Design and implementing securely hiding system using Neighborhoods of the pixels

Wijdan R Abdulhussien
College of Computer and Mathematical
Thi-Qar University
Wijdan_r_a@yahoo.com

Abstract

Embedding techniques play an important role in concealing secret messages inside images; in this research a hide security of confidential message(text or image) system in the digital image has been proposed using a new way to hide data depending on the neighborhoods of pixels.Alsothe access has been restricted by a password requested from the user to add more security to the proposed system,the extraction algorithm that requires another password known only to thereliable recipient that was also concealed within the image.

Hiding the secret message inside the cover image is using the eight neighborhoods of the pixels, and the system will determine this pixel which will be concealment in its neighborhoods is accordance with an agreed formula between the sender and the recipient. Data embedding has been in a different manner from pixel to another depending on their location in the image, If it is in the individual sites, the embedding will be in anti-clockwise else it will be clockwise as well as the use of passwords given higher security and resistance against extraction by the attackers, thus proved the ability of the proposed algorithm to embed and extract the confidential messages without errors.

Keywords–Steganography, LeastSignificant Bit, pixels' Neighborhood processing**,** digital image.

1 Introduction

Since the rise of the internet, one of the most important factors of information technology and communicationhas been the security of information. Cryptography was created as a technique for securing the secrecy ofcommunication .Unfortunately it is sometimes not enough to keep the contents of a message secret, it mayalso be necessary to keep the existence of the message secret. The technique used to implement this, is calledsteganography (Morkeletal. 2005).

Steganography is the art of hiding information in waysthat prevent the detection of hidden messages. It comes under the assumptionthat if the feature is visible, the point of attack is evident, thusthe goal here is always to conceal the very existence of theembedded data (Nag etal.,2010), (Johnson&Jajodia, ,1998).In image steganography the information is hidden exclusively in images.

Steganography andcryptography are both ways to protect information from unwanted parties but neither technology alone is perfectand can be compromised (Wang &Wang ,2004),(Channalli&Jadhav ,2009).

The outline of the paper is as follows: An overview ofsteganography and imagesteganographywere reviewed in Section 2. The proposed system and steganography algorithm was presented in Sections3. Experimental results and conclusions are presented in Sections 4 and 5, respectively.

2Steganography

Steganography is hidden the secret message into another message, this message (secret messages) could not notice any body, if notice then it can be read (Kumar,2013).The goal of Steganography is tohide messages inside other harmless messages in away that does not allow any enemy to even detectthat there is a second message present (Thampi,2004).
The following is a list of steganography terms:
1) **Carrier file:** A file which has hidden information inside of it.
2) **Steganolysis:** The process of detecting hidden information inside a file.
3) **Stego-medium:** The medium in which the information is hidden.
4) **Redundant bit:** A pieces of information inside a file which can be overwritten without damaging the file.
5) **Payload:** The information which concealed.
Steganography are divided into four different categories: text, image, audio and video.

2.1Image Steganography

Image Steganography is widely used for message hiding process because this is quite simple and secure way to transfer the information over the communication network on the internet (Kumar, 2013).
Images are the most popular cover objects used for steganography. In the domain of digitalimages many different image file formats exist (Khareetal., 2010).In digital image steganography, the secret message is embedded within a digital image called cover-image. Cover-image carrying embedded secret data is referred as stego-image (Saha& Sharma, 2012).

2.2Image Definition

To a computer, 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. Most images on the Internet consists of a rectangular map of the image's pixels (represented as bits) where each pixel is located and its colour. These pixels are displayed horizontally row by row (Morkeletal. 2005).
The number of bits in a colour scheme, called the bit depth, refers to the number of bits used for each pixel. The smallest bit depth in current colour schemes is 8, meaning that there are 8 bits used to describe the colour of each pixel. Monochrome and grey scale images use 8 bits for each pixel and are able to display 256 different colours or shades of grey. Digital colour images are typically stored in 24-bit files and use the RGB colour model, also known as true colour (Morkeletal. 2005) ,(Kumar,2013),(Khare etal.,2011).

2.3Image Domain

Information can be hidden many different ways in images. Straight message insertion can be done, which will simply encode every bit of information in the image. More complex encoding can be done to embed the message only in ``noisy" areas of the image that will attract less attention. The message may also be scattered randomly throughout thecover image. The most common approaches to information hiding in images are:

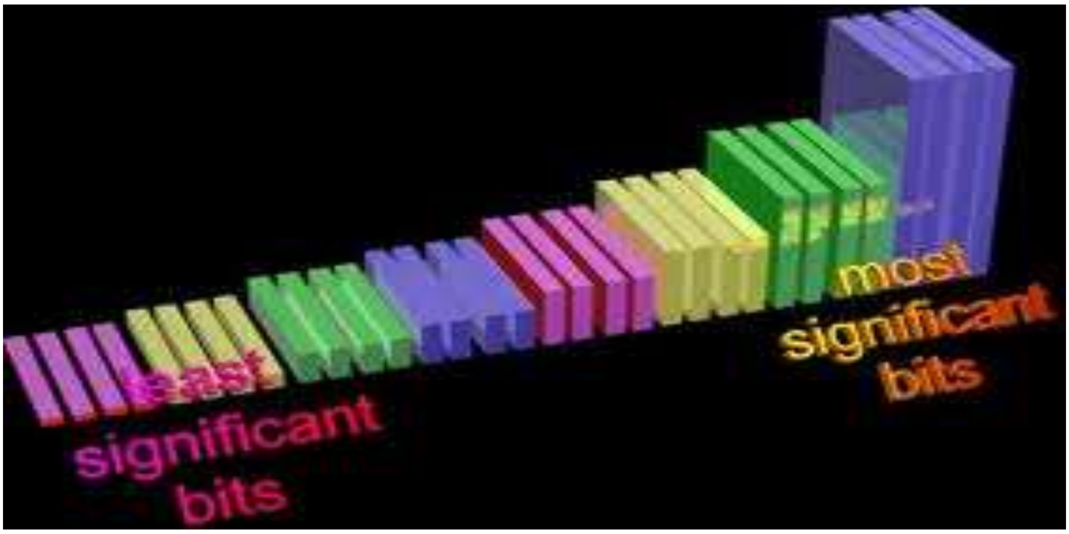
- Least significant bit (LSB) insertion
- Masking and filtering techniques
- Transformations

2.3.1 Least Significant Bit

The simplest approach to hiding data within an image file is called least significant bit (LSB) insertion. In the LSB insertion method we can take a binary representation of hidden data and overwrite the LSB of each byte within the cover image (Kumar,2013).
When using a 24-bit image, a bit of each of the red, green and blue colourcomponents can be used, since they are each represented by a byte(Morkeletal. 2005).When applying LSB techniques to each byte of a 24-bit image, three bits can be encoded into each pixel. Any changes in the pixel bits will be indiscernible to the human eye (Thampi,2004).
The high- order, or most significant , bit is the one with highest arithmetic value (i.e.,2^7 =128) while the low-order ,or least significant ,bit is the one with lowest arithmetic value (i.e.,2^0 =1) see figure 1.

3- The Proposed System

In this paper we proposes a system to protect the privacy of the data using an algorithm that is designed to hide the data inputted within an image. The proposed system provides an image platform for user to input image and a text box to insert texts. Once the proposed algorithm is adapted, user can send the stego-image that can later send to other computer user so that the receiver is able to retrieve and read the data which is hidden in the stego -image by using the same proposed system.



Figure(1): high and Low – order bit

3-1 The Components of the Proposed System

Figure2 describe the proposed system starting from login the system by either sender or receiver. Once getting the granted access user can use the application or he may logout. While using the system we can embed or extract the secret message.

After login, the user canloading image and enter secret message(text or image) then performing embedding stage of the proposed algorithm by replacing the LSBs of the neighborhoods by bits of secret message either clockwise or anti-clockwise as a different manner from pixel to another depending on the position of central pixel,also before applying the algorithm the sender use another password for embedding that also embedding in an image which gave resistance against extraction by the attackers.

Figure 3 show the proposed method for positions of Neighborhoods that have been used for hiding secret message and the central pixels that have been used for hiding the embedding the password.

As we taking the eight Neighborhoods of central pixels, by using blocks of 3*3 then

$$The\ number\ of\ central\ pixels = int\left(\frac{no.rows*no.columns}{3*3}\right)\ldots\ldots\ \ (1)$$

This will expanding for 16 and 24 bit image if we take into account the RGB bits thus will increase the number of characters that have been hidden.

The number of characters that can be hiding in an image depending on the type of image (8, 16, 24).

As example: in 8 bit image, the equation that used is as follows:-

$$The\ number\ of\ characters = the\ number\ of\ central\ pixels\ \ldots\ldots\ \ (2)$$

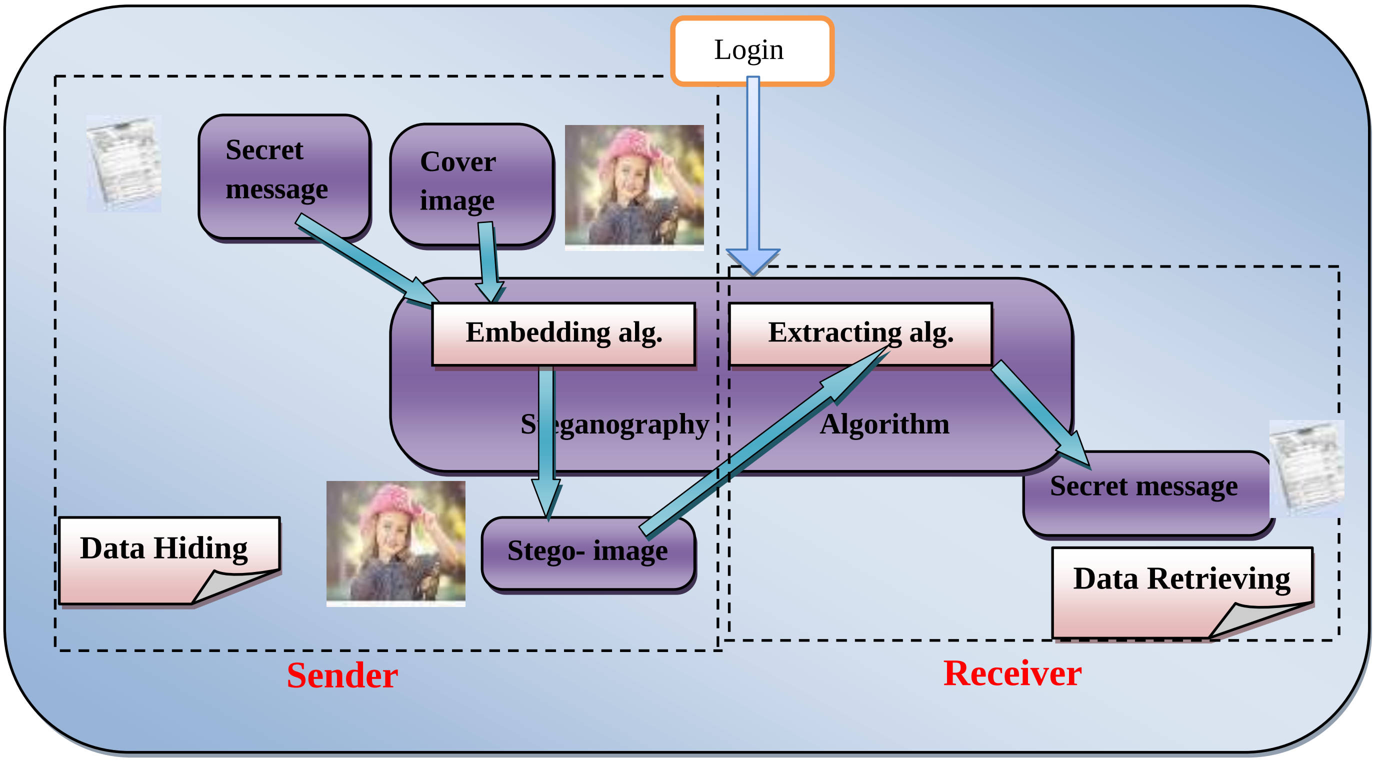


Figure (2): The framework for the system

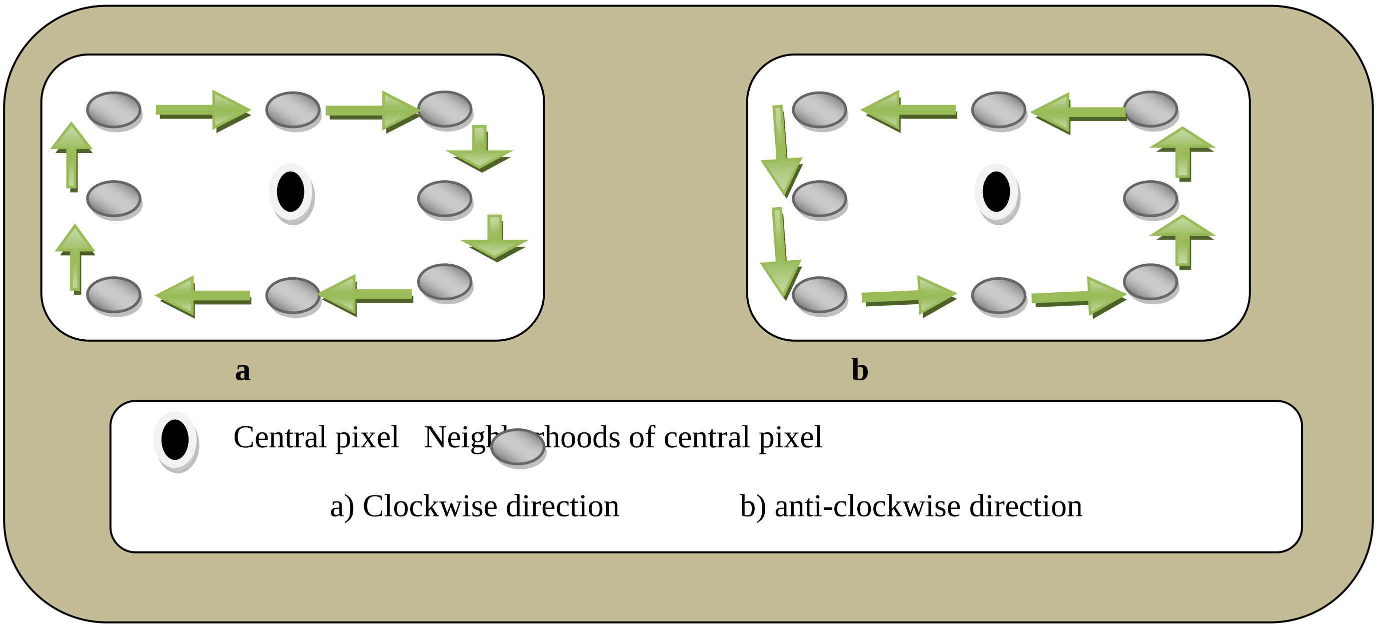


Figure (3): The clockwise and anti-clockwise direction

3.1.1 Proposed Steganography Algorithm

In general, the proposed algorithm consists of two basic stages; each stage consists of many steps, as illustrated bellow.

First Stage: Message Hiding Stage:

For embedding a message, a new method has proposed using the eight Neighborhoods of the pixelsin a different manner from pixel to another as explain in figure 3.also the embedding password has been used as more secure for the system ,Figure(4)showsthe flowchart for embedding algorithm.

The algorithm for embedding in an image:-

Step 1: -inter the embedding password.

Step2:- image units of the cover image are converted to the ASCIIcode thento binary representation,thus value of 255 turnsto11111111.

Step 3:- Add a sign"#" at the end of the secret message as an indicationof the end of the text (this will be useful in the extracting stage).

Step 4: -Each text characters(or pixels values of secret image) turned into a digital value using ASCIIcode.

Step 5: -Each value (ASCII) of the text(or pixels)has been turned into a binaryrepresentation, as example (value 65 for the character (A)turns to 01000001), and starting from the position (row=2, col=column =2).

Step 6: Hiding the embedding password by applying the following:-

1- Adding a sign "*" at the end of it as an indication of the end of it. Repeat steps 4 and 5on embedding password to obtain the binary representation of it (binary-embedding-pass), starting from pixel (2, 2).

2- While not reach the length (binary-embedding-pass) do
Replace the least significant bit of the pixel (row.col) by bit of the (binary-embedding-pass).

- Find the next central pixel (row,col) tomake sure not intersect with the position of Neighborhoods of pixel that have been used for hiding secret message.
- Take the next bit of the (binary-embedding-pass).

Step 7:-For each character and starting from pixel (row=2, col=2) ofthe cover image do:

1- For pixel (row, col), finding the eight Neighborhoods of pixel.

2- If (row+col) Mod 2=0

- Replace the least significant bits of the eight Neighborhoods of the pixel by eight bits of binary representation of thecharacter (or binary representation of pixel)using clockwisemethod.

Else

- Replace the least significant bits of the eight Neighborhoods of the pixel by eight bits of binary representation of the character (or binary representation of pixel)using anti-clockwise method.

3- If not reach the end of secret text (or the pixels for the secret image)

- Get the next character.
- Find the next pixel that will hiding in its Neighborhoods
- Repeat step 5 starting from the new pixel (row, col).

Else

- Store the newstego-image.

Step 8: -end

Second Stage: Message Extracting Stage:

In the process of disclosing secret message process, we have to login the system by giving the correct password. If the password is not correct as the password given at time of embedding, the system will not allowed to disclose the secret message.

For retrieving the data from an image, a stego-image, the length of message and the extracting algorithm is required, we can dispense with knowledge of the length of the secret message which was hidden in the image can be attained by finding the same symbol that has been put at the end of the secret message at embedding stage.
Figure5describe the flowchart for the extracting algorithm.

The algorithm for retrieving is as the following:-

Step 1: - image units of the cover image are converted to the ASCII code.
Step 2: -ASCII code are converted to the binary representation.
Step 3:-Enter Rec-password (must be exactly as embedding password).
Step 4:-Extract the embedding password by applying the following:-

1- Starting from pixel (2, 2)char –Sen="".
2- While char –Sen don't equal to"*" do
    -Sen-pass=Sen-pass+Char-Sen.
    - char-Sen="" ,Bin-Sen="",i=0.
    -Repeat until i==8.
    - get the LSB from the pixel(Row.Col),
    - i=i+1,Bin-Sen=Bin-Sen+LSB.
    - Get the next pixel (Row=Row+3, Col).

- Find the ASCII code for(Bin-Sen).
- Find the string character for ASCII code"Char-Sen".
- i=0.

Step 5:-if (Sen-pass #Rec-password) then print" uncorrected password" and exit the algorithm by go to step 8.
Elsecomplete the remaining steps of the extraction algorithm.
Step 6:-Initialize (Text="") andboth row and column for the pixel as(row=2, col=2).
Step 7: - For pixel (row, col) do:

1- Finding the eight Neighborhoodsof pixel.
2- If (row+col) mod 2= =0

- Getting the least significant bits of the eight Neighborhoods of the pixels using clockwise method.

Else

- Get the least significant bits of the eight Neighborhoods of the pixels using anti-clockwise method?

3- Assembled them to form the eight bits of binary representation of thecharacter(for secret image, it represent the value of the pixel).
4- Find the ASCII code from binary code representation.
5- Find the string character for each ASCII code.
6- Add the character to the last of the text, Text=Text character (for secret image these values will be form the image).
7- If the character don’t equal to "#" or any code agreed between the sender and the recipient
    - Get the next character(or the next pixel for secret image).
    - Finding the next pixel that the bits have been stored in its Neighborhoods.
    - Repeat step 5 starting from the new position of the pixel.

Else

- Print secret text(or save the secret image).

Step 8: -end.

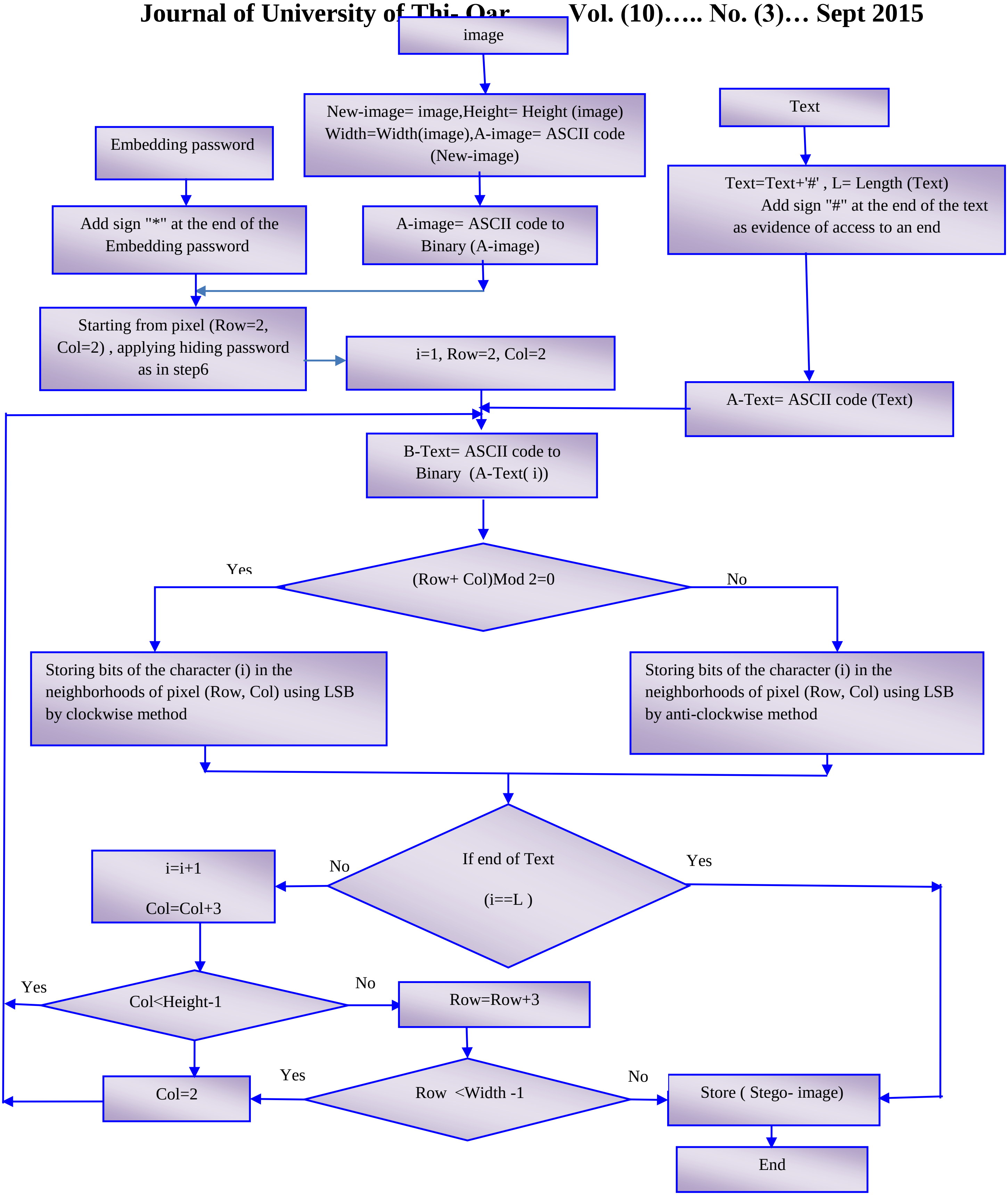


image
New-image= image,Height= Height (image) Width=Width(image),A-image= ASCII code (New-image)
Text
Embedding password
Add sign "*" at the end of the Embedding password
A-image= ASCII code to Binary (A-image)
Text=Text+'#' , L= Length (Text) Add sign "#" at the end of the text as evidence of access to an end
Starting from pixel (Row=2, Col=2) , applying hiding password as in step6
i=1, Row=2, Col=2
A-Text= ASCII code (Text)
B-Text= ASCII code to Binary (A-Text(i))
Yes
(Row+ Col)Mod 2=0
No
Storing bits of the character (i) in the neighborhoods of pixel (Row, Col) using LSB by clockwise method
Storing bits of the character (i) in the neighborhoods of pixel (Row, Col) using LSB by anti-clockwise method
i=i+1
Col=Col+3
No
If end of Text
(i==L)
Yes
Yes
Col<Height-1
No
Row=Row+3
Yes
Row <Width -1
No
Col=2
Store (Stego- image)
End

Figure (4): Flowchart for embedding text in an image

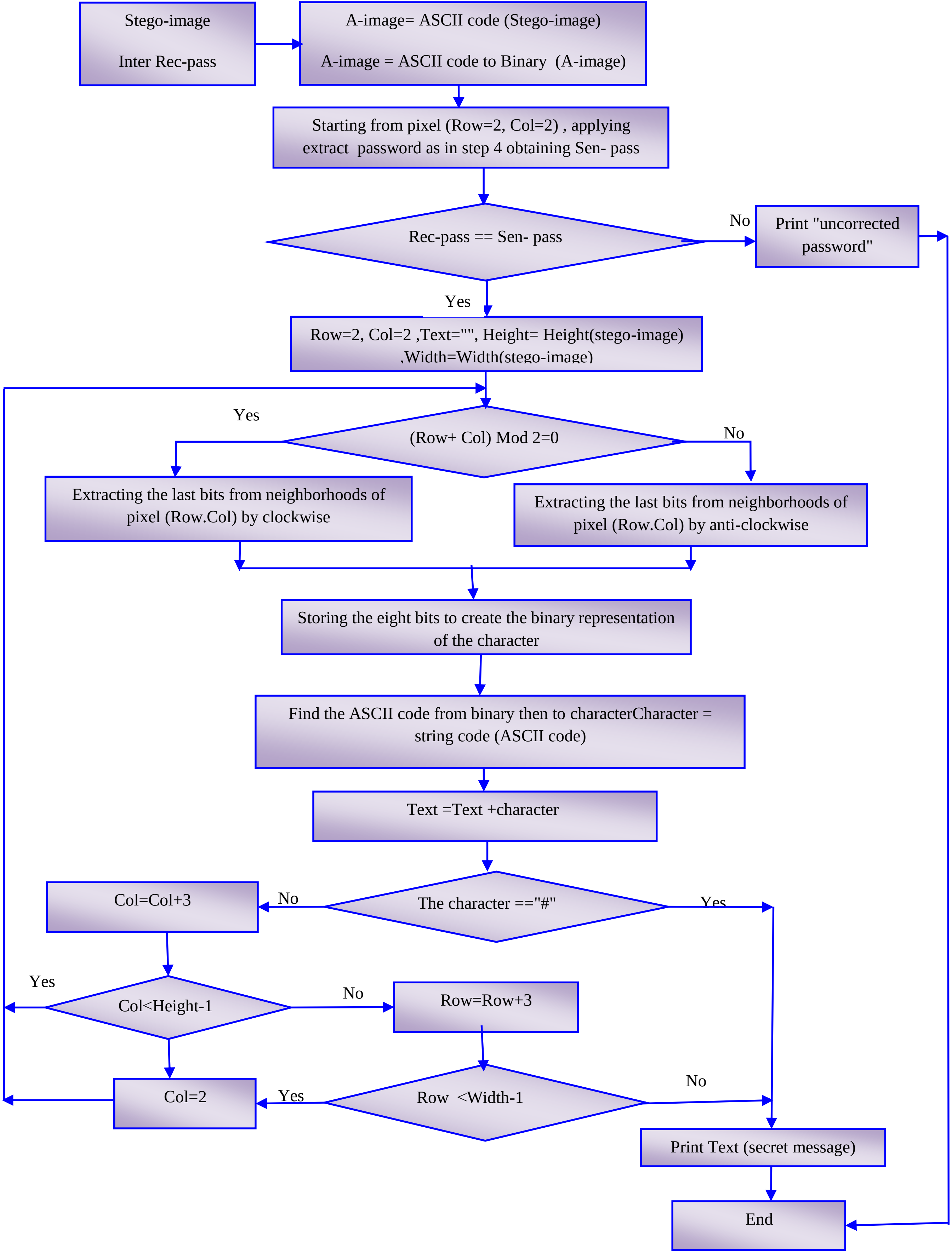
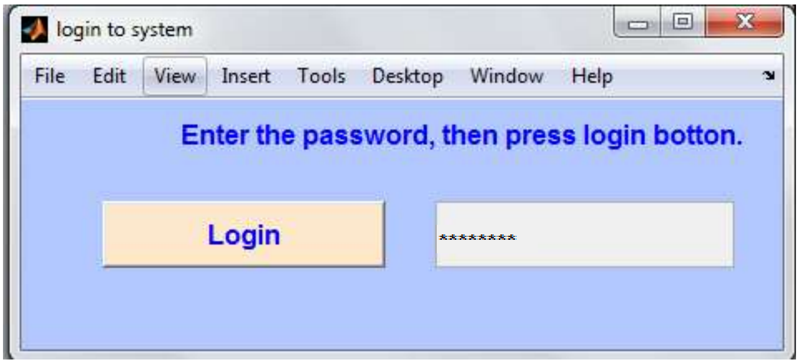

Stego-image
Inter Rec-pass
A-image= ASCII code (Stego-image)
A-image = ASCII code to Binary (A-image)
Starting from pixel (Row=2, Col=2) , applying extract password as in step 4 obtaining Sen- pass
Rec-pass == Sen- pass
No
Print "uncorrected password"
Yes
Row=2, Col=2 ,Text="", Height= Height(stego-image) ,Width=Width(stego-image)
Yes
(Row+ Col) Mod 2=0
No
Extracting the last bits from neighborhoods of pixel (Row.Col) by clockwise
Extracting the last bits from neighborhoods of pixel (Row.Col) by anti-clockwise
Storing the eight bits to create the binary representation of the character
Find the ASCII code from binary then to characterCharacter = string code (ASCII code)
Text =Text +character
Col=Col+3
No
The character =="#"
Yes
Yes
Col<Height-1
No
Row=Row+3
Col=2
Yes
Row <Width-1
No
Print Text (secret message)
End

Figure (5): Flowchart for retrieving text from an image

3 Experimental Results

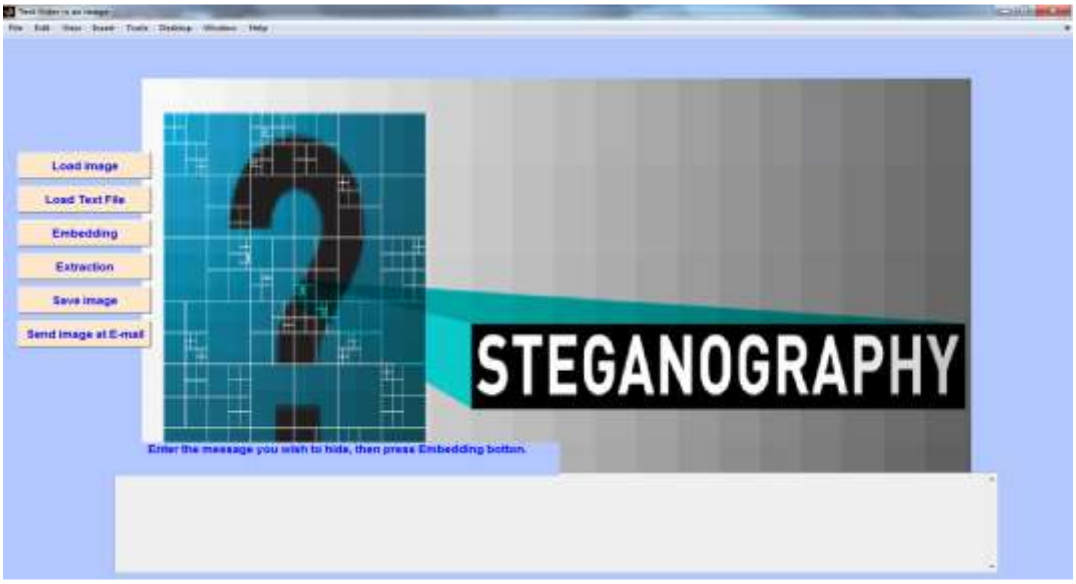
The program has been designed and implemented using Matlab program to implementing the proposed steganography algorithm, the figures (6,7,8,9,10,11,12) represented some of interfaces that have been used in system.
The system is able to hide the text files (or secret image) in images and also is able to retrieve the data back from the stego–image. When the system has been executed the menu for system login is displayed as shown in figure 6.



Enter the password, then press login botton.

Figure (6): Snapshot of Login system Menu

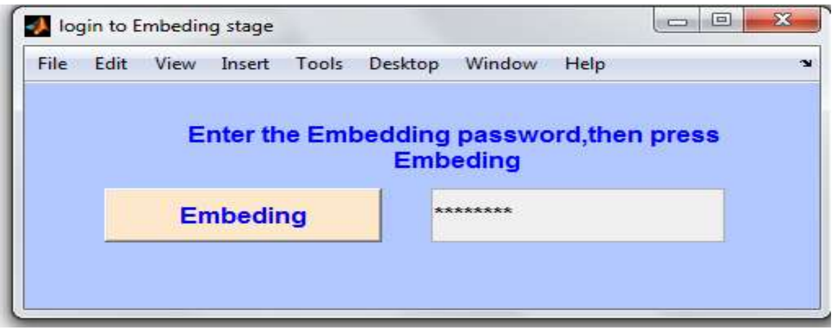
When the correct login, theinterface for steganography has been displayed asin figure 7.



Enter the message you wish to hide, then press Embedding botton.

Figure (7): Snapshot of Main Menu

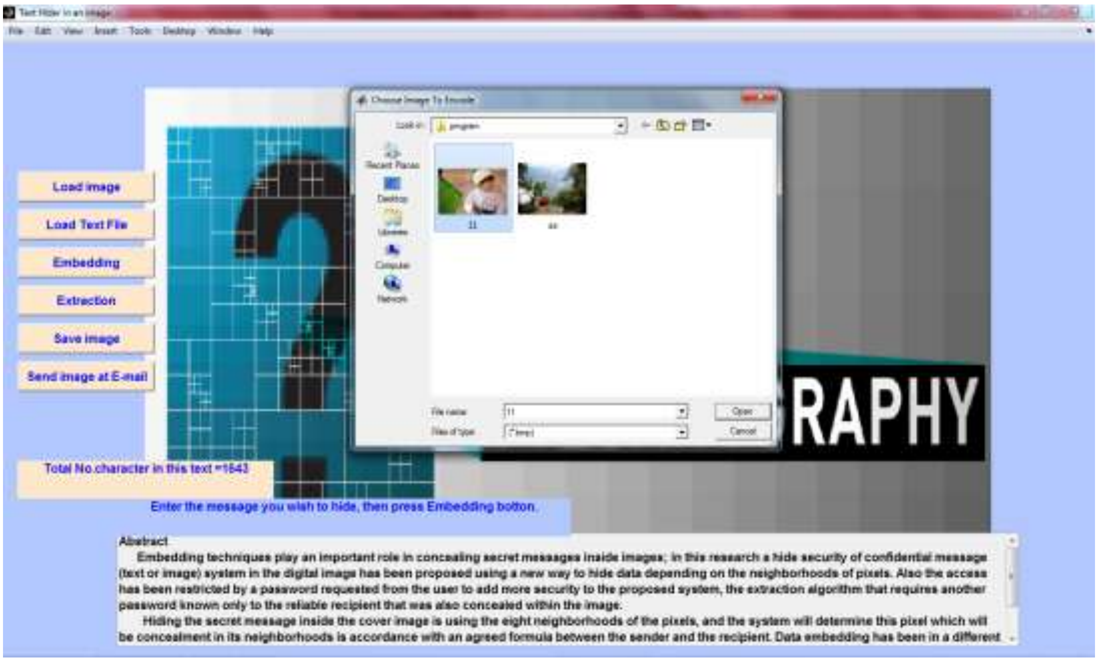
Afterthe text message has been entering in a text box and push the *embeddedbutton*,the system ask for another password as shown in figure(8),this password also has been hiding in the selected image as explained at embedding stage, figure(9) and figure (10) illustrate the embedded after hiding "the abstract of this paper"as an example in a selected cover image.



Enter the Embedding password,then press Embeding

****

Figure (8): Snapshot of Embedding Login Menu



Total No.character in this text =1643

Enter the message you wish to hide, then press Embedding botton.

Abstract

Embedding techniques play an important role in concealing secret messages inside images; in this research a hide security of confidential message (text or image) system in the digital image has been proposed using a new way to hide data depending on the neighborhoods of pixels. Also the access has been restricted by a password requested from the user to add more security to the proposed system, the extraction algorithm that requires another password known only to the reliable recipient that was also concealed within the image.

Hiding the secret message inside the cover image is using the eight neighborhoods of the pixels, and the system will determine this pixel which will be concealment in its neighborhoods is accordance with an agreed formula between the sender and the recipient. Data embedding has been in a different

Figure (9): Snapshot window of selecting cover imagefor embedding

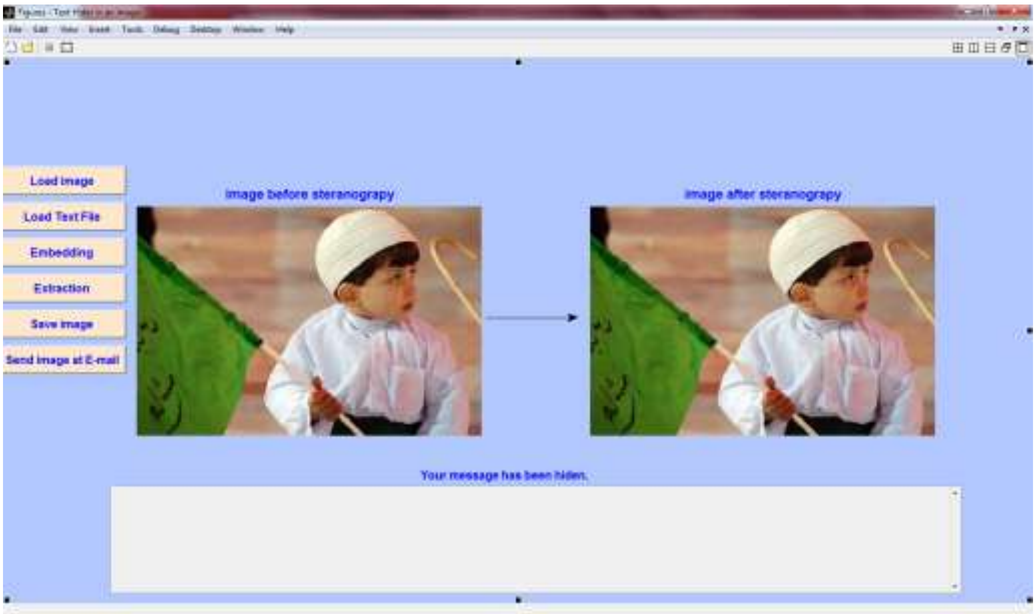
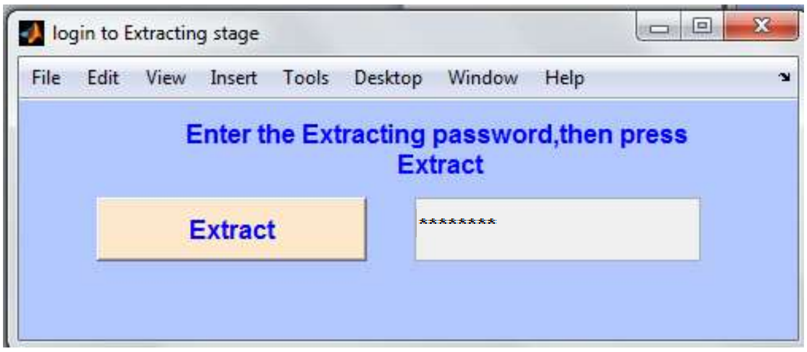


Figure - Text Hider in an image
File Edit View Insert Tools Debug Desktop Window Help
Load image
Load Text File
Embedding
Extraction
Save image
Send image at E-mail
image before steranograpy
image after steranograpy

Your message has been hiden.

Figure (10): Snapshot of Embedded Window

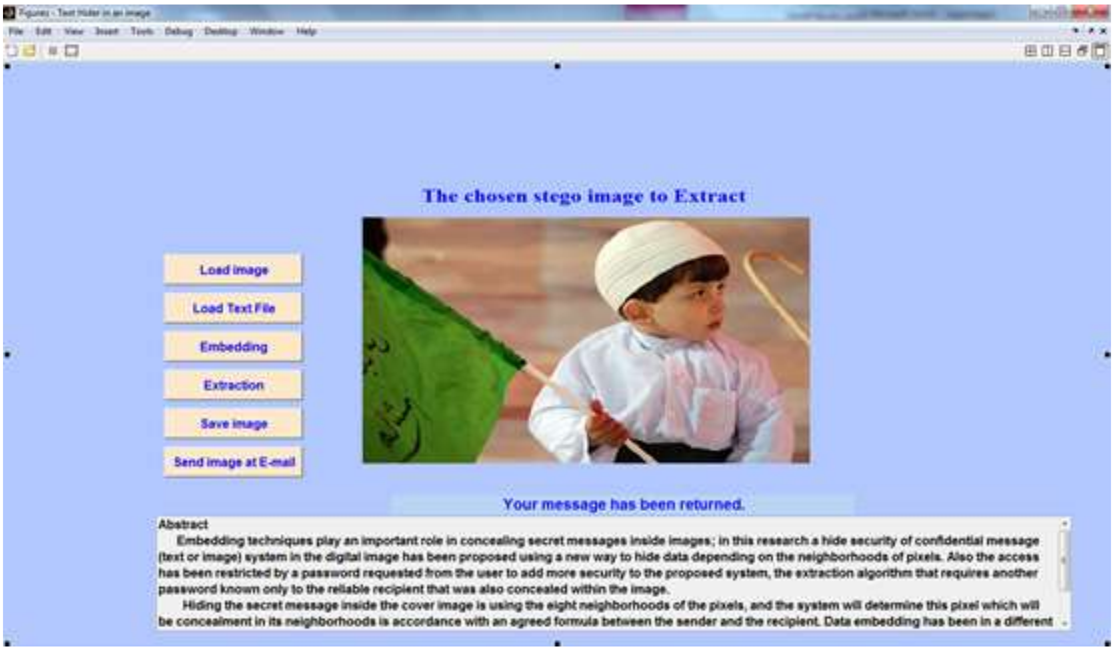
Then we can save the stego-image that now contains"the Embedding password and the secret message"and send it as an attachment by email using 'Send image at Email' button. Whenthe recipient wants to retrieve the message, he can use the same system and can easily push on button Extract then enter the correct password that has been used when embedding as shown in figure 11, thenselect the stego-image as in Figure 12that clarifies this operation for retrieving text message.


login to Extracting stage
File Edit View Insert Tools Desktop Window Help
Extract

Enter the Extracting password,then press Extract

****

Figure (11): Snapshot of Extractinglogin Menu



The chosen stego image to Extract

Your message has been returned.

Abstract

Embedding techniques play an important role in concealing secret messages inside images; in this research a hide security of confidential message (text or image) system in the digital image has been proposed using a new way to hide data depending on the neighborhoods of pixels. Also the access has been restricted by a password requested from the user to add more security to the proposed system, the extraction algorithm that requires another password known only to the reliable recipient that was also concealed within the image.

Hiding the secret message inside the cover image is using the eight neighborhoods of the pixels, and the system will determine this pixel which will be concealment in its neighborhoods is accordance with an agreed formula between the sender and the recipient. Data embedding has been in a different

Figure (12): Snapshot of Extract Window

5. Conclusion

This paper proposed a securely hiding system with a new steganographic algorithm for hiding secret message (text or image) in an imagewith exploit the Neighborhoods of the pixels.The images have been tested with different sizes of files to be hidden and concluded the following:-

1- The resulting stego-image does not have any noticeable changes and the proposed system does not affect the image resolution; we can say it is not noticeable for human eyes. To prove this we show the cover-images and the stage –images to a team of 20 persons to take their opinion ifthere is any different between the segoimage and the cover-image and their answer that there is nodifference between both images, hence this new steganographic approach is robust and very efficient for hiding in images.

2- Digital image steganography system allows a user to securely transfer a message after hiding it in an image using passwords for login system and for embedding algorithm.

Also we can encrypt the message before hiding to maximize the security and resistance against extraction by the attackers.

References

Channalli,S., Jadhav,A. (2009). "**Steganography an art of hiding data**" International Journal on Computer Science and Engineering, 1(3):137-141.

Johnson ,N.F. ,Jajodia, S.,(1998)."**Exploring steganography: Seeing the unseen**", IEEE Computer, Vol 31, No 2, 26-34.

Khare,P., Singh ,J., Tiwari ,M.,(2011) " **Steganography through digital image processing technique** "Journal Of Information, Knowledge And Research In Electronics And Communication Engineering, 1(02):137-142 .

Kumar ,S.,Singh, G., Kumar ,T., Nehra,M. S., (2013)."**Hiding the text messages of variable size using encryption and decryption algorithms in image steganography**" International Journal of Computer Applications (0975 – 8887), 61(6):47-52.

Morkel,T.,Eloff, JHP. ,Olivier, MS. (2005)."**An overview of image steganography**", proceedings of the fifth annual information security south Africa conference (ISSA2005),Sandton, south Africa .

Nag ,A., Biswas ,S., Sarkar ,D., Srkar,P. P.(2010). "**A novel technique for image steganography based on block-dct and hufman encoding**". International Journal of Computer Science and Information Technology, Vol 2, No 3, June.

Saha,B. , Sharma ,S. (2012),"S**teganographic techniques of data hiding using digital images**", Defence Science Journal,62(1):11-18.

Thampi,S. M. (2004),"I**nformation hiding techniques: a tutorial review**" ISTE-STTP on Network Security &Cryptography, LBSCE.

Wang ,H. ,Wang ,S. (2004). "**Cyber warfare: Steganography vs. Steganalysis**", Communications of the ACM, 47:10.

تصميم وتنفيذ نظام اخفاء آمن باستخدام مجاورات البكسل

وجدان رشيد عبد الحسين
كلية علوم الحاسوب والرياضيات- جامعة ذي قار

الخلاصة

تقنيات التضمين تلعب دورا مهما في اخفاء الرسائل السرية داخل الصور ، في هذا البحث تم اقتراح نظام اخفاء امن للرسالة السرية (نص او صورة) في بيانات صورة رقمية باستخدام طريقة جديدة لإخفاء البياناتاعتمادا على مجاورات البكسل، كما تم تقييد الدخول بواسطة كلمة مرور تطلب من المستخدم لإضافة امنية اكثر الى النظام

المقترح.كما ان خوارزمية الاستخراجتتطلب كلمة مرور اخرى معروفة لدى المستلم الموثوقفقط والتي تم اخفاؤها ايضا داخل الصورة.

إخفاء الرسالة السرية داخل صورة الغلاف تم باستخدام المجاورات الثمانية للبكسل ، ويقوم النظام بتحديد البكسلالذي سيتم الاخفاء في مجاوراته وفقا لصيغة متفق عليها بين المرسل والمستلم . تضمن البيانات باسلوب مختلف من بكسل لأخر اعتمادا على مواقعها في الصورة فاذا كانفي مواقع زوجية يتم التضمين باتجاه عقارب الساعة والا تضمن بعكس اتجاه عقارب الساعة اضافة الى استخدام كلمات المرور اعطى أمانا أعلى ومقاومة ضد الاستخراج من قبل المهاجمينوبذلك اثبتت الخوارزمية المقترحة للإخفاءقدرتها على تضمينواستخراج الرسائل السرية بدون أخطاء.

الكلمات المفتاحية:-اخفاء،البت الاقل اهمية ،معالجة مجاورات البكسل، صور رقمية.