جامعة القادسية

كلية علوم الحاسوب وتكنلوجيا المعلومات

قسم الوسائط المتعددة

Watermarking and steganography

بحث مقدم الى مجلس كلية علوم الحاسوب وتكنلوجيا المعلومات كجزء

من متطلبات نيل شهادة البكلوريوس

أعداد

عباس خضير مرزوك

أشراف

أ.رشا فلاح

2018-2017

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

" انما يخشى الله من عباده العلماء"

صدق الله العلي العظيم

أهداء

أحمد الله عز وجل على منه و عونه لإتمام هذا البحث

إلى الذي وهبني كل ما يملك حتى أحقق له آماله، إلى من كان يدفعني قدما نحو الأمام لنيل المبتغى، إلى الإنسان الذي إمتلك الإنسانية بكل قوة، إلى الذي سهر على تعليمي بتضحيات جسام مترجمة في تقديسه للعلم، إلى مدرستي الأولى في الحياة، أبي الغالي على قلبي أطال الله في عمره؛ إلى التي وهبت فلذة كبدها كل العطاء و الحنان، إلى التي صبرت على كل شيء، التي رعتني حق الرّعاية و كانت سندي في الشدائد، و كانت دعواها لي بالتوفيق، تتبعتني خطوة خطوة في عملي، إلى من إرتحت كلما تذكرت إبتسامتها في وجهي نبع الحنان أمي أعز ملاك على القلب و العين جزاها الله عني خير الجزاء في الدارين؛ إليهما أهدي هذا العمل المتواضع لكيّ أُدخل على قلبهما شيئا من السعادة إلى أخوتي و أخواتي الذين تقاسموا معي عبئ الحياة ؛ كما أهدي ثمرة جهدي لأستاذتي الكريمة: رشا فلاح الذي كلما تظلمت الطرق أمامي لجأت إليها فأنارتها لي و كلما دب اليأس في نفسي زرعت فيا الأمل لأسير قدما و كلما سألت عن معرفة زودتني بها و كلما طلبت كمية من وقتها الثمين وفرته لي بالرغم من مسؤولياتها المتعددة؛ إلى كل أساتذة قسم الوسائط المتعددة؛ و إلى كل من ...يؤمن بأن بذور نجاح التغيير هي في ذواتنا و في أنفسنا قبل أن تكون في أشياء أخرى

الى كل هؤلاء أهدي هذا العمل

Abstract

In this paper we will use both the watermark and steganography to embedding image by using LSB technique .In the watermark in the image where the logo is a binary image and the host image is a image with a grayscale ,the result is watermarked image . Steganography is one of the most powerful techniques to conceal the existence of hidden secret data inside a cover object. Images are the most popular cover objects for Steganography and in this work image steganography is adopted. There are several techniques to conceal information inside cover-image.in this project we will embedding logo(binary image) into grayscale image this will result the watermark image ,and then imbedding the watermark in cover image to obtain the stego image. This work has been implemented through MATLAB.

Contents

Chapter one

Steganography and watermarking

1-1:Introduction

Because of the spread of the Internet, the concept of watermarks was widely disseminated. At the time, a water message was inserted into the image to be transmitted so that the message would remain invisible to the intended or unintentional attacks. Komatsu and Tominaga was probably the first to use the term “digital watermarking” [1]. The purpose of digital watermarks is to protect the copyright and copyright of the intellectual property in digital form .

The watermark should not appear as a mark from the original image. Integrity and Security are also two essential requirements of ideal watermarking [4, 5]. If the water is used as a reference quality, Very strong so that they are highly resistant to any deformation that can be introduced during normal use (third attack), or deliberate effort to remove or change the watermark contained in the data / image that is transferred (intentional attack). Safety and security are also basic requirements of the watermark. water Its powerful is that withstand a wide range of attacks. . The information / logo is called in the image the watermark of the digital image. The information / logo where the watermark is to be embedded is called the host image [2, 3].

On other side the Steganography is a method or technique to hide information within a digital medium(sound,video,image).Derived from the Greek Covered Book and basically meant hiding information.Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient

knows of the existence of the message [1]. It is a way of communicating so that it can not detect the existence of a hidden message.

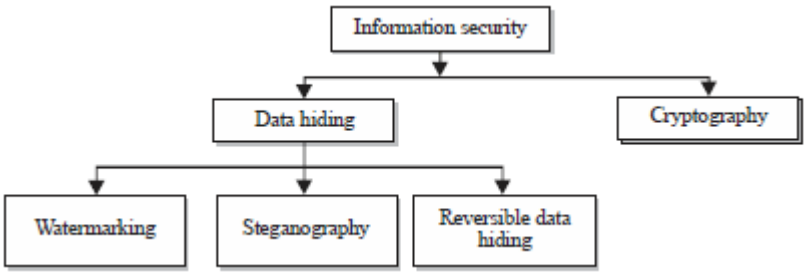
. The information that is hidden in the cover data is known as "stego". Data "stego" is the data that contains both the cover and the "embedded" information. Logically, the process of placing hidden or embedded data is sometimes defined in the casing data as the inclusion.

1-2: Differences Between Watermarking and Steganography

1-2-1: Steganography is changing the image in a way that only the sender and the intended recipient is able to detect the message sent through it. It is invisible, and thus the detection is not easy. It is a better way of sending secret messages than encoded messages or cryptography as it does not attract attention to itself.

There are many ways in which steganography is done. The messages appear as articles, images, lists, or sometimes invisible ink is used to write between the lines. Steganography is achieved by concealing the information in computer files. Sometimes steganography codes are inside the transport layer like an image file, document file, media files, etc. Due to the large size of the media files, they are considered ideal for steganography.

1-2-2: Watermarking is used to verify the identity and authenticity of the owner of a digital image. It is a process in which the information which verifies the owner is embedded into the digital image or signal. These signal could be either videos or pictures or audios. For example, famous artists watermark their pictures and images. If somebody tries to copy the image, the watermark is copied along with the image.



1-3: Watermarking is of two types; visible watermarking and invisible watermarking.

1-3-1:Visible Watermarking

As the name suggests, visible watermarking refers to the information visible on the image or video or picture. Visible watermarks are typically logos or text. For example, in a TV broadcast, the logo of the broadcaster is visible at the right side of the screen.

1-3-2:Invisible Watermarking

Invisible watermarking refers to adding information in a video or picture or audio as digital data. It is not visible or perceivable, but it can be detected by different means. It may also be a form or type of steganography and is used for widespread use. It can be retrieved easily.

1-4:Spatial domain and transform domain are two approaches for embedding watermarkin.

1-4-1:Spatial Domain Digital Watermarking

Spatial Domain Digital Watermarking is a technique for the insertion of watermarked information (side information defined by the owner) into the source (cover) image/video in the spatial domain.The most common

algorithm for spatial domain watermarking is Least Significant Bit Modification. This method changes the least significant bits (LSB) of chosen pixels in the image. It is possible to use more LSB bits of the container image in a similar way.

This method is comparatively simple. It can survive simple operations such as cropping and addition of noise. However lossy compression is going to defeat the watermark. Also, a simple attack that sets all the LSB bits to '1' will defeat the watermark with negligible perceptual impact to the cover object.

To extract the watermark, the LSB plane is extracted from the watermarked image and an exclusive-or operation is done using the watermark template.

1-4-2.Transform Domain Watermarking

The transform domain watermarking is better as compared to the spatial domain watermarking. The image is represented in the form of frequency in the transform domain watermarking. In the transform domain watermarking techniques, firstly conversion of the original image is done by a predefined transformation. Then we embed the watermark in the transform image or in the transformation coefficients. Finally, we take the inverse transform to get the watermarked image . Commonly used transform domain methods are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Discrete Fourier Transform (DFT).

Chapter two

matlab

2-1:MATLAB is a tool for technical computing, computation and visualization in an integrated environment. This document explains the basic concepts in MATLAB.MATLAB is an abbreviation for MATrix LABoratory, so it is well suited for matrix manipulation and problem solving related to Linear Algebra.MATLAB offers lots of additional Toolboxes for different areas such as Control Design, Image Processing, Digital Signal Processing, etc.

2-2:Some commands of watermark algorithm.

1-Uigetfile:

It allows you to access any file (image, sound or text) in any folder.

2-imread:

A = imread(filename) reads the image from the file specified by filename, inferring the format of the file from its contents. If filename is a multi-image file, then imread reads the first image in the file.

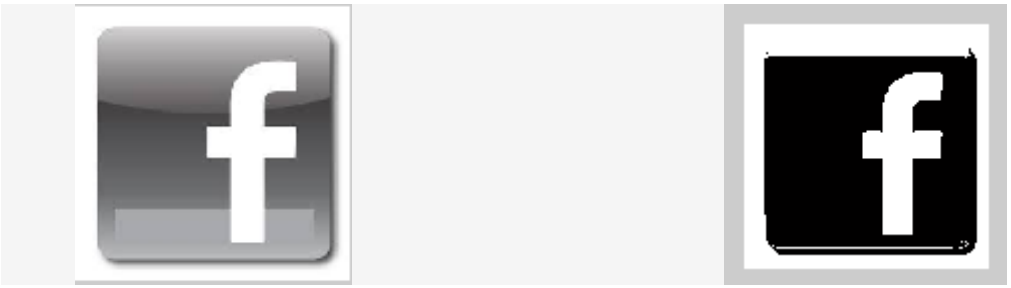
Convert RGB image or colormap to grayscale

3-Im2bw

converts the grayscale image I to a binary image. The output image BW replaces all pixels in the input image with luminance greater than level

with the value 1 (white) and replaces all other pixels with the value 0 (black). Specify level in the range [0,1]. This range is relative to the signal levels possible for the image's class. Therefore, a level value of 0.5 is midway between black and white, regardless of class. To compute the level argument, you can use the function graythresh. If you do not specify level, im2bw uses the value 0.5.

gray scale image binary image



4-inputdlg:

Create and open input dialog box

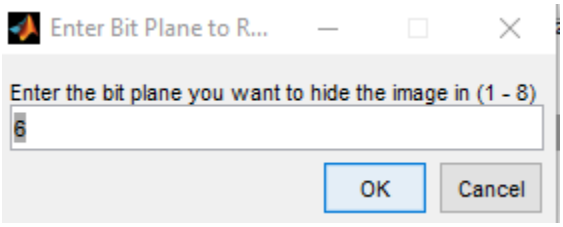
Example 1

Create a dialog box named Enter the bit plane you want to hide the image in (1 – 8)

```
prompt = 'Enter the bit plane you want to hide the image in (1 - 8) ';
dialogTitle = 'Enter Bit Plane to Replace';
numberOfLines = 1;
defaultResponse = {'6'};
bitToSet=str2double(cell2mat(inputdlg(prompt,dialogTitle,numberOfLines,defaultResponse)));
```

5-str2num:

matlab stores accept the input as a string,so convet the string to number using str2num



6-Size: it is used to find Size of object array

For example**:**

Create a random matrix and compute the number of rows and columns.

A = rand(4,3);

[m,n] = size(A) returns the number of rows and columns when A is a matrix.

m = 4

n = 3

7-imresize:it resize the dimension of image

B = imresize(A, [numrows numcols]) returns image B that has the number of rows and columns specified by [numrows numcols]. Either numrows or numcols may be NaN, in which case imresize computes the number of rows or columns automatically to preserve the image aspect ratio

for example :if we have the image A with dimension 177x284and we want to resize the dimension to

194*259

B = imresize(A, [194 259]);

The image B will be

Image A image B

8-bitset:

Set bit at specific location.

For example:

```
bits = 2:6;
val = [1 0 0 1 1];
intout = bitset(0,bits,val,'int8');
```

intout = 1*5

2 0 0 16 32.

9-Bitget:

Get bit at specified position.

For example:

From the another example of bitset we get the bits as follow:

```
Bits=2:6;
Getbit=bitget(intout,bits);
```

Getbit=

1 0 0 1 1.

2-3:Some commands steganography algorithm.

The instruction that we use to hide gray scale image in another is:

1-Dec2bin: Convert decimal to binary number in string.

Examples

Decimal 23 converts to binary 010111:

```
1-dec2bin(23)
ans =
  10111
```

2-Bin2dec: Convert binary number string to decimal number.

Example;

Binary 010111 converts to decimal 23:

```
bin2dec('010111')
ans =
  23
```

3-Reshape:it is used to reshape the dimension of array, The size of the array must remain the same after and before reshape.

Example; Reshape a 3-by-4 matrix into a 2-by-6 matrix.

```
A =
   1   4   7   10
   2   5   8   11
   3   6   9   12
    B = reshape(A,2,6)
B =
  1   3   5   7   9   11
   2   4   6   8   10   12
```

Chapter three

Algorithm and representation

3-1:LSB watermarking

In this technique we will merge the bits of the image to empedd with the host image if we has the first pixel of the original image = 118 and the first pixel of the logo image is = 1 and add to the LSB of original pixel image, the original will be 119 This methods called the lsb Watermarking.for example

1 180 = 181

1 166 = 167

1 135 = 136

0 131 = 130

0 142 = 142

3-2:Image Steganography

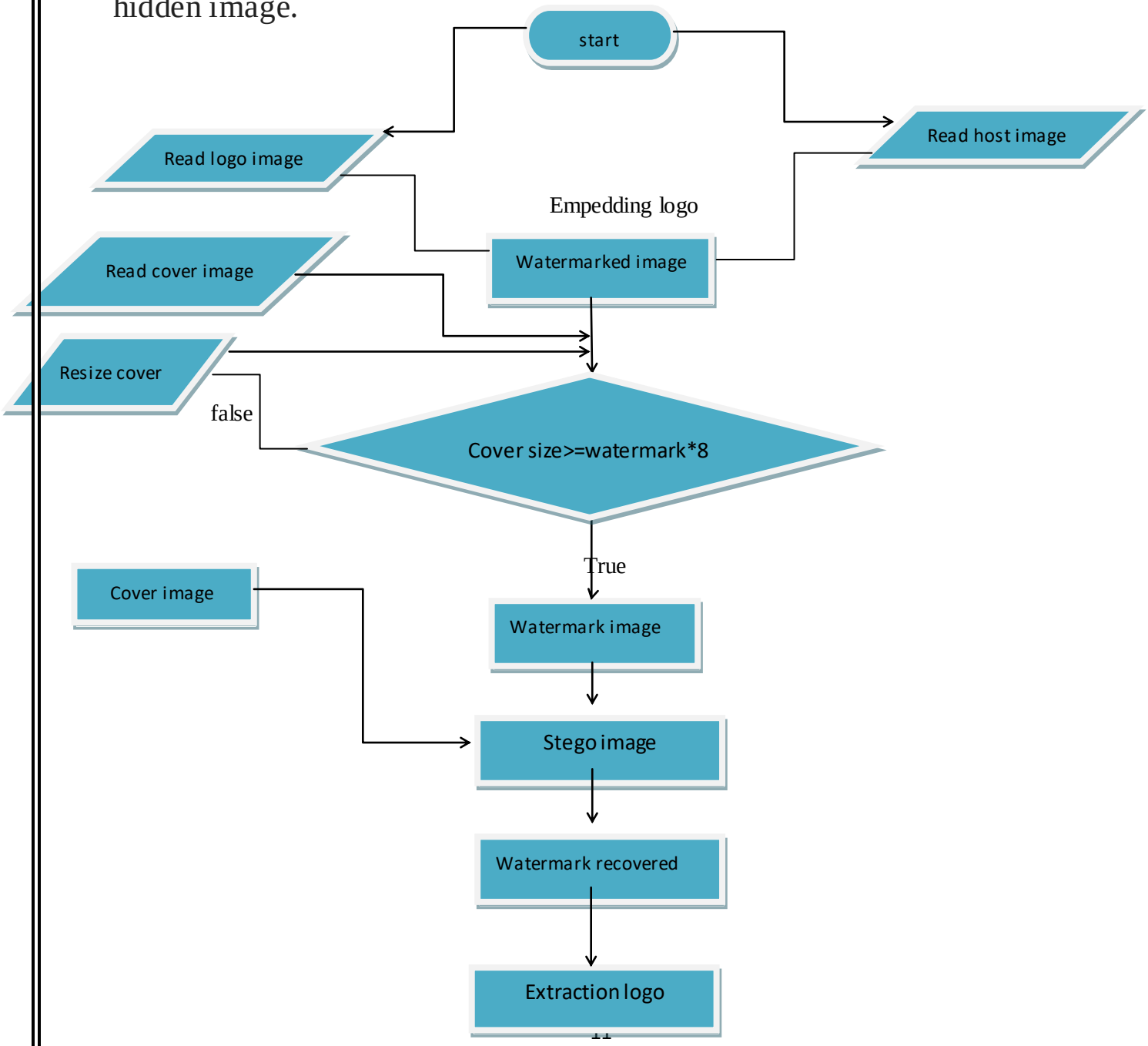
The image steganography is the process in which we hide the data within an image so that there will not be any perceived visible change in the original image. The conventional image steganography algorithm is LSB embedding algorithm.

3-3: LSB steganography

In LSB steganography, the least significant bits of the cover media's digital data are used to conceal the message. The simplest of the LSB steganography techniques is LSB replacement. [6] LSB replacement steganography changes the last bit of each of the pixel values to reflect the message that needs to be hidden. Consider an 8- bitgrayscale bitmap image where each pixel is stored as a byte representing a gray scale color value. Suppose the first eight pixels of the original image have the following gray color values:01010010 01001010 10010111 11001100 11010101 01010111 00100110 01000011

To hide the letter A whose binary value of ASCII code is 10110101, we would replace the LSBs of these pixels to have the following new values: 01010011 01001010 10010111 11001101 11010100 01010111 00100110 01000011.

If we use this technique to hide the image inside the image you will be hiding every bit of the hidden image in the LSB From the original image, in this case one bit of the hidden image will be hidden in eight bits of the original image, so the original image must be 8 times larger than the hidden image.



3-4:Algorithm of watermark and steganography:

A-hidden process:

Step 1:Read host image and convert it to gray scale image.

Step 2:read logo image and convert it to binary.

Step3:enter the bit plan that you want to hid binary image in using inputdlg.

Step4: make the host image and logo the same size using imresize.

Step5:find the size of the host image.

Step 6:store the host image in another variable called watermarked image.

Step 7:store first pixel value of logo to least significant bit of host image by using bitset function.

B- emppeding watermark image in cover image:

1-read original image(cover image) and convert it to grayscale image .

2-convert cover image from decimal 2bin number.

3-convert watermark image from decimal to bin.

4-find the size of cover image and watermark image.

a-If the size of the image cover is larger than the size of the watermark image then.

b-if the size of the image cover is smaller than the watermark image than we resize it.

5-embedding every bit from pixel of watermark image in LSB of cover image .

6-now we have the stego image but in bin number ,we must convert it to decimal number.

im1=uint8(bin2dec(host));

7-reshape the stego image to original size.

im1=reshape(im1,ori_row,ori_col);

8-imshow stego image

C-Extract watermark image from cover image as follow:

1-Find the size of cover image.

2-Create a zero matrix with the same sizes as the watermark image

3-convert the zero image from dec to bin number using dec2bin function.

4-convert the stego image from dec to bin number.

6-extract the watermark image from the stego.

7-now we obtain the watermark image but in bin number ,we convert it to dec number.

8-reshape the watermark image into the original sizes.

9-imshow the watermark image.

D. EXTRACTION OF WATERMARK USING LEAST SIGNIFICANT BIT Extracting watermark is the process of getting the logo from the host image. Algorithm to Retrieve Watermark:

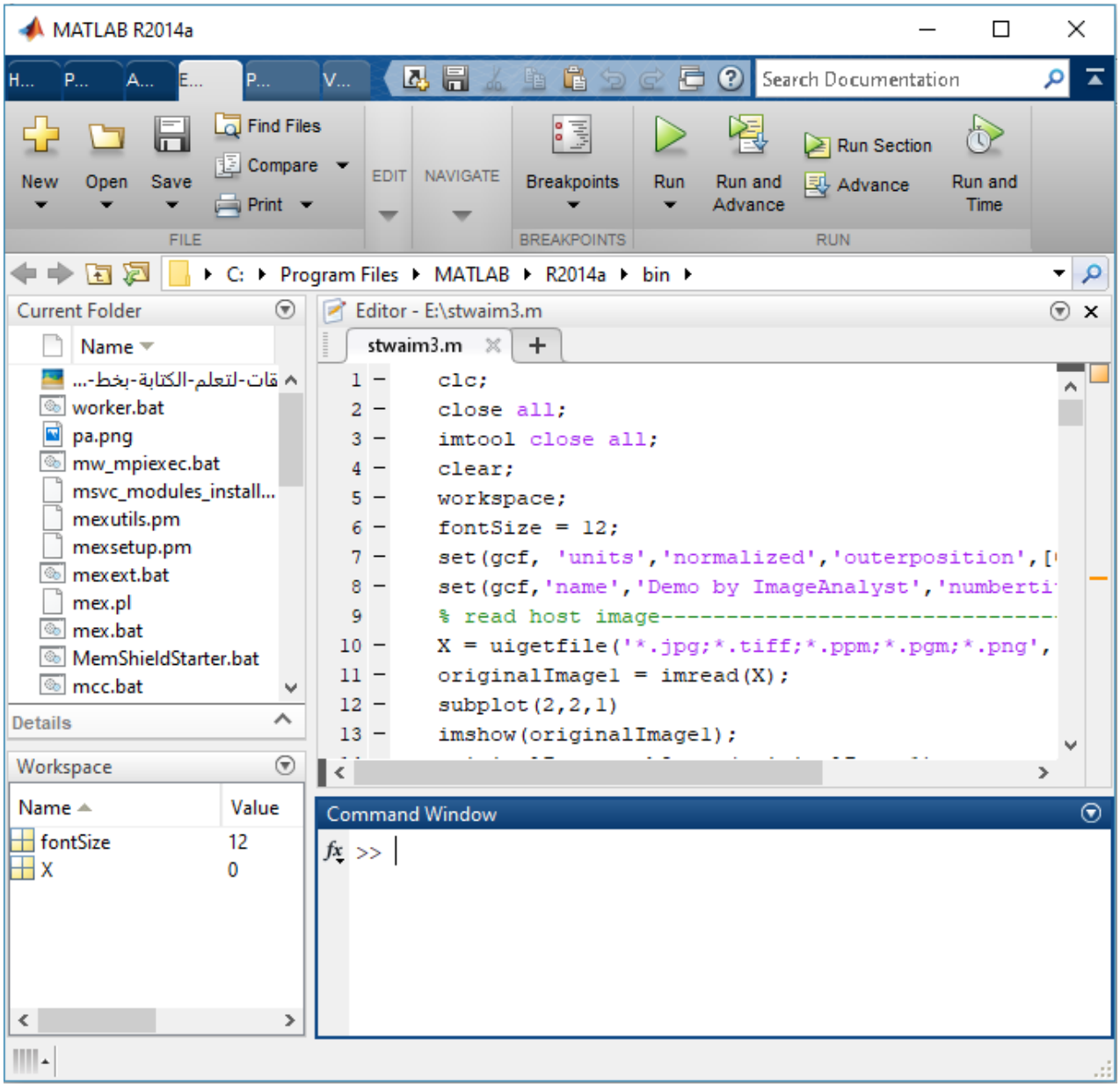
Step 1 : create of a zero matrix must be the same size as the image watermark.

Step 2 Extract least significant bit of watermarked object using bit get( ) function to obtain the watermark image, Then put the output in the zero matrix.

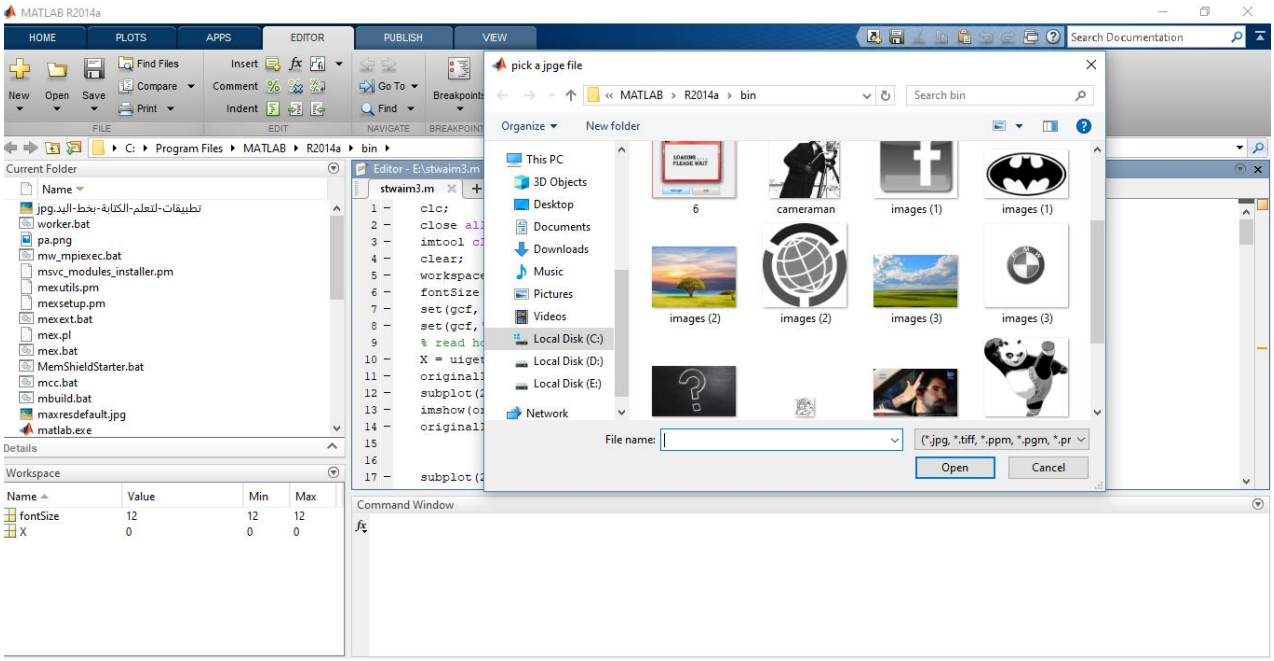
Step3:display the watermark image.

3-5:execution in matlab.

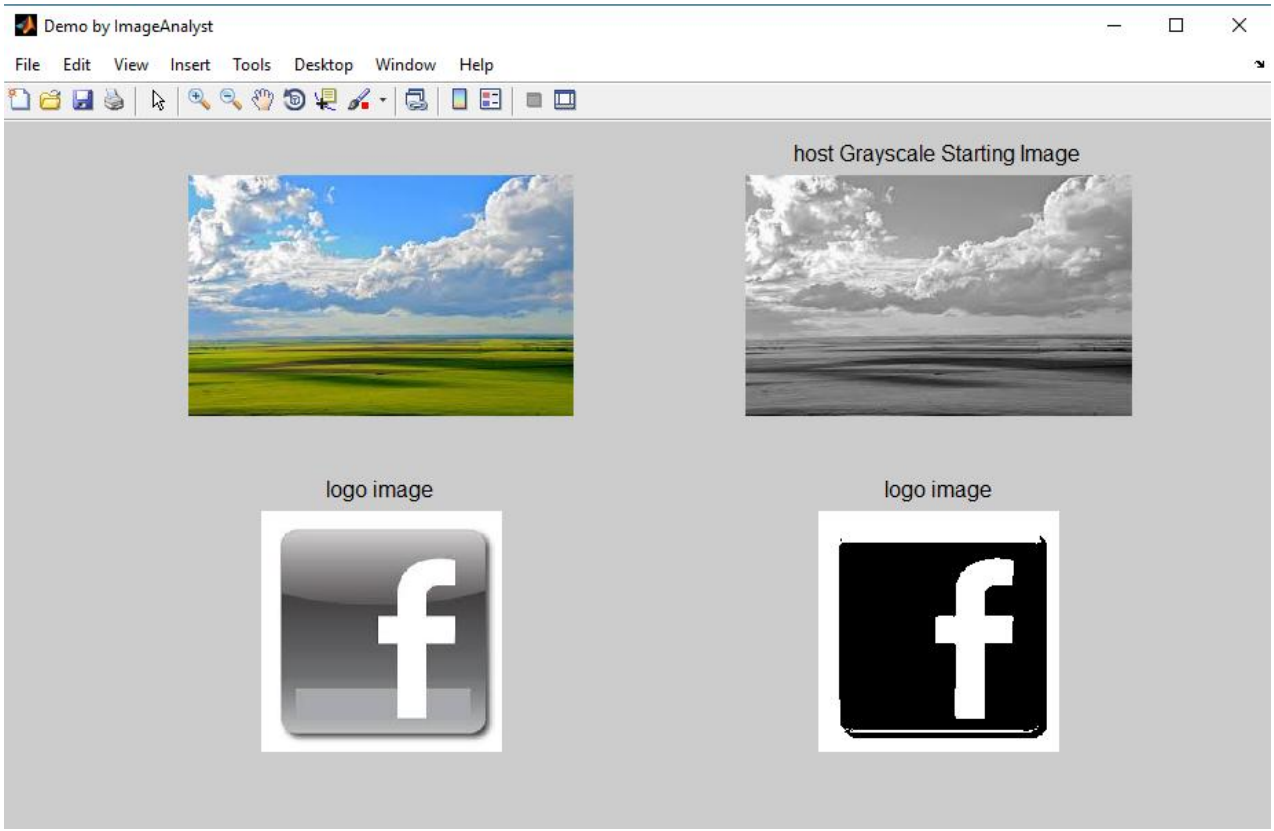
1-open matlab.



2-read image



3-result of the execution process.



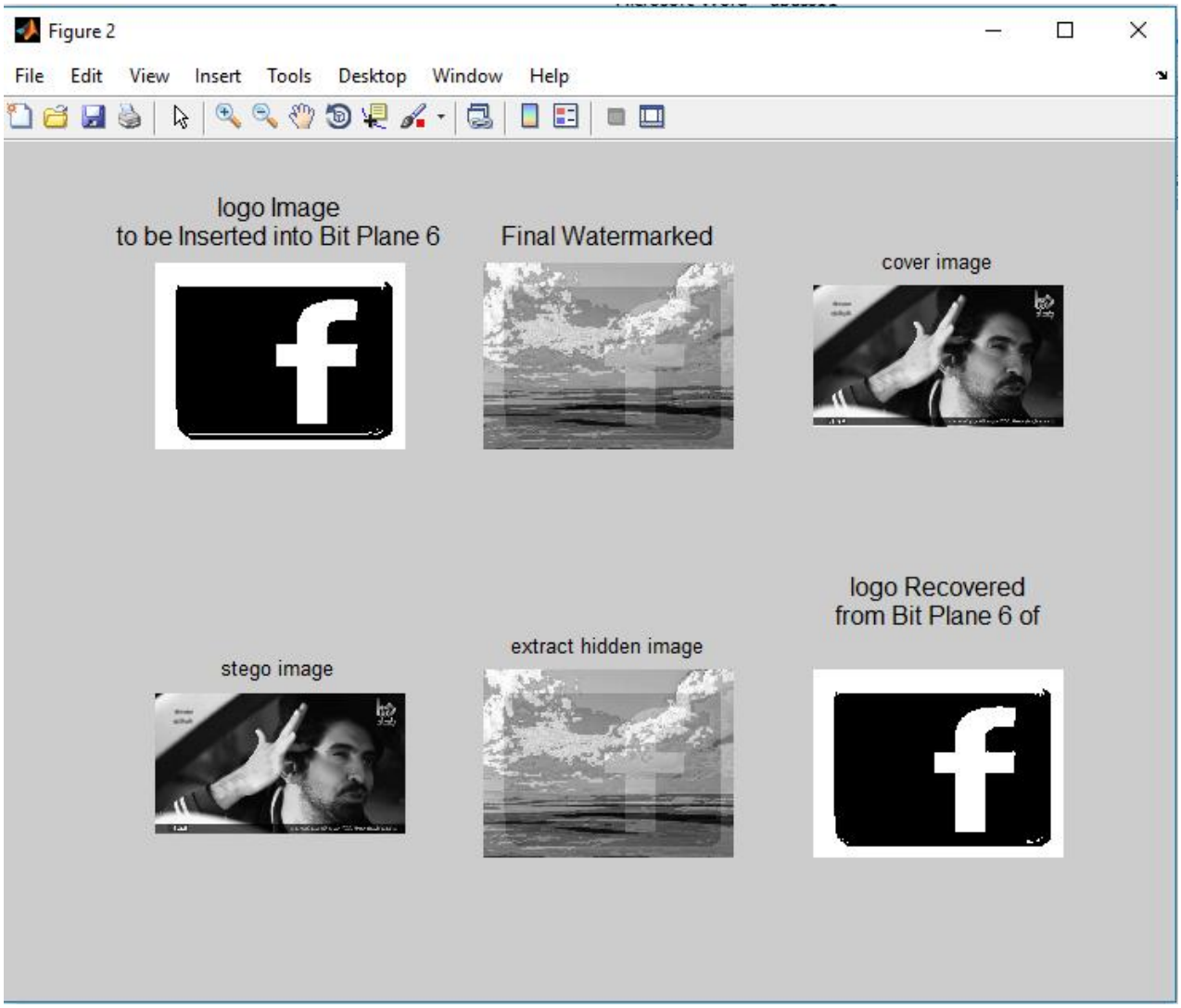


Figure 2
File Edit View Insert Tools Desktop Window Help
logo Image
to be Inserted into Bit Plane 6
Final Watermarked
cover image
logo Recovered
from Bit Plane 6 of
extract hidden image
stego image

Chapter four

Conclusion and discussion

4-1. Conclusion and discussion

1-choosing of the image(we must choose the cover image that is larger than the hidden image).

2-in the watermark the size of the host image is the same size of the logo.

3-typing of the image we using the binary image in watermark to hidden in grayscale,and hidden grayscale watermark image in grayscale image.

4-2: feature work

1-we can use the color image in watermark.

2-we can use the color image in steganography.

3-we can use watermark image in video.

4-we can use hidden image in video.

5-we can use watermark and hidden image in video.

Chapter five

Refrences

References:

[1] Bender, W., Gruhl, D., Morimoto, N. and Lu, A(1996).: Techniques for data hiding. IBM Systems Journal, vol. 35, nos. 3&4.

[2] Saraju Prasad Mohanty(‚January 1999)“Watermarking of Digital Images”, Submitted at Indian Institute of Science Bangalore, pp. 1.3 –1.6.

[3] Katzenbeisser, S. and Petitcolas, F(1999).: Information hiding techniques for steganography and digital watermarking. Artech House Books.

[4] Van Dijk, M. and Willems, F(May 15-16, 2001).: Embedding information in grayscale images. Proc. 22 nd Symposium on Information and Communication Theory in the Benelux, pp. 147-154, Enschede, the Netherlands.

[5] R. Chandramouli and N. Memon,"Analysis of LSB based Image Steganography", IEEE ICIP, pp. 1022-1022, Oct. 2001.

[6] M. Pavani1, S. Naganjaneyulu, C. Nagaraju, ”A Survey on LSB Based Steganography Methods” International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 8 August, 2013 Page No. 2464-2467