IMAGE STEGANOGRAPHY

**APPLICATION DEVELOPMENT – iii**

**IMPLEMENTATION** **PHASE**

*Submitted in partial fulfilment for the award of the degree*

*of*

**Master of Technology**

***in***

**Information Technology**

*by*

**Bhuvana Chandra Pathi**

**(17MIN0618)**



**School of Information Technology and Engineering**

September 2020



**School of Information Technology and Engineering**

**DECLARATION BY THE CANDIDATE**

I hereby declare that the thesis entitled **“IMAGE STEGANOGRAPHY”** submitted by **Bhuvana Chandra (17MIN0618)** to Vellore Institute of Technology, Vellore, in partial fulfillment of the requirement for the award of the degree of **Master of Technology** in **Information Technology** is a record of bona fide APD work carried out by me. I further declare that the work reported in this project has not been submitted and will not be submitted, either in part or in full, for the award of any other degree or diploma in this institute or any other institute or university.

**Place**: Hyderabad

**Date**: 29-09-2020 **Signature of the Candidate**

Contents

[1. INTRODUCTION 5](#_Toc3488918)

[1.1 Steganography 5](#_Toc3488919)

[1.2 Steganography vs. Cryptography: 5](#_Toc3488920)

[1.3 Types of steganography 5](#_Toc3488921)

[1.3.1 Spatial domain Techniques: 5](#_Toc3488922)

[1.3.2 Transform domain techniques: 6](#_Toc3488923)

[1.4 Challenges in Steganography 7](#_Toc3488924)

[1.5 Objective of the project 7](#_Toc3488925)

[1.6 Tool Used: 7](#_Toc3488926)

[1.7 Achievements 9](#_Toc3488932)

[2. DETAILED MODULE DESCRIPTIONS 10](#_Toc3488933)

[2.1 JPEG Compression 10](#_Toc3488934)

[2.2 JPEG Steganography 15](#_Toc3488935)

[2.2.1 Jpeg-Jsteg: 16](#_Toc3488936)

[2.2.2 Steg-Hide: 18](#_Toc3488937)

[3. SAMPLE CODE 21](#_Toc3488938)

[3.1 Jpeg-Jsteg Method 21](#_Toc3488939)

[3.1.1 Encryption 21](#_Toc3488940)

[3.1.2 Decryption 25](#_Toc3488941)

[3.2 Steg-Hide Method 26](#_Toc3488942)

[3.2.1 Encryption 26](#_Toc3488943)

[3.2.2 Decryption 28](#_Toc3488944)

[4. SCREEN SHOTS 30](#_Toc3488945)

[4.1 Encryption 30](#_Toc3488946)

[4.2 Decryption 36](#_Toc3488947)

# 1. INTRODUCTION

## 1.1 Steganography

Steganography is the art of hiding information within innocuous cover carriers in ways such that the hidden message is undetectable. In Greek, „stego‟ means „covered‟ or „secret‟ and „graphy‟ means „to write‟ and therefore, steganography becomes “covered or secret writing”. The information to be hidden is embedded into the cover object which can be a text matter, some image, or some audio/video file in such a way that the very existence of the message is undetected by maintaining the appearance of the resulted object exactly same as the original. The main goal of steganography is to hide the fact that the message is present in the transmission medium.

## 1.2 Steganography vs. Cryptography:

Cryptography is the science of encrypting data in such a way that one cannot understand the encrypted message, whereas in steganography the mere existence of data is concealed, such that even its presence cannot be noticed. Using cryptography might raise some suspicion whereas in steganography the existence of secret message is invisible and thus not known. We can think of steganography as an extension of cryptography.

## 1.3 Types of steganography

On the basis of cover object steganography may be of many types like Audio Steganography, Video Steganography, image Steganography etc. Image Steganography is very popular because of popularity of digital image transmission over the internet. Image Steganography use redundancy of digital image to hide the secret data. It may be divided into two categories. They are spatial-domain methods and frequency-domain ones. In the spatial domain, the secret messages are embedded in the image pixels directly. In the frequency-domain, however, the secret image is first transformed to frequency-domain, and then the messages are embedded in the transformed.

### 1.3.1 Spatial domain Techniques:

**Least Significant Bit (LSB) substitution**- LSB substitution method, which uses fixed k LSBs in each pixel to embed secret message, is the easiest method to hide message in an image. However, it is easy to reveal a stego-image produced by the LSB insertion method.

**Distortion technique**- In distortion technique some pixel property of cover image is changed according to secret message and then deflection of distorted from original image contains secret information.

### 1.3.2 Transform domain techniques:

If we embed information in spatial domain, it may be subjected to the losses if the image undergoes any image processing technique like compression, cropping etc. To overcome this problem we embed the information in frequency domain such that the secret information is embedded on the significant frequency values while higher frequency part is omitted. We first apply transformations to the image then data is to be hidden by changing the values of the transformation coefficients accordingly.

There are mainly three transformation techniques:

**Fast Fourier Transform (FFT) Steganography**- In this technique two dimensional FFT is used to convert the cover image into transform domain first and then secret bits are embedded on the significant coefficients. FFT includes complex term also, hence it computes more mathematical computations and time complexity is higher than DCT steganography.

**Discrete Cosine Transform (DCT) Steganography**- In this technique two dimensional DCT is used for transformation of cover image. DCT is derived from the FFT, however it requires fewer multiplications than the FFT since it works only with real numbers. Also, the DCT produces fewer significant coefficients in its result, which leads to greater compression. Hence DCT is the popular technique in the field of steganography.

If after DCT transformation, quantization step is also taken as in Joint Photographic Experts Group (JPEG) compression then it becomes robust to JPEG compression and this technique is called as JPEG steganography.

**Discrete Wavelet Transform (DWT) Steganography**- In this technique DWT is used to separate high frequency components from low frequency components and then replacing the high frequency part by secret data. The embedding capacity of this technique is far greater than DCT steganography.

## 1.4 Challenges in Steganography

The major challenges of effective steganography are:-

**Security of Hidden Communication**: In order to avoid raising the suspicions of eavesdroppers, while evading the meticulous screening of algorithmic detection, the hidden contents must be invisible both perceptually and statistically. Steganography techniques should produce high imperceptible Stego-image.

**Size of Payload:** Unlike watermarking, which needs to embed only a small amount of copyright information, steganography aims at hidden communication and therefore usually requires sufficient embedding capacity. Requirements for higher payload and secure communication are often contradictory. Depending on the specific application scenarios, a tradeoff has to be sought.

**Robustness**: Stego-image should provide robustness to image processing techniques like compression, cropping, resizing etc. i.e. when any of these techniques are performed on stego-image, secret information should not be destroyed completely.

## 1.5 Objective of the project

In this project my task is to implement 2 techniques of spatial domain steganography(LSB substitution) and 2 techniques of JPEG steganography (Jsteg and Steghide) taking secret information as a data file and as an image and to do comparisons between them in terms of embedding capacity and quality of produced stego-image and robustness to attacks.

## 1.6 Tool Used:

MATLAB is used as simulator to implement the techniques of steganography. MATLAB provides highly computing environment and advanced in-built function for image processing.

## 1.7 Achievements

The aim of this project work was to implement various spatial and transform domain steganographic techniques. The following achievements or we can say objectives were achieved as follows:

|  |  |
| --- | --- |
|  | Spatial domain techniques are easy ways to embed information, but they are highly vulnerable to even small cover modifications. |

|  |  |
| --- | --- |
|  | The embedding capacity of Jpeg steganography is very less than spatial domain  techniques. |

|  |  |
| --- | --- |
|  | The spatial domain techniques provide high PSNR, high perceptual quality and high embedding capacity but these not provide robustness. |

|  |  |
| --- | --- |
|  | Transform domain provide robustness while providing very less embedding capacity, low PSNR and low perceptual quality**.** |

# 2. DETAILED MODULE DESCRIPTIONS

In the project JPEG steganography is implemented which use Discrete Cosine Transform to convert image into frequency domain. Before discussing these techniques in detail we first discuss the JPEG compression because JPEG steganography is just the modified version of JPEG compression.

## 2.1 JPEG Compression

The Joint Photographic Experts Group developed the JPEG algorithm in the late 1980‟s and early 1990‟s. to address the problems of that era, specifically the fact that consumer-level computers had enough processing power to manipulate and display full color photographs. However, full color photographs required a tremendous amount of bandwidth when transferred over a network connection and required just as much space to store a local copy of the image. Other compression techniques had major tradeoffs. They had either very low amounts of compression, or major data loss in the image. Thus, the JPEG algorithm was created to compress photographs with minimal data loss and high compression ratios.

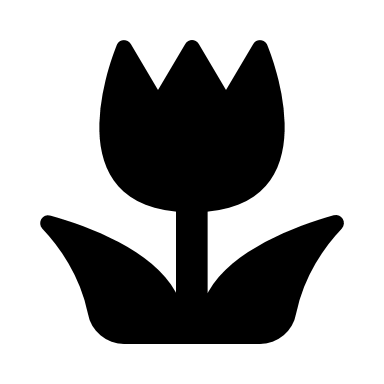
JPEG compression and decompression consist of 4 distinct and independent phases. First, the image is divided into 8 x 8- pixel blocks. Next, a discrete cosine transform is applied to each block to convert the information from the spatial domain to the frequency domain. After that, the frequency information is quantized to remove unnecessary information. Finally, standard compression techniques compress the final bit stream. The basic flow of JPEG is as below:

***JPEG Compression Interface***

DCT

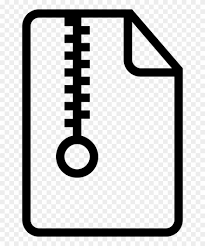
Quantizer

Huffman Coder



Quantization Table

Table



**Source Image**

**8 X 8 Blocks**

**Compressed Image**

Phase One: Divide the Image

Attempting to compress an entire image would not yield optimal results. Therefore, JPEG divides the image into matrices of 8 x 8 pixel blocks. If the image dimensions are not multiples of 8, extra pixels are added to the bottom and right part of the image to pad it to the next multiple of 8 so that we create only full blocks. The dummy values are easily removed during decompression. From this point on, each block of 64 pixels is processed separately from the others, except during a small part of the final compression step.

It may optionally include a change in colorspace. Normally, JPEG will convert RGB colorspace to YCbCr colorspace. In YCbCr, Y is the luminance, which represents the intensity of the color. Cb and Cr are chrominance values, and they actually describe the color itself. YCbCr tends to compress more tightly than RGB.

Phase Two: Conversion to the Frequency Domain

In JPEG all 8 x 8 blocks are converted to frequency domain using DCT. The Discrete Cosine Transform (DCT) is derived from the FFT, however it requires fewer multiplications than the FFT since it works only with real numbers. Also, the DCT produces fewer significant coefficients in its result, which leads to greater compression. That is why DCT is used for transformation purpose. The 2D discrete cosine transform equation is given below

where f (x, y) is the 8-bit image value at coordinates (x, y) and F (u, v) is the new entry in the frequency matrix. Also, C(x) = 1/√ 2 if x is 0, and C(x) = 1 for all other cases.

The frequency domain matrix contains values from -1024…1023. The upper-left entry, also known as the DC value, is the average of the entire block, and is the lowest frequency cosine coefficient. As we move right the coefficients represent cosine functions in the vertical direction that increase in frequency. Likewise, as we move down, the coefficients belong to increasing frequency cosine functions in the horizontal direction. The highest frequency values occur at the lower-right part of the matrix. The higher frequency values also have a natural tendency to be significantly smaller than the low frequency coefficients since they contribute much less to the image. Typically, the entire lower-right half of the matrix is factored out after quantization. This essentially removes half of the data per block, which is one reason why JPEG is so efficient at compression. Computing the DCT is the most time-consuming part of JPEG compression. Thus, it determines the worst-case running time of the algorithm.

Phase Three: Quantization

Having the data in the frequency domain allows the algorithm to discard the least significant parts of the image. The JPEG algorithm does this by dividing each cosine coefficient in the data matrix by some predetermined constant, and then rounding up or down to the closest integer value. These predefined constants are then entered into another 8 x 8 matrix, called the „quantization matrix‟. Each entry in the quantization matrix corresponds to exactly one entry in the frequency matrix. A typical quantization matrix will be symmetrical about the diagonal and will have lower values in the upper left and higher values in the lower right. Since any arbitrary values could be used during quantization, the entire quantization matrix is stored in the final JPEG file so that the decompression routine will know the values that were used to divide each coefficient. The constant values that are used in the division may be arbitrary, although research has determined some very good typical values. The standard quantization matrix used in JPEG is as below:

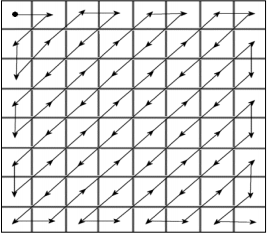
Dividing by a high constant value can introduce more error in the rounding process, but high constant values have another effect. As the constant gets larger the result of the division approaches zero. This is especially true for the high frequency coefficients, since they tend to be the smallest values in the matrix. Thus, many of the frequency values become zero. Phase four takes advantage of this fact to further compress the data.

The algorithm used to calculate the quantized frequency matrix is fairly simple. It takes a value from the frequency matrix (F) and divides it by its corresponding value in the quantization matrix (Q). This gives the final value for the location in the quantized frequency matrix (Fquantize). The quantization equation that is used for each block in the image is below:

By adding 0.5 to each value, we essentially round it off automatically when we truncate it, without performing any comparisons.

Phase Four: Entropy Coding:

After quantization, the algorithm is left with blocks of 64 values, many of which are zero. Of course, the best way to compress this type of data would be to collect all the zero values together, which is exactly what JPEG does. The algorithm uses a zigzag ordered encoding, which collects the high frequency quantized values into long strings of zeros. To perform a zigzag encoding on a block, the algorithm starts at the DC value and begins winding its way down the matrix, as shown in figure. This converts an 8 x 8 table into a 1 x 64 vector



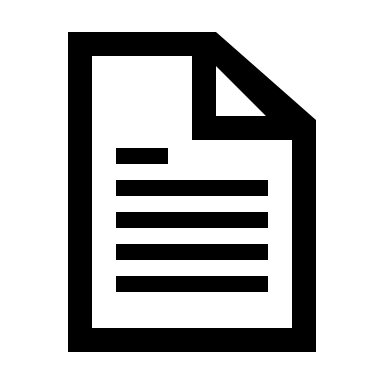
*Zig-Zag Ordered Encoding*

All of the values in each block are encoded in this zigzag order except for the DC value. For all of the other values, there are two tokens that are used to represent the values in the final file. The first token is a combination of {size, skip} values. The size value is the number of bits needed to represent the second token, while the skip value is the number of zeros that precede this token. The second token is simply the quantized frequency value, with no special encoding. At the end of each block, the algorithm places an end- of-block sentinel so that the decoder can tell where one block ends and the next begins.

The first token, with {size, skip} information, is encoded using Huffman coding. Huffman coding scans the data being written and assigns fewer bits to frequently occurring data, and more bits to infrequently occurring data. Thus, if a certain value of size and skip happen often, they may be represented with only a couple of bits each. There will then be a lookup table that converts the two bits to their entire value. JPEG allows the algorithm to use a standard Huffman table, and also allows for custom tables by providing a field in the file that will hold the Huffman table. DC values use delta encoding, which means that each DC value is compared to the previous value, in zigzag order. This is the only instance where blocks are not treated independently from each other. The difference between the current DC value and the previous value is all that is included in the file.

## 2.2 JPEG Steganography

JPEG steganography is more important and popular because stago-image produce by these techniques are robust to jpeg compression. In this technique secret data is embed after quantization phase of JPEG compression. Only significant quantized DCT coefficients are modified according to secret bits. Remaining steps are similar to JPEG compression. In this way stego-image is produced in .jpg format directly. The basic flow diagram of embedding and extraction process is as below:



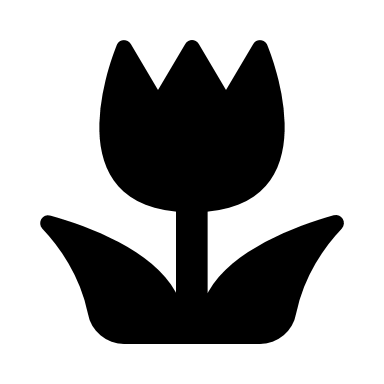
Quantization Table

8 X 8 Block DCT

Quantizer

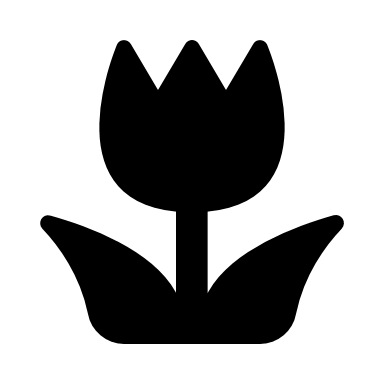
Embedding

Entropy Coding



Secret message into bit stream conversion

Secret Message



Stego Image

Cover Image

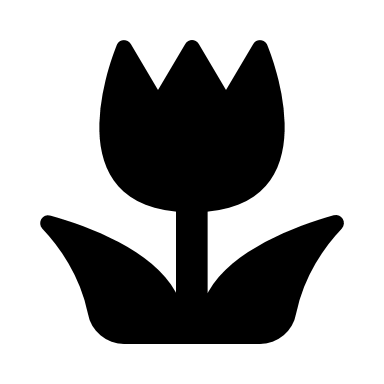
*Block diagram of Embedding process of JPEG Steganography*

8 X 8 Block DCT

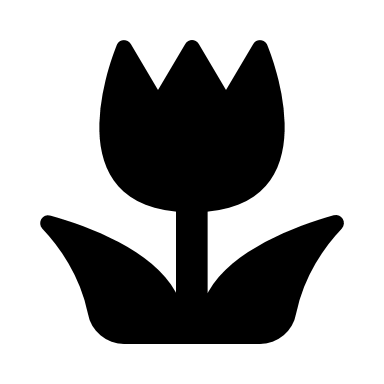
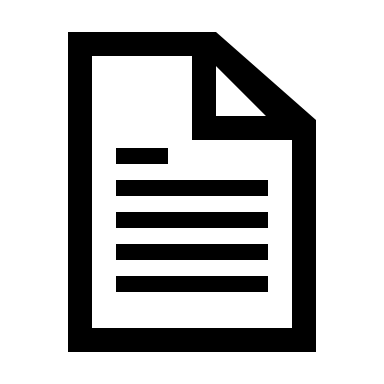
Quantizer

Embedding

Entropy Coding



Secret message in bit stream



Quantization Table

Secret Message

Distorted Cover Image

Stego Image

*Block diagram of Extraction process of JPEG Steganography*

Following are some JPEG steganography techniques:

1. Jsteg 2) Outguess 3) Steghide 4) F3,F4,F5 5) J3

In the project only 2 techniques Jsteg and Steghide is implemented and these are explained below with algorithms.

### 2.2.1 Jpeg-Jsteg:

In Jpeg–Jsteg, the secret messages are embedded in LSB of quantized DCT coefficients whose values are not (0, 1, or 1). Its execution steps are described briefly as follows. First, JPEG partitions a cover-image into non-overlapping blocks of 8\*8 pixels, and then it uses DCT to transform each block into DCT coefficients. The results of the DCT coefficients are scaled according to a quantization table.

The standard quantization table is listed in Fig., which is a matrix that contains 64 coefficients. Next, Jpeg–Jsteg uses an encryption algorithm to protect the message. A message after encrypting is called secret message S={s1, s2, s3, s4, . . .,sn }, where si is a secret bit. After the above steps, Jpeg–Jsteg embeds si into LSB of quantize DCT coefficients whose values are not 0, 1, or 1. The bit-flip diagram of J-steg is as below:

JPEG Coefficients

in cover image -4 -3 -2 -1 0 0 1 2 3 4

0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1

JPEG coefficients

in Stego-image

*Bit-flip in JPEG-JSTEG*

The embedding sequence employed in Jpeg–Jsteg is in the zigzag scan order, which is listed in fig. After embedding the secret message in each block, Jpeg–Jsteg uses Huffman coding, Run-Length coding, and DPCM of JPEG entropy coding to compress each block. Finally, Jpeg–Jsteg obtains a JPEG stego-image. The message capacity of Jpeg–Jsteg is limited. If there are many quantifized coefficients equal to 0, 1, or 1, then the message capacity of Jpeg–Jsteg will be decreased. Besides, in DCT transformation, most important coefficients are located around the low-frequency part. Jpeg– Jsteg modifies the quantized DCT coefficients right in the low-frequency part. Therefore, the image quality of Jpeg–Jsteg is degraded, especially when the cover-image undergoes a high compression ratio.

Embedding Algorithm:

Input: secret message, cover image

Procedure:

**Step1:** Convert the secret message into bit stream

**Step2:** Divide the cover image into 8x8 blocks

**Step3:** Calculate DCT coefficients for each block

**Step4:** Quantize the coefficients

**Step5:** while complete message not embedded do

{get next DCT coefficient

if DCT ≠ 0, DCT ≠1 and DCT ≠ -1 then

{get next bit from message

replace DCT LSB with message bit}

}

**Step6:** De-quantize and take inverse DCT to obtain stego-image. End.

Output: Stego- image

Extracting Algorithm:

Input: Stego image

Procedure:

**Step1:** Divide the stego image into 8x8 blocks

**Step2:** Calculate DCT coefficients for each block

**Step3:** Quantize the coefficients

**Step4:** While secret message not completed do

{ Get next DCT coefficient

If DCT ≠ 0 , DCT ≠1and DCT ≠ -1 then

{ Concatenate DCT LSB to secret message bit steam } }

**Step5:** Convert secret message bit stream into the message. End.

Output: Secret message

***Advantage:***

* Robust to JPEG compression.
* Less bandwidth requirement for stego image transmission because its size can be reduced.

***Disadvantage:***

* Only few secret messages can be embedded in cover image.
* High detectability due to the fact that it introduces characteristic artifacts into the first order statistics (histogram) of DCT coefficients.

### 2.2.2 Steg-Hide:

Steghide uses a graph-theoretic approach to steganography. Steghide embeds by swapping DCT coefficients and thus avoids changing the histogram. The fact that the embedding is done by exchanging pixel values implies that the first-order statistics (i.e. the number of times a colour occurs in the picture) is not changed. During the encoding process, the sender splits the cover image in 8 x 8-pixel blocks; each block encodes exactly one secret message bit. The embedding process starts with selecting a pseudorandom block bi which will be used to code the ith message bit. Before the communication starts, both sender and receiver have to agree on the location of two DCT coefficients, which will be used in the embedding process; let us denote these two indices by (u1,v1) and (u2, v2). The two coefficients should correspond to cosine functions with middle frequencies; this ensures that the information is stored in significant parts of the signal (hence the embedded information will not be completely damaged by JPEG compression).

Embedding Algorithm:

Input: secret message, cover image

Procedure:

**Step1:** Convert the secret message into bit stream

**Step2:** Divide the cover image into 8x8blocks

**Step3:** Calculate DCT coefficients for each block

**Step4:** Quantize the coefficients

**Step5:** While complete message not embedded do

{ Get next block

If block(u1,v1) ≠ block(u2,v2)

then { get next bit from message stream

if bit =1 and block(u1,v1)< block(u2,v2)

{ swap(block(u1,v1),block(u2,v2) }

If bit =0 and block(u1,v1)> block(u2,v2)

{ swap(block(u1,v1),block(u2,v2) } } }

**Step6:** De-quantize and take inverse DCT to obtain stego-image End.

Output: Stego- image

Extracting Algorithm:

Input: Stego image

Procedure:

**Step1:** Divide the stego image into 8x8 blocks

**Step2:** Calculate DCT coefficients for each block

**Step3:** Quantize the coefficients

**Step4:** While secret message not completed do

{ Get next block

If block(u1,v1) ≠ block(u2,v2)

then { If block(u1,v1)< block(u2,v2)

{ concatenate 0 to bit stream Else Concatenate 0 to bit stream } }

}

**Step5:** Convert secret message bit stream into the message. End.

Output: Secret message

***Advantage:***

* It cannot be detected by steganalysis which uses first order characteristics, because histogram is preserved.
* It provides Robustness to JPEG compression.

***Disadvantage:***

* Its embedding capacity is less than Jsteg too.
* Cover size in which message embedded is always multiple of 8 which can be used to detect the presence of secret message.

# 3. SAMPLE CODE

## 3.1 Jpeg-Jsteg Method

### 3.1.1 Encryption

clear all;% clear all variables from previous sessions

close all;

covername = input('Enter image file name with extension: ', 's');

messagename = input('Enter message image file name with extension: ', 's');

cover = imread(covername);

sz = size(cover);

rows = sz(1,1);

cols = sz(1,2);

colors = max(max(cover));

%r=1;

%for i=1:rows

% for j=1:3:cols

% rgb(r,1)=cover(i,j);

% rgb(r,2)=cover(i,j+1);

% rgb(r,3)=cover(i,j+2);

% r=r+1;

% end

%end

%gray=rgb2gray(rgb);

%cover=gray;

fd = fopen (messagename, 'r');

message = fgetl(fd);

messagelength = length(message);

figure(1), imshow(cover); title('Original Image (Cover Image)');

%disp(message);

%cover=double(cover);

%message=double(message);

message = uint8(message);

coverzero = cover;

%disp(coverzero);

%coverzero=imread('GrayScale.bmp');

quant\_multiple = 1;

blocksize = 8;

DCT\_quantizer = ...

[ 16 11 10 16 24 40 51 61; ...

12 12 14 19 26 58 60 55; ...

14 13 16 24 40 57 69 56; ...

14 17 22 29 51 87 80 62; ...

18 22 37 56 68 109 103 77; ...

24 35 55 64 81 104 113 92; ...

49 64 78 87 103 121 120 101; ...

72 92 95 98 112 100 103 99 ];

%figure(1)

%image(coverzero)

figure(2);imshow(coverzero);

%colormap(map)

title('Original image');

%figure(2)

%coverzero = coverzero - ceil(colors/2);

%figure(2);imshow(coverzero);

pad\_cols = (1 - (cols/blocksize - floor(cols/blocksize))) \* blocksize;

if pad\_cols == blocksize, pad\_cols = 0; end

pad\_rows = (1 - (rows/blocksize - floor(rows/blocksize))) \* blocksize;

if pad\_rows == blocksize, pad\_rows = 0; end

for extra\_cols = 1:pad\_cols

coverzero(1:rows, cols+extra\_cols) = coverzero(1:rows, cols);

end

cols = cols + pad\_cols; % coverzero is now pad\_cols wider

for extra\_rows = 1:pad\_rows

coverzero(rows+extra\_rows, 1:cols) = coverzero(rows, 1:cols);

end

rows = rows + pad\_rows; % coverzero is now pad\_rows taller

for row = 1: blocksize: rows

for col = 1: blocksize: cols

DCT\_matrix = coverzero(row: row + blocksize-1, col: col + blocksize-1);

DCT\_matrix = DCT2(DCT\_matrix);

% quantize it (levels stored in DCT\_quantizer matrix):

%DCT\_matrix = floor (DCT\_matrix ...

% ./ (DCT\_quantizer(1:blocksize, 1:blocksize) \* quant\_multiple) + 0.5);

DCT\_matrix = round(DCT\_matrix ...

./ (DCT\_quantizer(1:blocksize, 1:blocksize) \* quant\_multiple));

%DCT\_matrix=round(DCT\_matrix);

% place it into the compressed-image matrix:

jpeg\_img(row: row + blocksize-1, col: col + blocksize-1) = DCT\_matrix;

end

end

figure(3);hist(jpeg\_img);

figure(4);imshow(jpeg\_img);

bitlength=1;

%messagebit=zeros(messagelength\*8);

for i=1:messagelength

%imbed=7;

for imbed=1:8

messageshift=bitshift(message(i),8-imbed);

showmess=uint8(messageshift);

showmess=bitshift(showmess,-7);

messagebit(bitlength)=showmess;

bitlength=bitlength+1;

%coverindex = coverindex+1;

end

end

%embedding

i=1;

for row=1:rows

for col=1:cols

x=jpeg\_img(row,col);

if (x~=0) && (x~=1)

r=mod(x,2);

if r==0 %

if messagebit(i)==1

x=x+1;

end

else

if messagebit(i)==0

x=x-1;

end

end

i=i+1;

end

jpeg\_img(row,col)=x;

if i==bitlength

break;

end

end

if i==bitlength

break;

end

end

figure(5);hist(jpeg\_img);

% Reconstructing image

recon\_img = coverzero - coverzero; % zero the matrix for the reconstructed image

for row = 1: blocksize: rows

for col = 1: blocksize: cols

IDCT\_matrix = jpeg\_img(row: row + blocksize-1, col: col + blocksize-1);

%IDCT\_matrix = floor(idct2(IDCT\_matrix .\* ((DCT\_quantizer(1:blocksize, 1:blocksize) \* quant\_multiple))-0.5));

%IDCT\_matrix = floor(idct2(IDCT\_matrix .\* (DCT\_quantizer(1:blocksize, 1:blocksize) \* quant\_multiple)));

IDCT\_matrix = round(idct2(IDCT\_matrix .\* (DCT\_quantizer(1:blocksize, 1:blocksize) \* quant\_multiple)));

recon\_img(row: row + blocksize-1, col: col + blocksize-1) = IDCT\_matrix;

end

end

%recon\_img = recon\_img + ceil(colors/2);

%coverzero = coverzero + ceil(colors/2);

% Clip off padded rows and columns

rows = rows - pad\_rows;

cols = cols - pad\_cols;

recon\_img = recon\_img(1:rows, 1:cols);

figure(6);imshow(recon\_img);

%disp(recon\_img);

%recon\_img = recon\_img - ceil(colors/2);

pad\_cols = (1 - (cols/blocksize - floor(cols/blocksize))) \* blocksize;

if pad\_cols == blocksize, pad\_cols = 0; end

pad\_rows = (1 - (rows/blocksize - floor(rows/blocksize))) \* blocksize;

if pad\_rows == blocksize, pad\_rows = 0; end

for extra\_cols = 1:pad\_cols

recon\_img(1:rows, cols+extra\_cols) = recon\_img(1:rows, cols);

end

cols = cols + pad\_cols; % coverzero is now pad\_cols wider

for extra\_rows = 1:pad\_rows

recon\_img(rows+extra\_rows, 1:cols) = recon\_img(rows, 1:cols);

end

rows = rows + pad\_rows; % coverzero is now pad\_rows taller

jpeg\_img=jpeg\_img-jpeg\_img;

for row = 1: blocksize: rows

for col = 1: blocksize: cols

DCT\_matrix = recon\_img(row: row + blocksize-1, col: col + blocksize-1);

DCT\_matrix = DCT2(DCT\_matrix);

% quantize it (levels stored in DCT\_quantizer matrix):

%DCT\_matrix = floor (DCT\_matrix ...

% ./ (DCT\_quantizer(1:blocksize, 1:blocksize) \* quant\_multiple) + 0.5);

DCT\_matrix = round (DCT\_matrix ...

./ (DCT\_quantizer(1:blocksize, 1:blocksize) \* quant\_multiple));

%DCT\_matrix=round(DCT\_matrix);

% place it into the compressed-image matrix:

jpeg\_img(row: row + blocksize-1, col: col + blocksize-1) = DCT\_matrix;

%disp(jpeg\_img(row: row + blocksize-1, col: col + blocksize-1));

end

end

stego=jpeg\_img;

%stego = uint8(jpeg\_img);

%stego = int8(jpeg\_img);

%disp(stego(1:8,1:8));

### 3.1.2 Decryption

%stego = uint8(jpeg\_img);

%disp(stego(1:8,1:8));

stegoindex=1;

imbed=1;

messagechar=0;

messageindex=1;

%for i=1:(messagelength\*8)

for row=1:rows

for col=1:cols

stegomessage = stego(row,col);

if (stegomessage~=0)&&(stegomessage~=1)

r=mod(stegomessage,2);

if (r==0)

showmess=0;

else showmess=1;

end

showmess=uint8(showmess);

%showmess=bitshift(stegomessage,7);

showmess=bitshift(showmess,(imbed-1));

messagechar=uint8(messagechar+showmess);

stegoindex = stegoindex+1;

imbed=imbed+1;

if (imbed==9)

messagestring(messageindex)=messagechar;

messageindex=messageindex+1;

messagechar=0;

imbed=1;

end

end

if (stegoindex==messagelength\*8)

break;

end

end

if (stegoindex==messagelength\*8)

break;

end

end

%end

disp(messagestring);

## 3.2 Steg-Hide Method

### 3.2.1 Encryption

clear all;

[dir\_input, dir\_output, dir\_results] = steganography\_init();

carrier\_image\_filename = 'peppers.jpg';

output\_image\_filename = 'stegoimage\_egypt.jpg';

%@@ Message string to encode into carrier image

secret\_msg\_str = '';

use\_greyscale = true;

channel = 3;

iteration\_total = 101;

% Name of folder to store test results in

if use\_greyscale

test\_name = ['Egypt\_', carrier\_image\_filename, '\_grey'];

else

test\_name = ['Egypt\_', carrier\_image\_filename];

end

% Create directory for results if running iteration test

if iteration\_total > 1

[dir\_results\_full, ~] = create\_directory\_unique([dir\_results, test\_name]);

iteration\_data = zeros(7, iteration\_total);

output\_csv\_filename = [dir\_results\_full, test\_name, '\_results.csv'];

end

for iteration\_current = 1:iteration\_total

secret\_msg\_w = 96;

secret\_msg\_h = 96;

%@@ Output image quality

if iteration\_total == 1

output\_quality = 100;

else

% If performing a test, try all qualities from 100 to 0

output\_quality = 100 - (iteration\_current - 1);

end

%@@ Wavelet transformation

%@@ [Default: 'idk' or sometimes 'haar']

mode = 'idk';

%@@ Block size: Size in pixels of the blocks that the secret binary image

%@@ is split up into. Generally, smaller values lead to more accuracy and

%@@ robustness, but slower calculation and larger keys.

%@@ [Default: usually between 1 and 32]

block\_size = 4;

%@@ Square size: When converting the secret message into a binary image,

%@@ this controls the size in pixels of the squares used to represent each

%@@ bit. Generally, larger values lead to more robustness, but less

%@@ capacity.

%@@ [Default: 1 to 16]

square\_size = 3;

% Set to true, because we are encoding secret binary data, not an image

is\_binary = true;

% Load images

im = imload([dir\_input, carrier\_image\_filename], use\_greyscale);

[im\_carrier\_w im\_carrier\_h ~] = size(im);

if isempty(secret\_msg\_str)

secret\_msg\_str = generate\_test\_message(((secret\_msg\_w / square\_size) \* (secret\_msg\_h / square\_size)) / 8);

end;

secret\_msg\_bin = str2bin(secret\_msg\_str);

if use\_hamming

% Hamming encode

secret\_msg\_bin\_raw = zeros(1, length(secret\_msg\_bin));

secret\_msg\_bin = secret\_msg\_bin(1:length(secret\_msg\_bin)/2);

secret\_msg\_bin\_hamming = hamming\_encode\_chunk(secret\_msg\_bin);

secret\_msg\_bin\_raw(1:length(secret\_msg\_bin\_hamming)) = secret\_msg\_bin\_hamming;

else

secret\_msg\_bin\_raw = secret\_msg\_bin;

end

if use\_greyscale

imc = im;

else

imc = im(:,:,channel);

end

tic;

% Convert binary data to image

im\_secret = bin2binimg(secret\_msg\_bin\_raw, secret\_msg\_w / square\_size, secret\_msg\_h / square\_size, square\_size, 255);

[imc\_stego, key1, key2, im\_wavelet\_stego, im\_wavelet\_secret] = steg\_egypt\_encode(imc, im\_secret, mode, block\_size, is\_binary);

encode\_time = toc;

if use\_greyscale

im\_stego = imc\_stego;

else

im\_stego = im;

im\_stego(:,:,channel) = imc\_stego;

end

% Write stego image to file

imwrite(uint8(im\_stego), [dir\_output, output\_image\_filename], 'Quality', output\_quality);

### 3..1 Decryption

im\_stego = imload([dir\_output, output\_image\_filename], use\_greyscale);

% Perform Egypt decoding

if use\_greyscale

imc\_stego = im\_stego;

else

imc\_stego = im\_stego(:,:,channel);

end

tic;

[im\_extracted, im\_errors] = steg\_egypt\_decode(imc\_stego, secret\_msg\_w, secret\_msg\_h, key1, key2, mode, block\_size, is\_binary);

% Extract the binary data from the extracted image

extracted\_msg\_bin\_raw = binimg2bin(im\_extracted, square\_size, 127);

if use\_hamming

% Hamming decode

extracted\_msg\_bin = hamming\_decode\_chunk(extracted\_msg\_bin\_raw);

else

extracted\_msg\_bin = extracted\_msg\_bin\_raw;

end

decode\_time = toc;

% Take the raw extracted image, and make the values either 0 or 255

im\_extracted\_bin = im\_extracted;

im\_extracted\_bin(im\_extracted\_bin < 127) = 0;

im\_extracted\_bin(im\_extracted\_bin >= 127) = 255;

% Calculate min & max values to ensure wavelet based images use same scale

wmin = min(min(min(min(im\_wavelet\_secret)), min(min(im\_wavelet\_stego))), min(min(im\_errors)));

wmax = max(max(max(max(im\_wavelet\_secret)), max(max(im\_wavelet\_stego))), max(max(im\_errors)));

% Output results

subplot(2,3,1);

imshow(im\_wavelet\_secret, [wmin wmax]);

title('Secret image (wavelet transformed)');

subplot(2,3,4);

imshow(im\_wavelet\_stego, [wmin wmax]);

title('Stego image (wavelet transformed)');

subplot(2,3,2);

imshow(uint8(im\_stego), [0 255]);

title('Stego image');

subplot(2,3,5);

imshow(im\_errors, [wmin wmax]);

title('Error blocks');

subplot(2,3,3);

imshow(im\_secret, [0 255]);

title('Secret image - before');

subplot(2,3,6);

imshow(im\_extracted\_bin, [0 255]);

title('Secret image - after');

% Print statistics

[length\_bytes, msg\_similarity\_py, msg\_similarity, im\_psnr] = steganography\_statistics(imc, imc\_stego, secret\_msg\_bin, extracted\_msg\_bin, encode\_time, decode\_time);

% Log data if running multiple tests

if iteration\_total > 1

iteration\_data(((iteration\_current - 1) \* 7) + 1:((iteration\_current - 1) \* 7) + 1 + 6) = [output\_quality, msg\_similarity\_py \* 100, msg\_similarity \* 100, im\_psnr, encode\_time, decode\_time, length\_bytes];

imwrite(uint8(im\_stego), sprintf('%s%d.jpg', dir\_results\_full, output\_quality));

end

end

% Save data log to file

if iteration\_total > 1

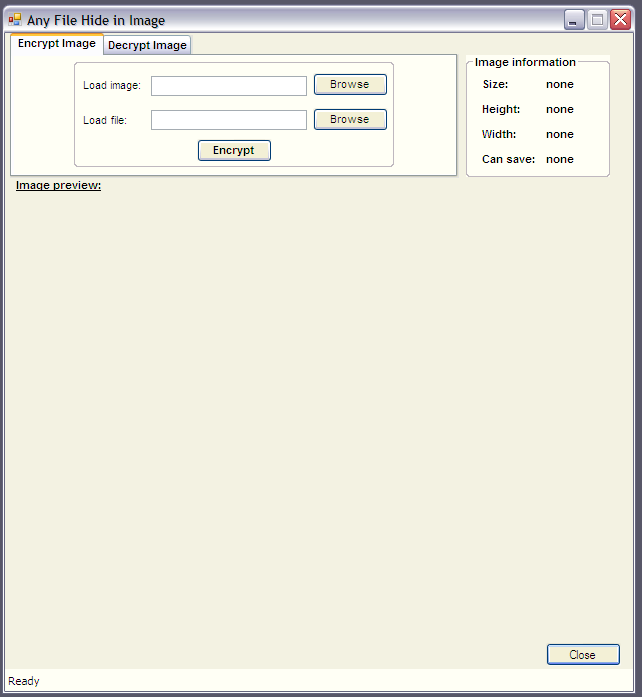
test\_data\_save(output\_csv\_filename, iteration\_data');

fprintf('Saved results at: %s\n', output\_csv\_filename);

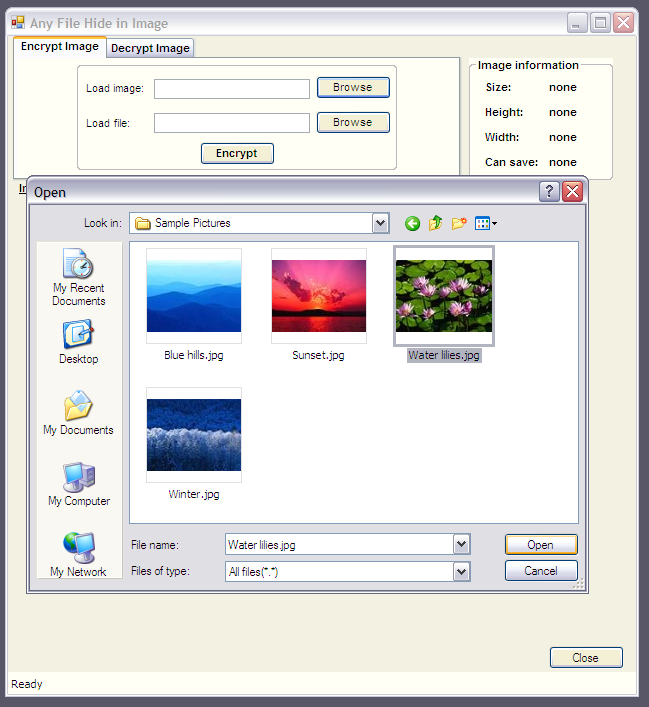
end

# 4. SCREEN SHOTS

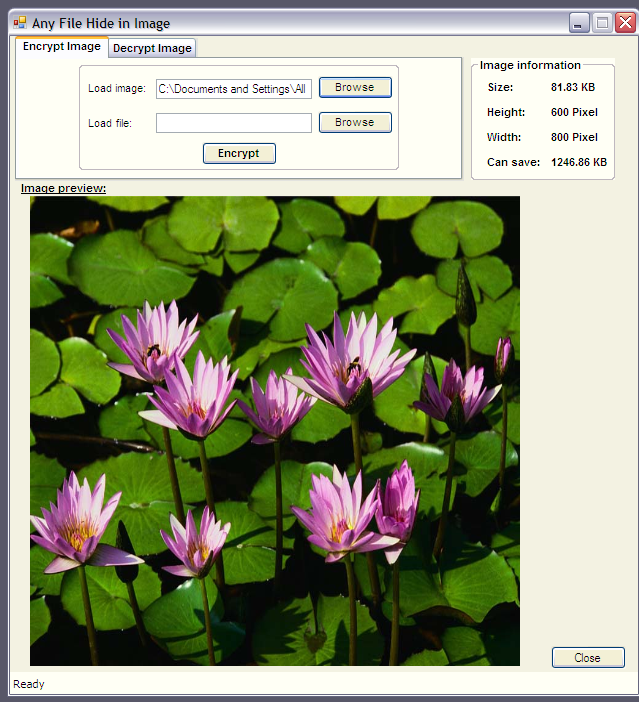
## 4.1 Encryption



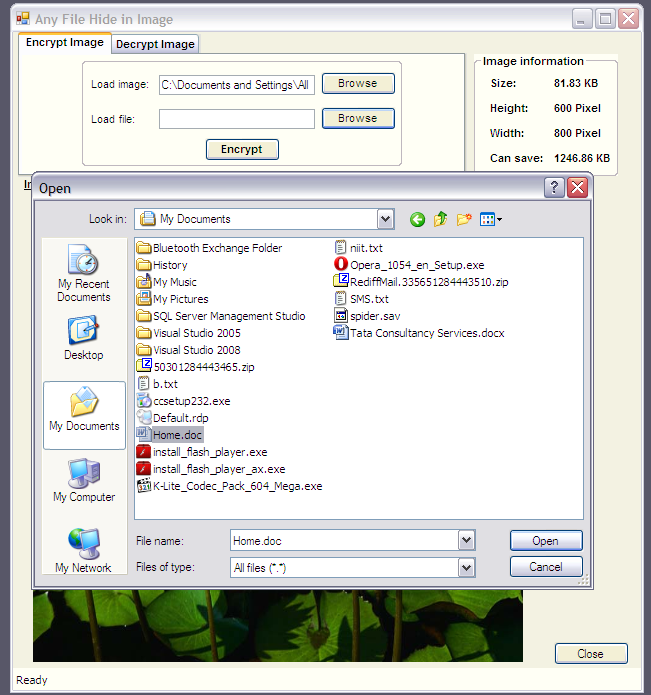
*1.For Encryption select Encrypt Image tab option*



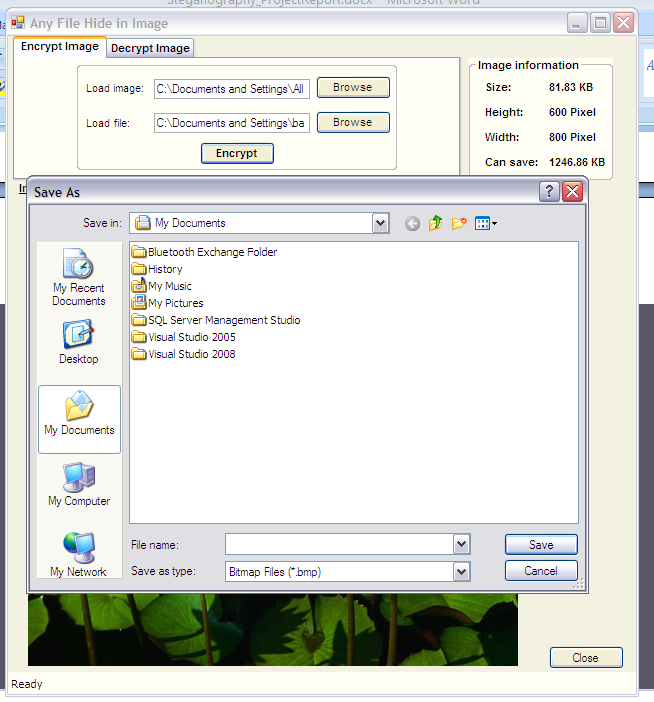
*2.For load image click on button “Browse” that is next to the Load Image textbox. The file open dialog box will displays as follows, select the Image file, which you want to use hide information and click on Open button.*



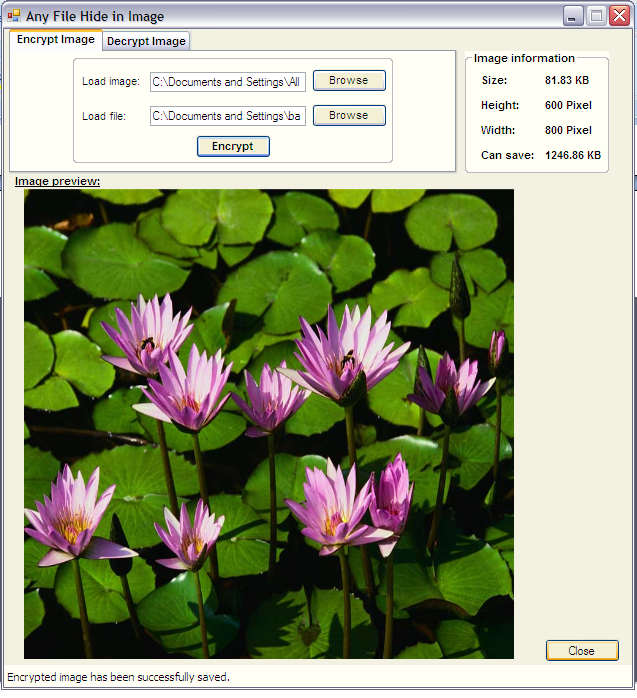
*3. The image file will opened and is displays as follows. Next, click on “Browse” button that is next to the Load File textbox.*



*4. Again the file open dialog box will appear, select any type of file whatever you want to hide with the image and click on ok button.*

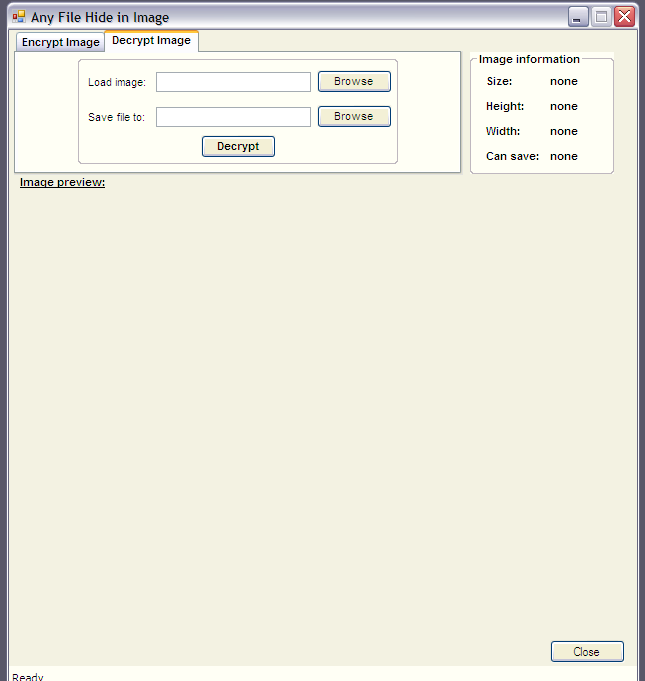


*5. The next step is to encrypt the file. Now click on “Encrypt” button, it will open the save dialog box which ask you to select the path to save the New image file and the Image file name. The default format of image file is BMP.*

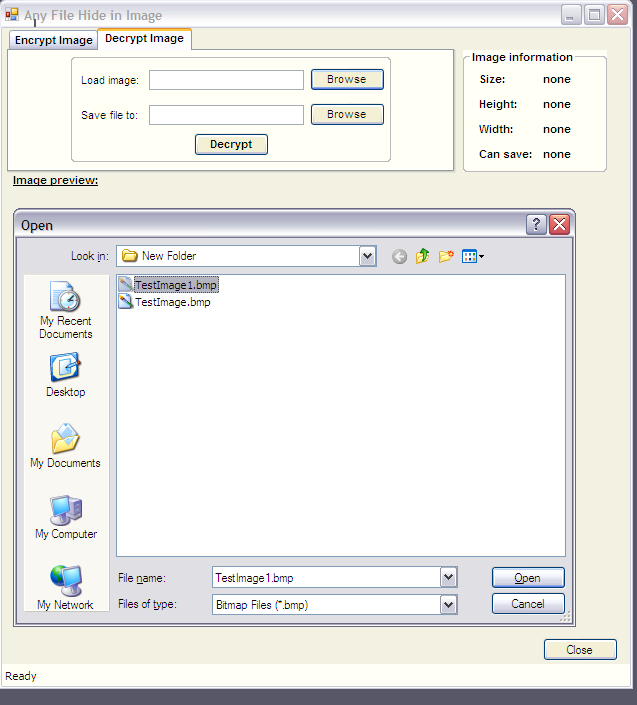


*6.Click encryption to encrypt image*

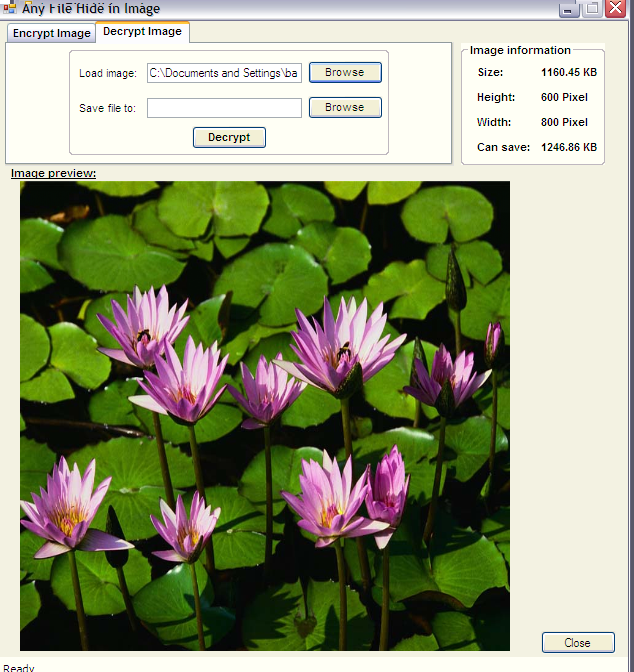
## 4.2 Decryption



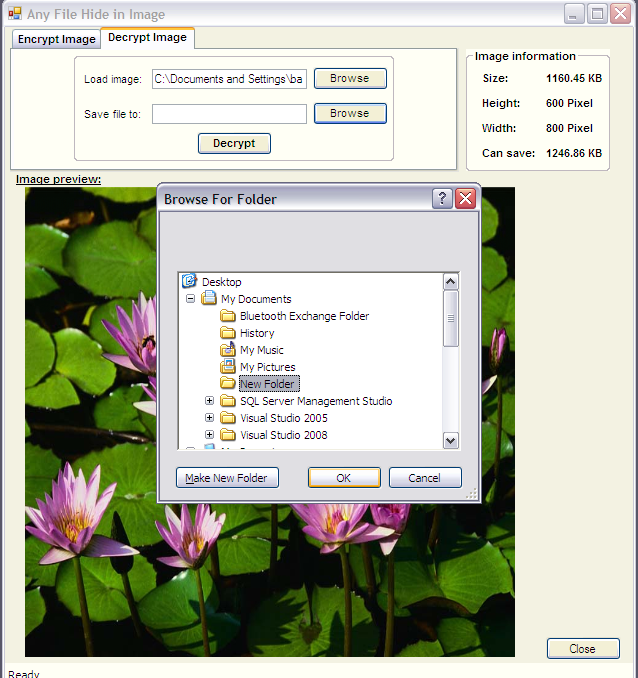
1. *Select the Decryption Image tab option*



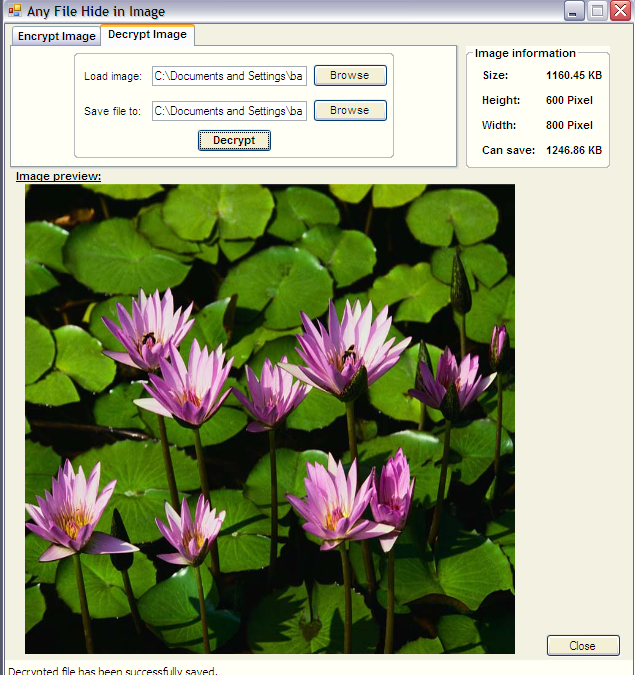
1. *Next click on the “Browse” button, which open the Open file dialog box, here you have to select the image which is Encrypted and has hidden information file. Select the image file and click on Open button.*



1. *The image file displayed as follows:*



1. *Now click on “Browse” button which is next to “Save file to” textbox. It will open a dialog box that is “Browse for folder”. It ask you to select the path or folder, where you want to extract the hidden file. Select the folder and click on Ok button.*



1. *Now click on Decrypt button, it will decrypt the image, the hidden file and image file is saved into selected folder. The message for successful decryption is displayed on the status bar which is places at bottom of the screen.*