جمهورية العراق

وزارة التعليم العالي والبحث العلمي

كلية علوم الحاسوب وتكنولوجيا المعلومات\جامعة القادسية

University of Al-Qadisiyah

College Of Information Technology

مشروع تخرج بعنوان

Insert And Hide Watermark

إدراج وإخفاء العلامة المائية

إعداد الطلبة

اثير سجاد هادي

سجاد اديب صبر

عبدالله صالح عبد السادة

علي كاظم هلال

إشراف

م.م زينة حسين تومان

قدم هذا المشروع استكمالا لنيل درجة البكالوريوس

في قسم علوم الحاسوب

للعام الدراسي (2018-2019)

April 2019

بسم الله الرحمن الرحيم

((اقرأ بأسم ربك الذي خلق (١) خلق الانسان من علق(٢) اقرأ وربك الأكرم(٣) الذي علم بالقلم (٤)علم الانسان مالم يعلم(٥))) سورة العلق

صدق الله العلي العظيم

إهـــــــداء

بكل الحب .....

الى الشمعتين اللتين انرتا درب نجاحي

امي وابي

الى كل انسان علمني قيمة الموقف والمبادئ في الحياة

الى المدرسة التي علمتني

الى كل اللذين وقفوا معي يتأملون نجاحي

كلمة شكر

لابد لنا ونحن نخطوا خطواتنا الأخيرة في الحياة الجامعية من وقفة نعود إلى أعوام قضيناها في رحاب الجامعة مع أساتذتنا الكرام الذين قدموا لنا الكثير باذلين بذلك جهودا كبيرة في بناء جيل الغد لتبعث الأمة من جديد ...

وقبل أن نمضي تقدم أسمى آيات الشكر والامتنان والتقدير والمحبة إلى الذين حملوا أقدس رسالة في الحياة ...

إلى الذين مهدوا لنا طريق العلم والمعرفة ...

إلى جميع أساتذتنا الأفاضل.....

"كن عالما .. فإن لم تستطع فكن متعلما ، فإن لم تستطع فأحب العلماء ،فإن لم تستطع فلا تبغضهم"

وأخص بالتقدير والشكر:

الدكتور هشام محمد البيرماني

الدكتور منتصر جابر جواد

الدكتور محمد عباس

الدكتور علي محسن

وكذلك نشكر كل من ساعد على إتمام هذا المشروع وقدم لنا العون ومد لنا يد المساعدة وزودنا بالمعلومات اللازمة لإتمام هذا المشروع ونخص بالذكر

م م . زينة حسين تومان

الذين كانوا عونا لنا في بحثنا هذا ونورا يضيء الظلمة التي كانت تقف أحيانا في طريقنا.

إلى من زرعوا التفاؤل في دربنا وقدموا لنا المساعدات والتسهيلات والأفكار والمعلومات، ربما دون يشعروا بدورهم بذلك فلهم منا كل الشكر

الشكر الجزيل لجميع اساتذة وتدريسي كلية علوم الحاسوب وتكنولوجيا المعلومات .

والله ولي التوفيق

Abstract

Digital image watermarking techniques have been developed widely in recent years to maintain the broadcasting media and content authentication, broadcast monitoring, copy control, and many other applications

Therefore, many studies have used digital image watermarking to solve these problem. This paper highlights digital image watermarking. It starts with a basic model of digital image watermarking, it discusses the main requirements and applications. Moreover, it reviews some of the techniques and algorithm used in image watermarking. In addition, digital image watermarking attacks are discussed. Lastly Watermarking evaluation system is described .

CHAPTER ONE

Introduction To Watermark

1.1 INTRODUCTION

Since the Internet has become very popular, and people can share whatever they want to share such as images, videos, documents, etc., there has been a need to protect publishing copyright. In addition, there has been also a significant demand for information security. For these

reasons and other reasons, digital image watermarking has become very popular recent years as a good solution for these cases. Many researches have gone through this field to create new techniques, and to enhance current techniques as proper solutions for previous problems. Digital image watermarking techniques stand on embedding a host image with information which is called watermark, then the watermarked image will be transmitted, and can be extracted at the receiver. There are two kinds of detection types at the receiver. The first type is called blind watermarking, because the detector doesn't need the original cover image to detect the watermark. The second type is called non-blind and it needs the original cover image to extract the watermark [1].

1.2. Basic Model Of Digital Image Watermarking

The basic model of digital image watermarking consists of two parts; the first part is the watermark embedding process which shown in Figure (1), and the second part is the watermark detection process which shown in Figure(2)

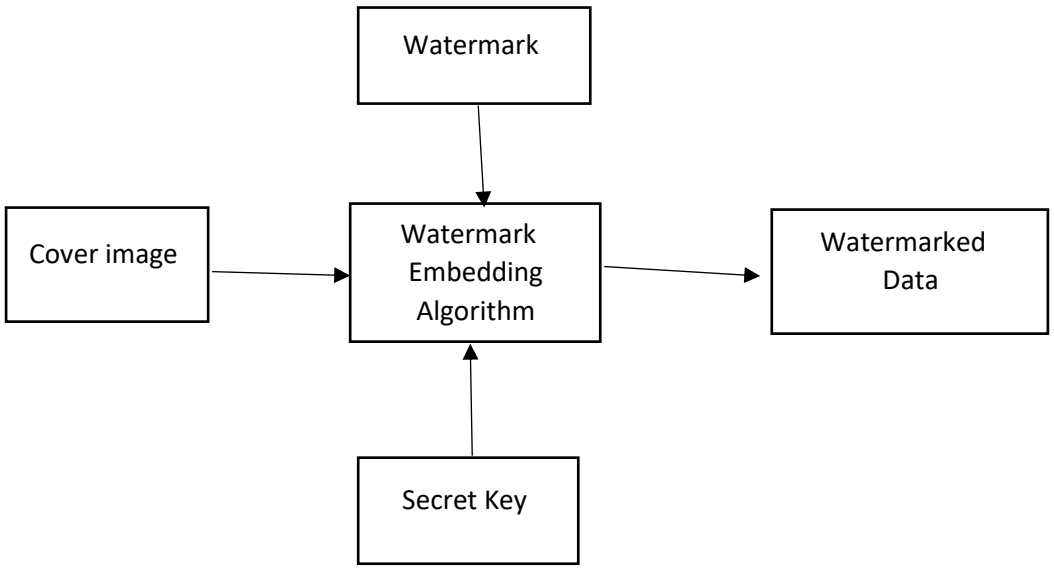


Fig 1. Watermark Embedding Process

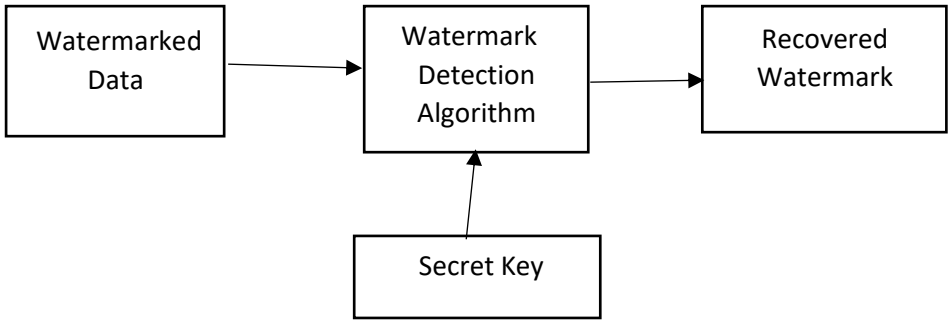


Fig 2. Watermark Detection Process

In Figure 1, which represents sender, the Watermark is embedded into the Cover Image with the Secret Key that ensures the security of watermarking process. The output is the Watermarked Image. In Figure 2, at the receiver side, the detector detects the watermark from the Watermarked Image by using the Secret Key to recover the Watermark [2].

1.3 Requirements Of Digital Image Watermarking

Digital image watermarking concerns to solve some issues properly, thus, this paper highlights the main requirements of watermarked image as following:

A. Robustness:

The robustness is the ability of detecting the watermark after some signal processing modification such as spatial filtering, scanning and printing, lossy compression, translation, scaling, and rotation , and other

operations like digital to analog (D/A), analog to digital (A/D) conversions, cutting, image enhancement [2].

B. Imperceptibility:

Imperceptibility (also known as Invisibility and Fidelity) is the most significant requirement in watermarking system, and it refers to the perceptual similarity between the original image before watermarking process and the watermarked image [2].

C. Capacity:

Capacity (also known as Payload) refers to the number of bits embedded into the image. The capacity of an image could be different according to the application that watermark is designed for [1].

D. Security:

Security is the ability to resist against intentional attacks. These attacks intended to change the purpose of embedding the watermark. Attacks types can be divided into three main categories: unauthorized removal, unauthorized embedding, and unauthorized detection [1] .

E. Low Complexity:

The cost is the reason behind studying the complexity, so it should be at a reasonable cost [1]. It describes the economics of using watermark embedders and detectors, because it can be very complicated and depends on business model that is used.

1.4 Applications Of Digital Image Watermarking

A. Copyright Protection:

The copyright information can be embedded as a watermark into the new production. Once there is a dispute on the ownership, the watermark can be extracted to provide the evidence of who is the owner of this product .

B. Content Authentication:

The watermark is embedded to detect if the image has been modified or not, this process can be used for authentication [2].

C. Broadcast Monitoring:

This type of monitoring is used especially in the advertisements to make sure that the content broadcasted as the contract between the advertisement company and the customer [2].

D. Owner Identification:

To achieve owner identification, there was a traditional form for intellectual ownership verification which was a visual mark. However, nowadays, this is easily overcome by the use of some software that modify images . .

E. Fingerprinting:

The main purpose of fingerprinting is to protect customers. If someone got a legal copy of a product, but redistributed illegally, fingerprinting can

prevent this . This can be achieved by tracing the whole transaction by embedding unique robust watermark for each recipient. Thus, the owner can identify who redistributed this product by extracting the watermark from the illegal copy [2].

F. Copy Control:

The watermark contains owner data and specifies the corresponding amount of copies allowed. This presupposes hardware and software for updating the watermark whenever it has been used .

G. Medical Applications:

Image watermarking can be used in medical images for several purposes. It's used to protect the patient's information from unauthorized people. In addition, it can be used for authentication if the patient lost the image. Moreover, it is needed to protect the copyright of the medical image [2]. For example, mammograms contain diagnostic information which can be used for early detection of breast cancer diseases and breast abnormality. easily distributed over the internet. For mammogram medical image, it should be sure that embedding watermark does not affect the diagnostic information of the mammogram [2].

1.5 Watermark Attacks[2]

Digital image watermarking attacks can be classified to intentional attacks and non-intentional attacks. An attack succeeds in overcome a watermarking scheme if it weakens the watermark less than acceptable limits. On the other hand, recall the differentiation between achieving robustness and imperceptibility at the same time, it should be a balance to

achieve them together. However, this paper highlights the attacks that affect the robustness directly, it highlights some common attacks such as JPEG compression attack, Noise, and Geometric attacks. First, JPEG is a standard compression technique, and it reduces the size of images for the goals of storage and transmission. As the compression rate increases, the quality of the image decreases. Second, Noise attacks are the data that are not part of the original image which caused by other sources. There are many types of noise such as Gaussian noise, and blurring noise . Lastly, Geometric attack is a set of parameters that can be applied on the image. There are many types of geometric attacks such as rotation, cropping, and other transformations .

1.6 Digital Image Watermarking Techniques

1.6.1 Spatial Domain This type of embedding relies on that information is inserted directly into the image [2]. There are many algorithms and techniques that use spatial domain such as and Least Significant Bit (LSB), Intermediate Significant Bit (ISB) , Patchwork, etc.

A. Least Significant Bit (LSB)[1]

LSB algorithm is considered as the simplest approach because the least significant bits carry less relevant information and their effect does not cause visible changes And this technique is used for simple operation to embed information into a host image. The idea behind LSB is very simple; the host image pixels are changed by no of bits of the secret

message. Despite of the number was embedded into the first 8 bytes of the grid, the 1 to 4 least bits needed to be modified according to the embedded secret message. On the average, only half of the bits in an image will need to be changed to hide a secret message using a host image. Because the quality of the Watermarked image is low, less than over the 4 least significant bits, changing the LSB of a pixel results in small changes in the intensity of the colors.

B. Intermediate Significant Bit (ISB)[2]

Although embedding watermark, within LSB gives the best image quality, embedding within the Most Significant Bit MSB gives the worst image quality. When starting from the MSB towards the LSB, embedding will improve the quality of watermarked image . Recently improved LSB to a new technique called intermediate significant bit (ISB). In the new method, the watermark pixel's location has been tested according to the range of each bit-plane. Thus, if the location of watermarked pixel is in the middle of the range, any effect on the pixel by attacks will make it difficult to move the selected bit to other range. Meanwhile, if the pixel value is located at the edges of the ranges, any small change caused by attacks will move the pixel from a range to other range, and the watermark cannot be extracted. [1].

C. Patchwork[4]

Patchwork algorithm inserts the information into the brightness of pixels by changing the statistical properties of the image. Patchwork selects randomly number of pairs of pixel points (ai,bi), and the difference

between two randomly selected pixels equals zero centered at Gaussian distribution. Then the brightness value of the pixel point ai increases by 1, the brightness value of pixel point bi reduces by 1 In this case, the distribution center will be changed, but the average brightness of the image will not be changed. For the goal of resisting the attack of loss compression and filtering process, it extends the pixels to pairs of blocks; thus, the brightness of pixels in one block will be increased, while the brightness of pixels in corresponding block will be reduced

1.6.2 Transform Domain[4]

This type of embedding uses the transform coefficients to embed the watermark. Moreover, transform domain techniques are very robust against attacks, because the watermark is spread in whole image [1]. The main techniques used in transform domain are: Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT), and many other techniques.

A. Discrete Cosine Transform (DCT)[4]

DCT is widely used in digital image watermarking since it has strong robustness. In addition, many frequency coefficients are obtained from DCT, such as single direct current DC coefficient, low frequency coefficients, mid frequency coefficients, and high frequency coefficients By the different characters of these coefficients, we can obtain different effects upon digital watermarking system Moreover, JPEG standard and Watson visual model are based on DCT with block size 8×8, which is commonly used in image watermarking .

B. secrete Wavelet Transform (DWT)[4]

Wavelet Transform has been used widely since it has been adopted in the established image coding standard and it produce considerably better quality for decoded image than JPEG. The main advantage that DWT has over Fourie r transforms is temporal resolution. It captures both location and frequency information .The basic idea of DWT is to separate frequency detail, which is multi-resolution decomposition. One time of decomposition can divide the image to four sub image.

*The Aim Of The Watermark Project

Study the characteristics of watermarks and identify their characteristics and the many benefits that can not be limited, as well as methods of use and addition of data and identify the algorithms used in the inclusion of the watermark as well as ways of adding images and different data and cash coins to obtain confidentiality and safety and ownership and others.

CHAPTER TWO

LSB Algorithm For Watermarks

The Least Significant Bit (LSB)[10] insertion method is a common, simple approach to embedding information in a graphical image file. In LSB insertion method the LSB of every pixel is replaced by every message bit. There is 50 % chance that the message may match with the LSB‟s of the Cover image. Thus only 50 % LSB‟s are likely to change. Also, the change occurs only in the bit which is least significant, thus keeping the other more significant bits unaltered.

Therefore, this does not affect the original image perceptibility. Hence it is a very popular technique. However, it is extremely vulnerable to attacks. Any image manipulations such as cropping, intensity changes for any enhancements such as contrast stretching, histogram equalization, addition of noise etc.. will destroy the embedded message.

The techniques other than LSB technique are complicated, although they are robust to most attacks. LSB technique can therefore be used wherever we want to store confidential information on a standalone PC or one which is shared among several users. LSB technique can be used to store personal data such as ATM PIN, Credit card details, salary statement, income tax data, passport information etc in an imperceptible way. So, wherever this kind of information is to be preserved in a manner that only legitimate user should be able to retrieve it whenever needed, by simple ways, LSB is a better solution.

Least Significant Bit (LSB) encoding is the easiest of the techniques used for embedding secret or confidential information in digital images. For a gray scale bitmap (BMP), using the LSB of each byte (8 bits) in an image, a secret message of size $1/8^{th}$ of the Cover image can be stored. This can be easily done by directly substituting every bit of the secret message into every LSB.

For a 24 bit color image as the cover image, since there are 3 bytes for every pixel, 3 bits of data can be stored in each pixel, so the capacity to store increases by 3 times thus making it 3/8 of the cover image size. If the message to be embedded is a text message a secret message of size $1/7^{th}$ of the grayscale cover image can be stored and in a 24 bit color image as cover a text message of size 3/7 can be embedded.

The confidential information which is embedded in the Cover image can be an image (grayscale, binary or color image), text or even audio. As the type and size of confidential information varies, the embedding capacity varies for a particular type of Cover used. LSB technique can be used either by directly replacing the Cover LSB‟s by the Secret information bits, or to add one more level of security, it can be encrypted and then inserted into the LSB‟s of the Cover.

2.1 Using 2 / 3 / n LSB's Technique

The technique [5] implemented in this section not only replaces the LSB, but the LSB is modified by taking into consideration the other bits of the

Cover and the message bit as well. Advantage of this method is it adds one more level of security, by encrypting the message bits before embedding with just a slight increase in the encoding / decoding complexity and Cover capacity remains the same as LSB substitution, accuracy of retrieval is 100%, and good perceptual transparency of cover image is achieved.

2.1.1 Embedding Algorithm [5]

Extract RGB components of pixel intensity values of message and the cover image if 24 bit color images are to be used else for a grayscale image every byte is the intensity of every pixel. In case text message is to be embedded, then their ASCII codes have to be considered. The procedure given below is by considering 24 bit color images. Take the successive R, G, and B component values of pixels and convert them into array of values for messages and the cover image. Convert every decimal value into 8 bit binary equivalent for cover and message images. Every message bit is embedded into LSB‟s of the cover image after processing. Processing is done as follows:

a) **LSB 2 Method:** [5]

If the message bit to be embedded is 0, then adjust the LSB such that the XOR operation on LSB and next to LSB is 0 and if the message bit to be embedded is 1, then adjust the LSB such that the XOR operation on LSB and next to LSB is 1 as shown in the Table 2.1 below.

Table 2.1 Truth Table for LSB 2 Bit Method

Next to LSB	LSB	Message Bit	LSB Adjusted
0	0	0	**No Change**
0	1	0	0
1	0	0	1
1	1	0	**No change**
0	0	1	1
0	1	1	**No change**
1	0	1	**No change**
1	1	1	0

Remark: There are 50 % chances that there will not be any change in the Stego.

b) **LSB 3 Method:** If the message bit to be embedded is 1, then the LSB is adjusted such that the XOR operation on LSB, next to LSB and next to next to LSB is 0. And if the message bit to be embedded is 1, then adjust the LSB such that the XOR operation on LSB next to LSB and next to next to LSB is 1 as shown in the Table 2.2 below.**[6]**

Table 2.2 Truth Table for LSB 3 Bit Method

to Next Next LSB	Next to LSB	LSB	Message Bit	LSB Adjusted
0	0	0	0	**No change**
0	0	1	0	0
0	1	0	0	1
0	1	1	0	**No change**
1	0	0	0	1
1	0	1	0	**No change**
1	1	0	0	**No change**
1	1	1	0	0
0	0	0	1	1
0	0	1	1	**No change**
0	1	0	1	**No change**
0	1	1	1	0
1	0	0	1	**No change**
1	0	1	1	0
1	1	0	1	1
1	1	1	1	**No change**

The message embedding in the cover image is over.

2.1.2 Retrieving Algorithm [7]

The message retrieving is done as per the algorithm given below

a) Extract Red, Green and Blue Components of pixel intensity values of Stego image.

b) Take successive Red, Green and Blue component values of pixels and convert them into array of values for message and Stego image.

c) Convert every decimal value into 8 bit binary equivalent for Stego image.

d) Retrieval of the message bit is done by using the XOR operation on the LSB and Next to LSB.

i. If it is 1 then message bit is 1. ii. If it is 0 then message bit is 0.

e) If during embedding the LSB 3 method is used then retrieval is done by performing XOR operation on LSB, next to LSB and Next to Next to LSB‟s.

i. If the result of XOR operation is 0, it means the decoded message bit value is 0 and

ii. If the result is 1, it means that the decoded message bit value is 1.

f) Convert every 8 bits to form a byte whose decimal value is the pixel intensity if the message embedded is a grayscale image otherwise this

decimal value forms the intensity of Red component of the first pixel of the Secret image, if the message embedded is a 24 bit color image. If the message that is embedded is a text message then after every 7 bits are retrieved convert them into decimal which forms the ASCII code of the 1st character. In this manner these steps are continued till the full message is retrieved.

g) In case of 24 bit, every byte forms either the Red, Green or Blue component of the message pixels in sequence. Take 3 bytes and group them as 3 RGB components of a 1 pixel.

Perform this step for the full message.

The message retrieval is over.

Instead of only 2 or 3 LSB‟s this method can be extended till all the 8 bits of the cover image are considered to encrypt the message bit, and then in that case the decryption will be done considering 2, 3 till 8 bits of the Cover image respectively.

2.2 Considering Parity

In addition to the above encryption method, one more simple method for encryption is suggested, which uses parity as a key for embedding. The embedding and retrieval is to be done as given below.

2.2.1 Embedding Algorithm [8]

Adjust the LSB of the byte of the Cover so that it is even parity after embedding if the message bit to be embedded is 0 and adjust the LSB of

the byte of the Cover so that it becomes odd parity after embedding of if the message bit to be embedded is 1. This is done till the embedding of all message bits is over.

2.2.2 Retrieval Algorithm: [8]

For retrieving the message the Stego image is taken. The parity of every byte is checked. If the parity is even that means the message bit is 0 and if the parity is odd it means the message bit is 1. The role of odd and even parity is interchangeable.

In this way after 8 such message bits are retrieved they are converted to decimal and this decimal number becomes the intensity value of the first message pixel for grayscale image or Red component of the first pixel if the message is 24 bit color image. If the message embedded was a text message, then after every 7 bits of message are retrieved they are converted to decimal and this decimal value is the ASCII code of the 1st character in the message. This procedure is repeated until the full message is retrieved, and the message image is formed or the full text message is retrieved.

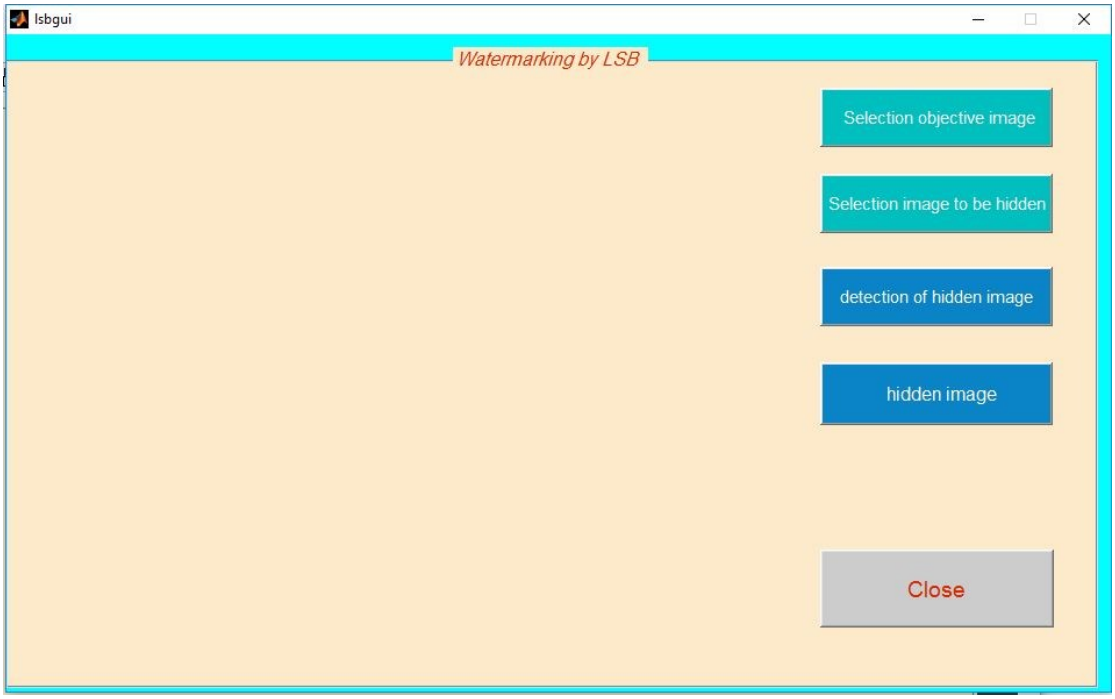
Chapter Three

Convert The Algorithm Into Programming Codes Using The Language Of The Matlab

There are a lot of programming methods for watermarks but we will use this simplified method .

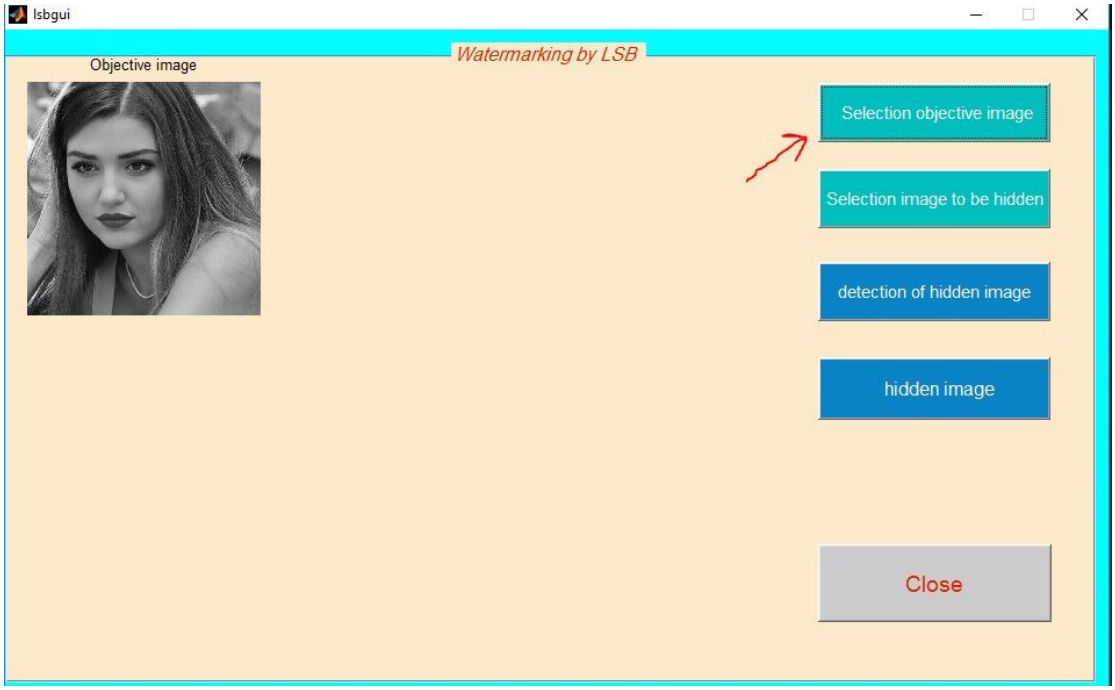
The application interface is programmed in the Matlab graphical interfaces and consists of five buttons each button with a specific layer

shown in image(1-3)



image(1-3)

The first button selects the objective image which we later hide another image shown in image (2-3).



Image(2-3)

The method of displaying the image is using Matlab by the following code

```
global im k
```
// Define variables to be used in other functions.

```
[path,user_cance]=imgetfile();//
```
There are many functions to call images and files and this function is used to fetch an image from the computer.

```
if user_cance
   msgbox(sprintf('Error'),'Error','Error');
```
// Warning message if we do not choose a picture.

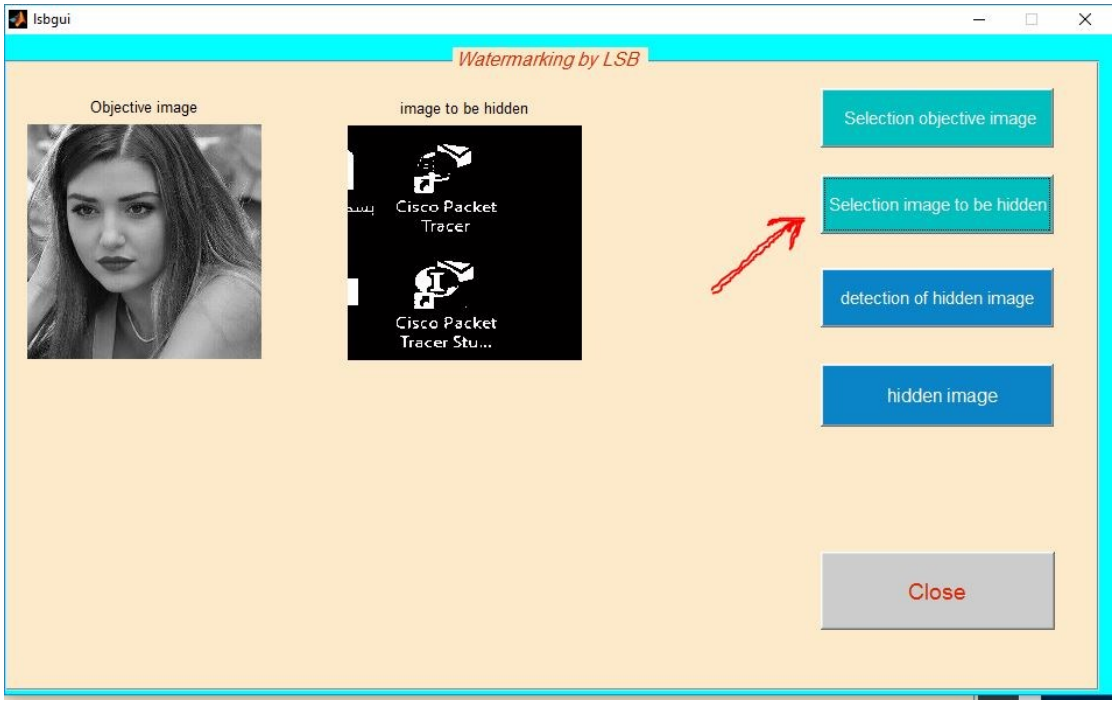
```
    Return
```
// Re-select the image again

```
end
im=imread(path);
j=imresize(im,[1000, 1000]);
```
//resizing taken image

```
k=rgb2gray(j);
```
//converting rgb image to gray image

```
axes(handles.a1); // View image in axes
imshow(k);// View the image after performing operations on it and converting it to a gray image.
```

The second button selects the image to be hidden or watermark from the computer shown in image(3-3)



Image(3-3)

When you press the button, it will fetch an image from the files and then convert it to a binary image according to the following code

```
global i z   // Define variables to be used in other functions.
[path,user_cance]=imgetfile();   //There are many functions to call images and files and this function is used to fetch an image from the computer.
```

```
if user_cance
    msgbox(sprintf('Error'),'Error','Error');  // Warning
```
message if we do not choose a picture.

```
    Return      // Re-select the image again
end
i=imread(path);
y=imresize(i,[1000, 1000]);\\ The function resizes the  image to
```
make the images the same size when installed or merged for the purpose of getting the best results.

```
z=im2bw(y);
axes(handles.a2);
imshow(z);
title('image to be hidden');
```

The third button is to hide the hidden image hidden in the first image after deleting the less important bits of the image as explained in the second chapter shown in image (4-3)

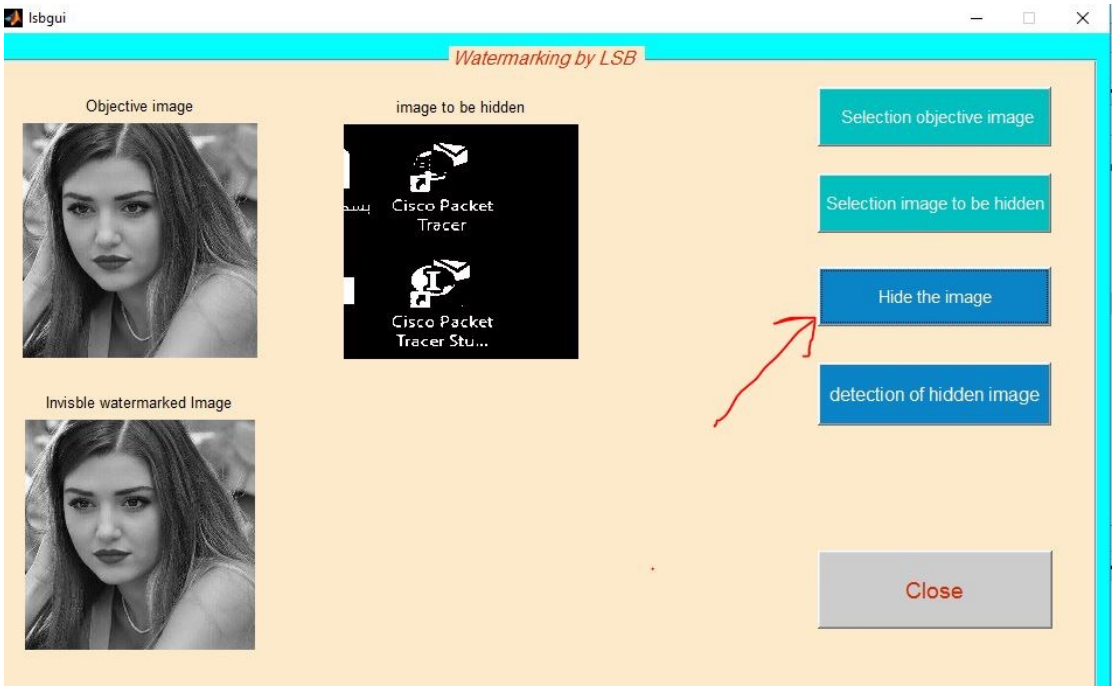


image (4-3)

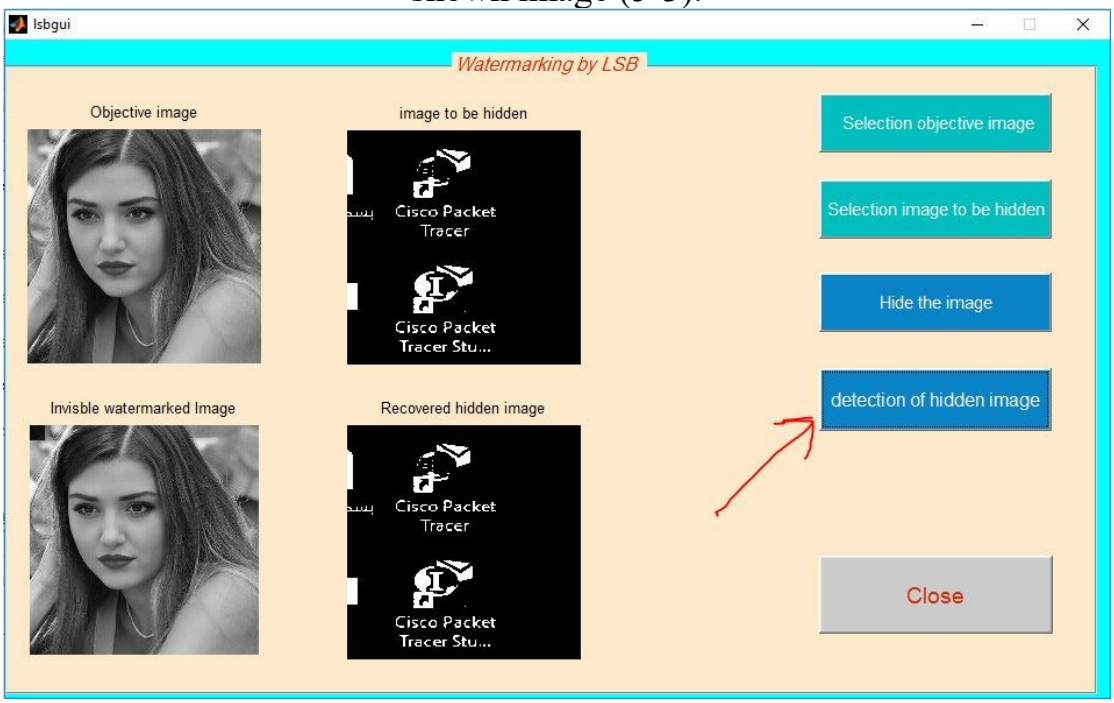
When you press the button, the Matlab will merge the two images, but after performing the LSB algorithm and the following code…

```
global l z k        // Define variables to be used in other functions.

z=double(z); \\ increasing range to double.

r=double(k+mod(k,2));\\ In this step we remove the LSB bit from the original image.


l=uint8(r+z); \\ Adding a little LSB to be hidden
```

The second image (watermark) is hidden in the original image where the bits have been deleted.

```
axes(handles.a3);
imshow(l)
title('Invisble watermarked Image');
```

The fourth button extracts the hidden image from the original image shown image (5-3).



Image(5-3)

Where the watermark is returned but not the same original quality as the following code……

```
global l   \\ Define variables to be used in other functions.

h=mod(l,2);
p=zeros(1000,1000);\\ The function resizes the  image to make the images the same size when installed or merged for the purpose of getting the best results.

for x=1:1000
    for y=1:1000
        if(h(x,y)==1)
            p(x,y)=255;
        end
    end
end
s=im2bw(p);
axes(handles.a4);
imshow(s);
title('Recovered hidden image')
```

What Is MATLAB?[11]

MATLAB is a high-performance language for technical computing. It integrates computation, visualization, and programming in an easy-to-use

environment where problems and solutions are expressed in familiar mathematical notation. Typical uses include:

- Math and computation
- Algorithm development
- Modeling, simulation, and prototyping
- Data analysis, exploration, and visualization
- Scientific and engineering graphics
- Application development, including Graphical User Interface building

MATLAB is an interactive system whose basic data element is an array that does not require dimensioning. This allows you to solve many technical computing problems, especially those with matrix and vector formulations, in a fraction of the time it would take to write a program in a scalar noninteractive language such as C or Fortran.

The name MATLAB stands for matrix laboratory. MATLAB was originally written to provide easy access to matrix software developed by the LINPACK and EISPACK projects, which together represent the state-of-the-art in software for matrix computation.

MATLAB has evolved over a period of years with input from many users. In university environments, it is the standard instructional tool for introductory and advanced courses in mathematics, engineering, and science. In industry, MATLAB is the tool of choice for high-productivity research, development, and analysis.

MATLAB features a family of application-specific solutions called toolboxes. Very important to most users of MATLAB, toolboxes allow you

to *learn* and *apply* specialized technology. Toolboxes are comprehensive collections of MATLAB functions (M-files) that extend the MATLAB environment to solve particular classes of problems. Areas in which toolboxes are available include signal processing, control systems, neural networks, fuzzy logic, wavelets, simulation, and many others.

THE MATLAB system consists of five main parts:

The MATLAB language.

This is a high-level matrix/array language with control flow statements, functions, data structures, input/output, and object-oriented programming features. It allows both "programming in the small" to rapidly create quick and dirty throw-away programs, and "programming in the large" to create complete large and complex application programs.

The MATLAB working environment.

This is the set of tools and facilities that you work with as the MATLAB user or programmer. It includes facilities for managing the variables in your workspace and importing and exporting data. It also includes tools for developing, managing, debugging, and profiling M-files, MATLAB's applications.

Handle Graphics.

This is the MATLAB graphics system. It includes high-level commands for two-dimensional and three-dimensional data visualization, image processing, animation, and presentation graphics. It also includes low-level commands that allow you to fully customize the appearance of graphics as well as to build complete Graphical User Interfaces on your MATLAB applications.

The MATLAB mathematical function library.

This is a vast collection of computational algorithms ranging from elementary functions like sum, sine, cosine, and complex arithmetic, to more sophisticated functions like matrix inverse, matrix eigenvalues, Bessel functions, and fast Fourier transforms.

The MATLAB Application Program Interface (API).

This is a library that allows you to write C and Fortran programs that interact with MATLAB. It include facilities for calling routines from MATLAB (dynamic linking), calling MATLAB as a computational engine, and for reading and writing MAT-file.

CONCLUSION

This paper reviewed the latest research work done on digital image watermarking. It presented the basic model of digital image watermarking for embedding and detection. Next, it mentioned the requirements of any digital image watermarking system. Then it listed some of the applications of digital image watermarking. Next, it showed the most significant techniques in both domains spatial domain and frequency domain. Then it mentioned the common attacks of digital image watermarking .

Finally, it highlighted the evaluation system of watermarking technology

REFERENCES

[1] Cox, I., Miller, M., & Bloom, J. , " Watermarking application and their properties ", paper presented at the proceedings of the international conference on information technology: coding and computing , Las Vegas, Nevada, 2000,March 27-29.

[2] 2013 IEEE 9th International Colloquium on Signal Processing and its Applications, 8 - 10 Mac. 2013, Kuala Lumpur, Malaysia" Properties of Digital Image Watermarking".

[3] Bender, W., " Techniques for Data Hiding ", IBM System Journal, Vol.35, 313(23), 1996.

[4] I.J. Cox, M.L. Miller, J.A. Bloom, Digital watermarking, Morgan Kaufmann, 2001

[5] A.Z. Tirkel, R.G. Van Schyndel, C.F. Osborne, A digital watermark, Proceedings of ICIP 1994, Austin Convention Center, Austin, Texas, Vol. II, 1994, pp. 86 –90.

[6] W. Bender, N. Morimoto, A. Lu, Techniques for data hiding, IBM Syst. J. 35 (3/4) (1996) 313–336.

[7] T.S. Chen, C.C. Chang, M.S. Hwang, A virtual image cryptosystem based upon vector quantization, IEEE Trans. Image Process. 7 (10) (1998) 1485–1488.

[8] L.M. Marvel, C.G. Boncelet, C.T. Retter, Spread spectrum image steganography, IEEE Trans. Image Process. 8 (8) (1999) 1075–1083.

[9] K.L. Chung, C.H. Shen, L.C. Chang, A novel SVD- and VQ-based image hiding scheme, Pattern Recognition Lett. 22 (9) (2001) 1051–1058.

[10] Chi-Kwong Chan, L.M. Cheng, Improved hiding data in images by optimal moderately signi7cant-bit replacement, IEE Electron. Lett. 37 (16) (2001) 1017–1018. [8] Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin, Image hiding by optimal LSB substitution and genetic algorithm, Pattern Recognition 34 (3) (2001) 671–683.

[11] wikipedia.MATLAB

[15] A. M. Zeki and A. Abdul Manaf, "A novel digital watermarking technique based on ISB (Intermediate Significant Bit)," World Academy of Science, Engineering and Technology, vol. 50, pp. 989-996, 2009.