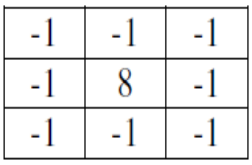
The Laplacian is a 2-D isotropic measure of the 2nd spatial derivative of an image. The Laplacian of an image highlights regions of rapid intensity change and is therefore often used for edge detection (see zero crossing edge detectors). The Laplacian is often applied to an image that has first been smoothed with something approximating a Gaussian smoothing filter in order to reduce its sensitivity to noise, and hence the two variants will be described together here. The operator normally takes a single graylevel image as input and produces another graylevel image as output.

The numerical implementation of the Laplacian function is sometimes done through the mask below [11]:



0	-1	0
-1	4	-1
0	-1	0

G_x



-1	-1	-1
-1	8	-1
-1	-1	-1

G_y

Figure(2.10): Mask Laplacian

The Laplacian Operator is sensitive to fine lines and independent points and measures edges from all directions. it's an passive effect on noise, though, and generates dual pixel edges[12].

2.4 Data Hiding Classifications:

The main categories of data hiding separated into two classes, the Digital Watermarking and Steganography. Note: in our research we shall use the Steganography line [13].

2.4.1 Steganography:

Steganography is the art of hiding transmitting data through apparently innocuous carries in effort to conceal the existence of the data. Though steganography is an ancient craft , the onset of computer technology has given it new life . Computer-based steganography techniques introduce change to digital cover to embed information foreignto the native cover. Such information may be communicated in the form of text, binary file , or provide additional information about the cover and its owner such as digital watermark or fingerprint. Steganography is based on the fact that artifacts like bitmaps and audio files contain redundant information. Hiding a message with steganography reduces the chance of a message being detected . if the message is also encrypted , it must also be decrypted if discovered thus providing another layer of protection. Steganography can be viewed as akin to cryptography. Both have been used throughout record history as means to add elements of secrecy to communication. Cryptography techniques "scramble" a message so that if it is intercepted , it cannot be understood.

This process is known as encryption and the encrypted message is sometimes referred to as ciphertext . Steganographic, in essence, "camouflages" a message to hide its existence and make it seem "invisible" thus concealing the fact that a message is being sent altogether . A cipher text message may draw suspicion while an invisible message will not.

Although steganography has been used since ancient time ,little is generally understood about its usage and

2.4.2 Steganography Definitions

following are most widely used definitions:

- Steganography is the art and science of hiding data in to innocent-looking cover-data so that no one can detect the very existence of the hiding data.
- Steganography is the art and science of communicating in a way which hiding the existence of the communication.
- Steganography encompasses methods of transmitting secret message in such a manner that the existence of the embedded message is undetectable.
- Steganography is the study of methods of concealing data in the noise of another data set.

-*Text steganography* Hiding information in text file is the most common method of steganography. The method was to hide a secret message into a text message. After coming of Internet and different type of digital file formats it has decreased in importance. Text stenography using digital files is not used very often because the text files have a very small amount of excess data.

-*Image steganography* Images are used as the popular cover medium for steganography. A message is embedded in a digital image using an embedding algorithm, using the secret key. The resulting stego image is send to the receiver. On the other side, it is processed by the extraction algorithm using the same key. During the transmission of stego image unauthenticated persons can only notice the transmission of an image but can't see the existence of the hidden message[3]. Figure(2.1) shows the steganography system overview [14]. A general Steganography system is assumed that the sender wishes to send via Steganographic transmission a message to a receiver. The sender begin with a cover message, which is an input to the stego-system, in which the embedded message will be hidden. The hidden message is called the embedded message. A

Steganographic algorithm combines the cover massage with the embedded message, which is something to be hidden in the cover .The algorithm may, or may not, use a Steganographic key (stego key), which is additional secret data that may be needed in the hidden process. The same key (or related one) is usually needed to extract the embedded massage again. The output of the Steganographic algorithm is the stego message. The cover massage and stego message must be of the same data type, but the embedded message may be of another data type. The receiver reverses the embedding process to extract the embedded message [15],[16],[17],[18].

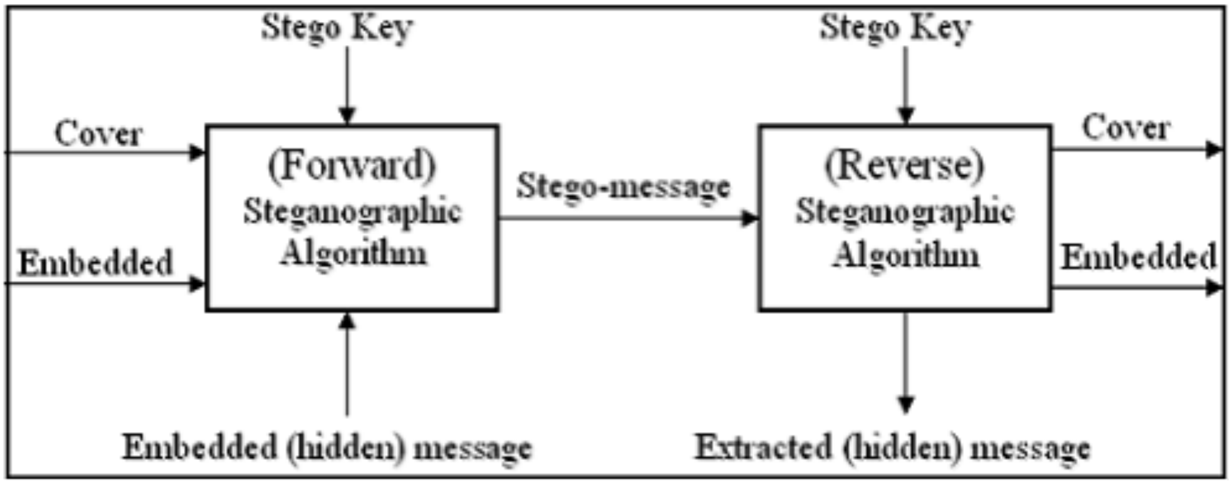


Figure (2.1): Steganography System

2.4.3 Applications of Steganography:

This section list some applications of steganography as follows:

(i)Secret Communications the use steganography does not advertise
secret communication and therefore avoids scrutiny of the sender, message, and recipient. A trade secret, blueprint, or other sensitive information can be transmitted without alerting potential attackers.

(ii) Feature Tagging Elements can be embedded inside an image, such as the names of individuals in a photo or locations in a map. Copying the stego-image also copies all of the embedded features and only parties who possess the decoding stego-key will be able to extract and view the features.

(iii) Copyright Protection Copy protection mechanisms that prevent data, usually digital data, from being copied. The insertion and analysis of watermarks to protect copyrighted material is responsible for the recent rise of interest in digital steganography and data embedding [1].

:Image Steganographic Techniques 2.4.4

There are several Steganographic techniques for image file format which are as follows:

:Spatial Domain Technique 2.4.4.1

There are many versions of spatial steganography, all directly change some bits in the image pixel values in hiding data. Least significant bit (LSB) based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values without perceptible distortions. To our human eye, changes in the value of the LSB are imperceptible. Embedding of message bits can be done either simply or randomly. Least Significant Bit (LSB) replacement technique, Matrix embedding, are some of the spatial domain techniques.

Advantages of spatial domain LSB technique are:

1.Degradation of the original image is not easy.

2.Hiding capacity is more i.e. more information can be stored in an image.

Disadvantages of LSB technique are:

1.robustness is low.

2.Hidden data can be destroyed by simple attacks [1].

2.4.4.2 Masking and Filtering:

Masking and Filtering is a steganography technique which can be used on gray scale images. Masking and filtering is similar to placing watermarks on a printed image. These techniques embed the information in the more significant areas than just hiding it into the noise level. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image.

Advantages of Masking and filtering Techniques:

This method is much more robust than LSB replacement with respect to compression.

Disadvantages: Techniques can be applied only to gray scale images and restricted to 24 bits[3].

2.4.4.3 Statistical Preservation

Statistical detectability is one of the main aspects of a steganography algorithm. To maintain statistical un detectability, the steganography techniques are designed with the aim of minimizing the artifacts introduced in the cover signal by the embedding technique. The main emphasis is on minimizing the noise added by embedding while increasing the payload. This is an important consideration in the design embedding algorithms, since the noise added effects the statistical properties of a medium. For a given medium, the steganography algorithm which makes fewer embedding changes or adds less additive noise will be less detectable as compared to an algorithm which makes relatively more changes or adds higher additive noise.

From the point of view of the steganoanlyst, the steganoanlytic attacks try to examine a signal and look for statistics which get distorted due to embedding. These statistics range from marginal statistics of first and second order in case of targeted attacks to extremely high order statistics (up to 9th order) in the case of blind steganalytic techniques which use machine learning techniques for estimating a model of the cover image from these high order statistics and reports an image to be containing steganographic embedding if it does not conforms to this model. So, in order to defeat the steganalytic attacks, there has been a shift from the above mentioned data hiding paradigm. Algorithms have been proposed which try to restore the statistics which get distorted during the embedding procedure and which may be used for steganalysis [2].

2.5 Performance Analysis: As a performance measure for image distortion due to hidding of message, the well-known peak-signal-to noise ratio (PSNR), which is categorized under difference distortion metrics, can be applied to stego images. It is defined as [20, 21]:

$$\mathrm{SNR}_{\mathrm{PEAK}} = 10\log_{10}\frac{(L-1)^2}{\frac{1}{N^2}\sum_{r=0}^{N-1}\sum_{c=0}^{N-1}[g(r,c)-I(r,c)]^2} \qquad ...(2.3)$$

Where N are the dimensions of the image, L : the number of gray levels (e.g., for 8 bits L =256).

The root-mean-square error is found by taking the square root of the error squared divided by the total number of pixels in the image

$$RMSE = \sqrt{\frac{1}{N^2}\sum_{r=0}^{N-1}\sum_{c=0}^{N-1}[g(r,c)-I(r,c)]^2} \qquad ...(2.4)$$

Chapter Three

The Applied Method

3.1 Introduction

Images are preferred medium for the current steganography techniques.The method that is suggested in this project embeds the message in the cover image to obtain the stego image. In other words, it first applies a preprocessing technique on the secret image, and then puts it into the cover image. To increase the security, the secret image is encrypted using ARNOLD method and then embeds it in the cover image based on hash function to add second layer of security. After that, the results are evaluated using different measures. The below block diagram in figure (3-1) depicts the stages and procedu;res.

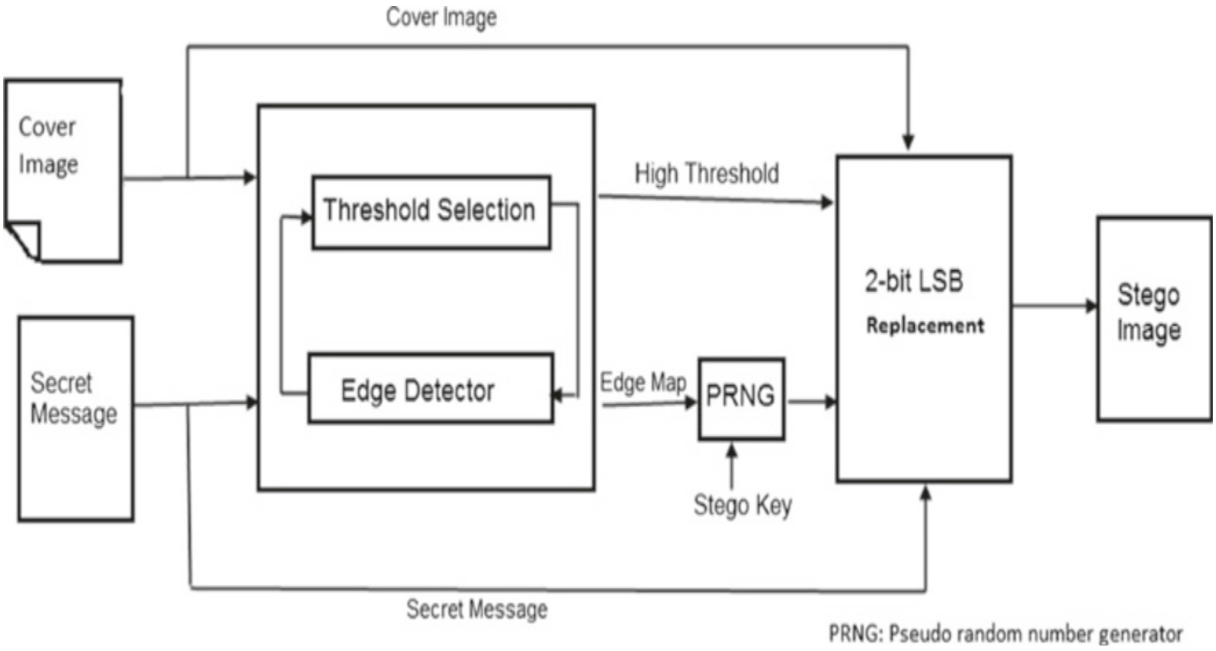
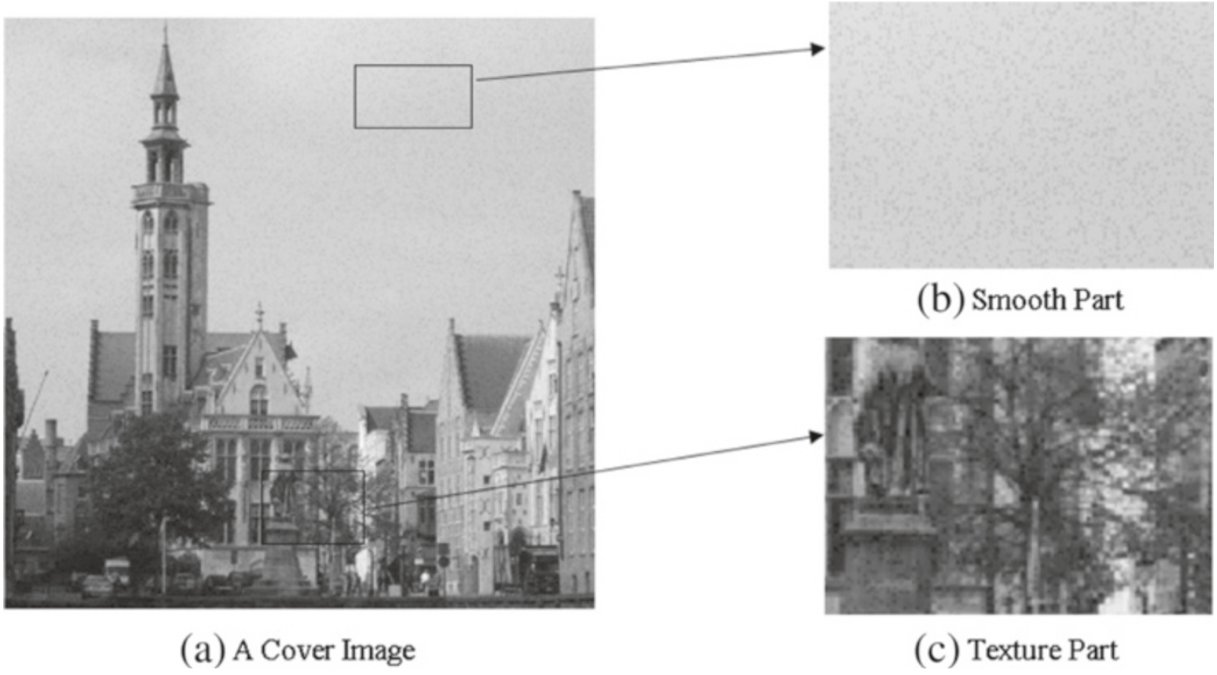


Figure (3.1): the stages of applied system

Security of any steganography technique depends on the selection of pixels for embedding. Pixels in noisy and textured area are better choice for embedding because they are difficult to model. Pixels in edges can be seen as noisy pixels because their intensities are either higher or lower than their neighboring pixels due to sudden change in the coefficient gradient. Due to these sharp changes in the visual and statistical properties, edges are difficult to model in comparison to pixels in smoother area. Therefore, edges make a better option to hide secret data than any other region of an image where a small distortion is much more noticeable. Figure 3.2a is an image with 20% of pixels modified to produce distortion. The image has some smooth parts such as sky and some parts with high concentration of edges, such as trees and buildings. Some areas from both smoother part and high texture part are cropped and zoomed as shown in Figure 3.2 b,c. It can be seen that the modified pixels in the smoother parts are clearly noticeable, whereas it is hard to detect these distortions in the high texture parts.



(a) A Cover Image

(b) Smooth Part

(c) Texture Part

Figure 3.2 Effect of embedding in an image. (a) Cover image. (b) Smooth part. (c) Textured part.

The following parts of this section explain the embedding and extraction stages of the image.

1. Procedure Embedding

An embedding process is done in the sender side. It includes many steps, which depict as follow:

1.1. Masking cover image

An image is a group of pixels that represent color values, or what is known as the image's density. Each pixel in the image consists of 8 bits, so at this stage clear the five least important bits of each pixel will be by substituting the value zero instead of the value of that bit. The following example depicts the clearing process to get the most significant bits image.

Pixels	Clearing five LSB	New pixels
155=10011011	10000000	128
126=01111110	01100000	96
88=01011000	01000000	64
156=10011100	10000000	128

1.2. Edge detection

This step is based on the previous stage, where the edge of the top four bits of importance is revealed by using Sobel filter for detecting edges. The following example shows how to detect the pixels in the most significant bits image in the previous step as edge pixel by assign the value (1) and non- edge pixel by assigning the value (0).

New pixels	128	96	64	128
Edge Pixels	1	0	0	1

The value of threshold is selected manaually.

Algorithm (3.1) shows the edge detection process using Sobel filter for detecting edges.

```
Algorithm (3.1): Edge detection
Steps for the method to detect edges
Input: Image Sample, Threshold T
Output: "Slope magnitude Image"
Step 1:  Image entry to read
Step 2: stratify Mx "horizontal mask" and My "vertical mask" to an image input
Step 3: Apply various "edge detection algorithms" and get a gradient
Step 4: Create separate image for both Mx and My $M_y$
Step 5: Results are combined to find the absolute gradient magnitude as per equation ( 2.1).
    $G\left[f(x,y)\right] = \sqrt{M_x^2 + M_y^2}$
Step 6: The absolute magnitude is the image of the magnitude of the resulting slope
Step7: if  G[f(x,y)]>T, then possible edge point
```

3.1.1.2 Embedding process

Most of the steganographic techniques embed data in LSB of pixels in the cover image pixel. Embedding is done by either LSB replacement or LSB matching. Depending on the previous stage, the cover image original pixels are classified into two categories, "non-edge pixels", and "edge pixels", respectively. Where "x and y" are used, where "x" means the number of secret bits to be included in 'non-edge pixels' and corresponding "y" means the "number of secret bits" to be included in "edge Pixels" are included for these two categories by replacing "k-LSB," where "k" is equal to either "x or y" which is determined by "edge information". Finally, I get a "stego-image.

3.2.2 Extraction Procedure

The embedded image will go through the clear pixel stage and edge detection stage. at the "extraction phase", the recipient first extracts twain "parameters x and y from the pixels of the image". Also, "edge information" is set identical within the embedding phase. Therefore, the key data are extracted exactly.

Chapter Four

Experiential Results and Discussions

4.1. Introduction

This work proposes a Steganography technique for the gray image. The edge of cover image is detected. Then, secret message is hidden by Least Significant Bits technique of the original cover image using edge and non-edge pixels. The developed system was established using Matlab (version 14) programming language. The programs work under windows XP service pack2 operating system, laptop computer with processor: Intel core2 CPU.

4-2 Test Material

All test images that implemented in our experiments are 256 gray levels. Figure (4-1) shows examples of these images.

(a)Original image (Lenna.bmp)

(b) Original image (House.bmp)

(c) Original image (Barbara.bmp)

(c) Original image (Girl.bmp)

Figure (4-1) Examples of tests cover images

4.3 Experiential Results

In this case, the LSB technique hides a secret message (*computer science)* in the grayscale image (lena.bmp) with size (256*256) as shown in Figure (4.2). The number of bits hidden in non-edge pixels is (1) and an edge pixel is (2).

Cover Image	The text to be hidden
	Computer science

Figure (4.2): the input image and input text

4.3.1 Embedding Process

In the first step, the ASCII code of each input character in the input text to be hidden is obtained. Table (4.1) shows the ASCII code for the input text ("computer science").

Table (4.1): ASCII code for input text

Text with characters	Text with value
computer science	99 111 109 112 117 116 101 114 32 115 99 105 101 110 99 101

Then convert each value to bits. Convert each letter to 7 bits as shown in Table (4.2).

Table (4.2): Binary code for input text

Text with characters	Text with value
99	1 0 1 0 1 1 1
111	1 1 1 1 0 1 1
109	1 0 0 0 1 1 1

The first five bits of each pixel in the image cleared, then the edge detected in one of the ways we touched on it as shown in Figure (4.3).

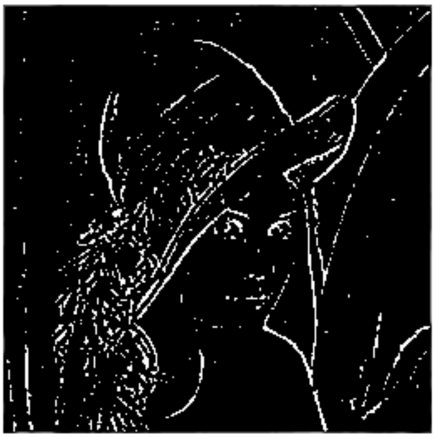
Image cover	Detection by LOG Threshold =20
	

Figure (4.3): The detected edge of the input image

Original image	Stego image	PSNR
		79.7975

Finally, the original and stego images are obtained as shown in **Error! Reference source not found.**(4.4).

Figure (4.4): steganography of thepropsed method (a) "original image" (b)" stego image"

4.3.2 Extraction Process

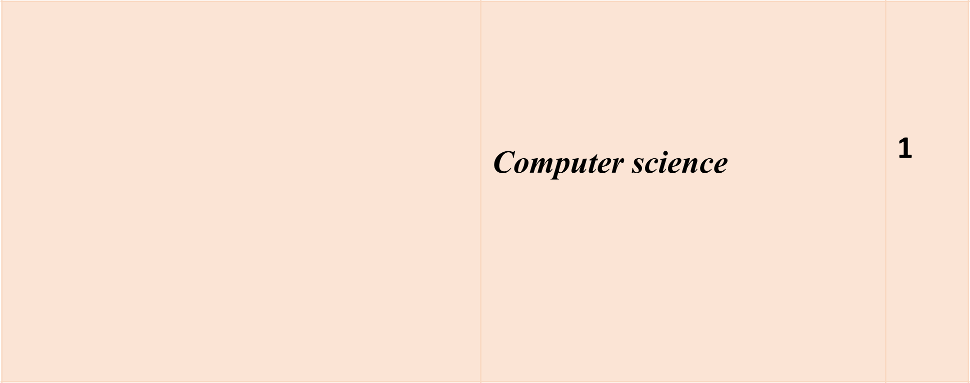
An image taken after hiding and passed through the previous slices explained in hiding were the first five bits detected. Edge detection is applied for remaining bits. Where is compared if the pixel in the image after masking is offset by a value of 255, we extract two bits from the image and if it corresponds to 0 it extracts one bit from the image as depicted in Table (4.3).

Table (4.3): Extraction of the secret message

Text in binary	Text in numeric	Text in character
1 0 1 0 1 1 1	99	c
1 0 1 1 1 1	111	o
1	109	m

The NC scale value is calculated which Measure the similarities between the original and extracted text as shown in Figure (4.5).

Stego image	Text	NC



stego image (b) extract secret message (a)

Figure (4.5): steganography of the applied method (a) stego image (b) extract secret message

4.3 Conclusions

In the applied method the secret message is hidden in the cover image. So there is a small visual change in between cover image and stego image. Due to strong security aspects this small amount of imperceptibility is acceptable. we notice that the peak noise signal (PSNR) is the best estimate of the optimization efficiency, the higher the PSNR quality, the "stego image" is extremely near the "original image". Also, An image with many objects is much better than an image with few objects because of the possibility of hiding it perceptible through HVS. Embedding capacity becomes larger as the texture of the image becomes more sophisticated because complex images can generate more pixel edges than simple .images

4.3 Future Works

In the following some suggested ideas are given below:

- This approach can be applied for image steganography in transform domain such Discreet Wavelet Transform (DWT) and Discreet Cosine Transform (DCT).
- The selection of threshold can be done automatically.

References

1. S. Gupta, G. Gujral and N. Aggarwal, "Enhanced least significant bit algorithm for image steganography", Int. J. Comput. Eng. Manage., vol. 15, no. 4, pp. 40-42, 2012.
2. R. Das and T. Tuithung, "A novel steganography method for image based on Huffman encoding", *Proc. 3rd Nat. Conf. Emerg. Trends Appl. Comput. Sci.*, pp. 14-18, Mar. 2012.
3. A. Singh and H. Singh, "An improved LSB based image steganography technique for RGB images", *Proc. IEEE Int. Conf. Electr. Comput. Commun. Technol. (ICECCT)*, pp. 1-4, Mar. 2015.
4. N. Patel and S. Meena, "LSB based image steganography using dynamic key cryptography", *Proc. Int. Conf. Emerg. Trends Commun. Technol. (ETCT)*, pp. 1-5, Nov. 2016.
5. Wang, Y., Tang, M., & Wang, Z.," High-capacity adaptive steganography based on LSB and Hamming code". Optik, vol. 213,2020, https://doi.org/10.1016/j.ijleo.2020.164685.
6. Delmi, A., Suryadi, S., & Satria, Y., "Digital image steganography by using edge adaptive based chaos cryptography". In Journal of

Physics: Conference Series,Vol. 1442, No. 1, pp. 1-7, IOP Publishing, January 2020, DOI: 10.1088/1742-6596/1442/1/012041

7. R.Anderson and F. Petitcolas, "On the limits of steganography", IEEE Journal of Selected Areas in Communications, Vol. 16, No. 4, May 1998.

8. Sujeet Das "Comparison of Various Edge Detection Technique".International Journal of Signal Processing, Image Processing, and Pattern Recognition Vol.9, No.2, 2016.

9. Deepak Mathur, Dr. Prabhat Mathur "Edge Detection Techniques In Image Processing With Elaborative Approach Towards Canny" Computer Science Department, Lachoo Memorial College Of Science & Technology,2016.

10. Mrs.Anandhi, Dr.M.S.Josephine, Dr.V.Jeyabalaraja, S.Satthiyaraj,St.Peter's "Comparison Of Canny And Sobel Edge In Detection Techniques", University, India Dr.MGR University, India Dr.Velammal Engineering College University College Of Engineering, Panruti,2015.

11. Ahmed Shihab, "Comparative Study Among Sobel, Prewitt And Canny Edge Detection Operators Used In Image Processing", University of Baghdad College of Nursing, October 2018.

12. Muthukrishnan R. "Edge Detection Techniques For Image Segmentation", International Journal of Computer Science & Information Technology (IJCSIT) Vol 3, No 6, Dec 2011.

13. K. Jenita Devi,"A Sesure Image Steganography Using LSB Technique and Pseudo Random Encoding Technique" , B.SC thesis, Department of Computer Science and Engineering National Institute of Technology, May 2013.

14. S. Majumder, K. J. Devi, and S. K. Sarkar, “Singular value decomposition and wavelet-based iris biometric watermarking”, IET Biometrics, vol. 2, no. 1, 2013.

15. Fabien A. P. Petitcolas, Ross J. Anderson, "Information Hiding" " Proceedings of the IEEE, special issue on protection of multimedia content" , 87(7), July 1999.

16. Md. Rafiqul Islam, A.W. Naji, A.A.Zaidan, B.B.Zaidan " New System for Secure Cover File of Hidden Data in the Image Page within Executable File Using Statistical Steganography Techniques", International Journal of Computer Science and Information Security (IJCSIS), ISSN: 1947-5500, P.P 273-279, Vol.7 , NO.1, January 2010,USA..

17. Hamdan. Alanazi, Hamid.A.Jalab, A.A.Zaidan, B.B.Zaidan, "New Frame Work of Hidden Data with in Non Multimedia File", International Journal of Computer and Network Security, 2010, Vol.2, No.1, ISSN: 1985-1553, P.P 46-54,30 January, Vienna, Austria.

18. M. K. I. Rahmani and N. P. KamiyaArora, "A crypto-steganography: A survey," International Journal of Advanced Computer Science and Application, vol. 5, pp. 149–154, 2014.

19. M. Li, T. Liang and Y. He, "Arnold Transform Based Image Scrambling Method",3rd International Conference on Multimedia Technology (ICMT-13), Atlantis Press, 2013.

20. S. Roy and A.K. Pal, "A robust blind hybrid image watermarking scheme in RDWT-DCT domain using Arnold scrambling", Multimedia Tools and Applications, 76(3), 3577-3616, 2017.

21. X. Yu, C. Wang, and X. Zhou, "A survey on robust video watermarking algorithms for copyright protection," Appl. Sci., vol. 8, no. 10, Oct,2018.

الخلاصة:

إخفاء المعلومات هو فرع من علم إخفاء البيانات يهدف إلى الوصول إلى مستوى مرغوب فيه من الأمان في تبادل البيانات العسكرية والتجارية الخاصة غير الواضحة. تم في هذا المشروع دراسة إخفاء البيانات النصية في صورة ذات تدرج رمادي والتي تسمى صورة الغلاف. يحتوي النظام على مشاركين رئيسيين هما المرسل والمستقبل. يقوم المرسل بتطبيق طريقة التضمين، وتتكون هذه الطريقة من عدة مراحل. للحصول على صورة stego، تم استخدام الحواف الموجودة في صورة الغلاف لتضمين الرسائل. ومن جهة المستلم سيتم تطبيق طريقة الاستخراج لاستخراج الرسالة السرية. تتكون هذه الطريقة من نفس الخطوات في طريقة التضمين ولكنها تطبق بشكل عكسي.

وزارة التعليم العالي والبحث العلمي
جامعة بابل / كلية العلوم للبنات
قسم علوم الحاسوب

أخفاء البيانات بالاعتماد على حواف الصورة

بحث مقدم لكلية العلوم للبنات
كجزء من متطلبات
درجة البكالوريوس العلوم في الحاسوب

مقدمة من قبل
بنين موسى

بأشراف
أ.د. سهاد احمد علي

1444 هـ 2024 م