GALGOTIAS UNIVERSITY

(Established under Galgotias University Uttar Pradesh Act No. 14 of 2011)

IMPLEMENTATION OF STEGANOGRAPHY

A Project Report for Capstone Project 2

Submitted by

ARJUN SHARMA

(1613101178/16SCSE101108)

in partial fulfillment for the award of the degree of

Bachelor of Technology

In

Computer Science and Engineering

Under the Supervision of

Dr. Avadhesh kumar,Professor&Dean Planning

April/May-2020

ABSTRACT

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. For hiding secret information in images, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points. Different applications may require absolute invisibility of the secret information, while others require a large secret message to be hidden. This project report intends to give an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good steganography algorithm and briefly reflects on which steganographic techniques are more suitable for which applications.

TABLE OF CONTENTS

TITLE	PAGE NO.
CERTIFICATE	ii
ABSTRACT	iii
LIST OF FIGURES	vi
LIST OF ABBREVIATIONS	vii
CHAPTER 1	x
1.1 IMPORTANCE OF STEGANGOGRAPHY	
1.2 WHAT ACTUALLY IS STEGANOGRAPHY?	
1.3 HISTORY OF STEGANOGRAPHY	
1.4 OVERVIEW OF SYSTEM	
1.5 OBJECTIVE	
CHAPTER 2	**xvii**
2.1 DETECTING STEGANOGRAPHY	
2.2 PROBLEM STATEMENT	
2.3 STEGANOGRAPHY VS CRYPTOGRAPHY	
2.4 STEGANOGRAPHY VS WATERMARKING	
2.5 STEGANOGRAPHY TECHNIQUES	
2.6 IMAGE STEGANOGRAPHY AND BITMAP PICTURES	
2.7 BITMAP STEGANOGRAPHY	
CHAPTER 3	**xxiii**
3.1 METHODOLOGY	
3.2 LIMITATIONS OF THE SYSTEM	
3.3 SYSTEM ANALYSIS AND DESIGN	
3.4 ENCRYPTION PROCESS	

3.6 DECRYPTION PROCESS
3.7 USER MANUAL
3.8 FOR ENCRYPTION
3.9 FOR DECRYPTION

CHAPTER 4 **xxxiii**
SUMMARY AND CONCLUSION
REFERENCES

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

Certified that this project report "IMPLEMENTATION OF STEGANOGRAPHY" is the bonafide work of "ARJUN SHARMA" who carried out the project work under my supervision.

SIGNATURE OF HEAD **SIGNATURE OF SUPERVISOR**

Dr. MUNISH SHABARWAL
Phd(Management),Phd(CS)
PROFESSOR & DEAN
School Of Computing Science
And engineering

Dr. AVADHESH KUMAR
Phd(CS)
PROFESSOR & DEAN
School Of ComputingScience
and engineering

LIST OF FIGURES

TITLE OF FIGURE	FIGURE NO.
Model of Steganography	Fig-1
Changeability function	Fig-2
Graphical representation of System	Fig-3
Encryption Process	Fig-4
Decryption Process	Fig-5
First Screen of Application	Fig-6
Image Loading Screen	Fig-7
File Loading Screen	Fig-8
Selection of file	Fig-9
Encrypting Stage	Fig-10
Resultant BMP image	Fig-11
Decryption Screen of Application	Fig-12
Selection of Encrypted Image	Fig-13
Loaded image in Application	Fig-14
Selection of Desired Save Location	Fig-15
Decrypting Desired Image	Fig-16

LIST OF ABBREVIATIONS

TITLE	ABBREVIATION
1.ICT	Information and communications technology
2.JPEG	Joint Photographic Experts Group
3.TCP	Transmission Control Protocol
4.UDP	User Datagram Protocol
5.IP	Internet Protocol
6.LSB	Least Significant bit
7.SIHS	Secure Information Hiding System
8.BMP	Bitmap
9.GIF	Graphics Interchange Format
10.MSB	Most Significant Bit

CHAPTER 1
INTRODUCTION

One of the reasons that intruders can be successful is the most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, through the use of steganography. Steganography is a technique of hiding information in digital media. In contrast to cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists.

1.1 IMPORTANCE OF STEGANOGRAPHY

Steganography become more important as more people join the cyberspace revolution. Steganography is the art of concealing information in ways that prevents the detection of hidden messages. Stegranography include an array of secret communication methods that hide the message from being seen or discovered.

Due to advances in ICT, most of information is kept electronically. Consequently, the security of information has become a fundamental issue. Besides cryptography, streganography can be employed to secure information. In cryptography, the message or encrypted message is embedded in a digital host before passing it through the network, thus the existence of the message is unknown. Besides hiding data for confidentiality, this approach of information hiding can be extended to copyright protection for digital media: audio, video and images.

The growing possibilities of modern communications need the special means of security especially on computer network. The network security is becoming more important as the number of data being exchanged on the internet increases. Therefore, the confidentiality and data integrity

are requires to protect against unauthorized access and use. This has resulted in an explosive growth of the field of information hiding
Information hiding is an emerging research area, which encompasses applications such as copyright protection for digital media, watermarking, fingerprinting, and steganography.

In watermarking applications, the message contains information such as owner identification and a digital time stamp, which usually applied for copyright protection.

Fingerprint, the owner of the data set embeds a serial number that uniquely identifies the user of the data set. This adds to copyright information to makes it possible to trace any unauthorized used of the data set back to the user.

Steganography hide the secrete message within the host data set and presence imperceptible and is to be reliably communicated to a receiver. The host data set is purposely corrupted, but in a covert way, designed to be invisible to an information analysis.

1.2 WHAT ACTUALLY IS STEGANOGRAPHY?

Steganography is the practice of hiding private or sensitive information within something that appears to be nothing out to the usual. Steganography is often confused with cryptology because the two are similar in the way that they both are used to protect important information. The difference between two is that steganography involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information.

What steganography essentially does is exploit human perception, human senses are not trained to look for files that have information inside of

them, although this software is available that can do what is called Steganography. The most common use of steganography is to hide a file inside another file.

1.3 HISTORY OF STEGANOGRAPHY

Through out history Steganography has been used to secretly communicate information between people.

Some examples of use of Steganography is past times are:

1. During World War 2 invisible ink was used to write information on pieces of paper so that the paper appeared to the average person as just being blank pieces of paper. Liquids such as milk, vinegar and fruit juices were used, because when each one of these substances are heated they darken and become visible to the human eye.
2. In Ancient Greece they used to select messengers and shave their head, they would then write a message on their head. Once the message had been written the hair was allowed to grow back. After the hair grew back the messenger was sent to deliver the message, the recipient would shave off the messengers hair to see the secrete message.

1.4 OVERVIEW OF SYSTEM

The word steganography comes from the Greek “Seganos”, which mean covered or secret and – “graphy” mean writing or drawing. Therefore, steganography mean, literally, covered writing. It is the art and science of hiding information such its presence cannot be detected and a communication is happening. A secrete information is encoding in a manner such that the very existence of the information is concealed.

Paired with existing communication methods, steganography can be used to carry out hidden exchanges.

The main goal of this projects it to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hider data. There has been a rapid growth of interest in steganography for two reasons:

The publishing and broadcasting industries have become interested in techniques for hiding encrypted copyright marks and serial numbers in digital films, audio recordings, books and multimedia products

Moves by various governments to restrict the availability of encryption services have motivated people to study methods by which private messages can be embedded in seemingly innocuous cover messages.

The basic model of steganography consists of Carrier, Message and password. Carrier is also known as cover-object, which the message is embedded and serves to hide the presence of the message.

Basically, the model for steganography is shown on following figure:

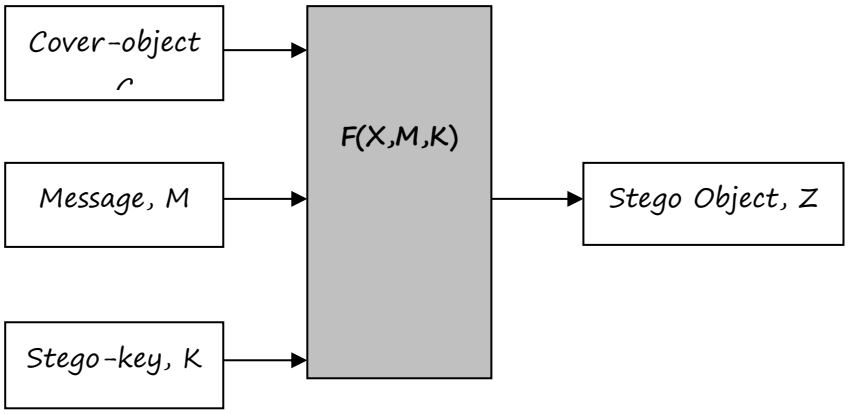


Fig-1

Message is the data that the sender wishes to remain it confidential. It can be plain text, ciphertext, other image, or anything that can be embedded in a bit stream such as a copyright mark, a covert communication, or a serial number. Password is known as *stego-key*, which ensures that only

recipient who know the corresponding decoding key will be able to extract the message from a *cover-object*. The *cover-object* with the secretly embedded message is then called the *Stego-object*.

Recovering message from a *stego-object* requires the *cover-object* itselt and a corresponding decoding key if a *stego-key* was used during the encoding process. The original image may or may not be required in most applications to extract the message.

There are several suitable carriers below to be the *cover-object:*

- Network protocols such as TCP, IP and UDP
- Audio that using digital audio formats such as wav, midi, avi, mpeg, mpi and voc
- File and Disk that can hides and append files by using the slack space
- Text such as null characters, just alike morse code including html and java
- Images file such as bmp, gif and jpg, where they can be both color and gray-scale.

In general, the information hiding process extracts redundant bits from *cover-object.* The process consists of two steps:

- Identification of redundant bits in a *cover-object.* Redundant bits are those bits that can be modified without corrupting the quality or destroying the integrity of the *cover-object.*
- Embedding process then selects the subset of the redundant bits to be replaced with data from a secret message. The *stego-object* is created by replacing the selected redundant bits with message bits

1.5 OBJECTIVE

The goal of steganography is covert communication. So, a fundamental requirement of this steganography system is that the hider message carried by stego-media should not be sensible to human beings.

The other goad of steganography is to avoid drawing suspicion to the existence of a hidden message. This approach of information hiding technique has recently became important in a number of application area
This project has following objectives:

- To product security tool based on steganography techniques.
- To explore techniques of hiding data using encryption module of this project
- To extract techniques of getting secret data using decryption module.

Steganography sometimes is used when encryption is not permitted. Or, more commonly, steganography is used to supplement encryption. An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered, the hidden message is not seen.

CHAPTER 2
LITERATURE REVIEW

To conclude with the literature survey,we can non arguably confine the content that this technique is chosen, because this system includes not only imperceptibility but also un-delectability by any steganolysis tool.

2.1 DETECTING STEGANOGRAPHY

The art of detecting Steganography is referred to as **Steganalysis.**

To put is simply Steganalysis involves detecting the use of Steganography inside of a file. Steganalysis does not deal with trying to decrypt the hidden information inside of a file, just discovering it.

There are many methods that can be used to detect Steganography such as:

“Viewing the file and comparing it to another copy of the file found on the Internet (Picture file). There are usually multiple copies of images on the internet, so you may want to look for several of them and try and compare the suspect file to them. For example if you download a JPED and your suspect file is also a JPED and the two files look almost identical apart from the fact that one is larger than the other, it is most probable you suspect file has hidden information inside of it.

2.2 PROBLEM STATEMENT

The former consists of linguistic or language forms of hidden writing. The later, such as invisible ink, try of hide messages physically. One disadvantage of linguistic steganography is that users must equip themselves to have a good knowledge of linguistry. In recent years,

everything is trending toward digitization. And with the development of the internet technology, digital media can be transmitted conveniently over the network. Therefore, messages can be secretly carried by digital media by using the steganography techniques, and then be transmitted through the internet rapidly

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. For hiding secret information in images, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points.

2.3 STEGANOGRAPHY VS CRYPTOGRAPHY

Basically, the purpose of cryptography and steganography is to provide secret communication. However, steganography is not the same as cryptography. Cryptography hides the contents of a secrete message from a malicious people, whereas steganography even conceal the existence of the message. In cryptography, the system is broken when the attacker can read the secret message. Breaking a steganography system need the attacker to detect that steganography has been used.

It is possible to combine the techniques by encrypting message using cryptography and then hiding the encrypted message using steganography. The resulting stego-image can be transmitted without revealing that secret information is being exchanged.

2.4 STEGANOGRAPHY VS WATERMARKING

Steganography pay attention to the degree of Invisibility while watermarking pay most of its attribute to the robustness of the message

and its ability to withstand attacks of removal, such as image operations(rotation, cropping, filtering), audio operations(rerecording, filtering)in the case of images and audio files being watermarked respectively.

It is a non-questionable fact that delectability of a vessel with an introduced data (steganographic message or a watermark) is a function of the changeability function of the algorithm over the vessel.

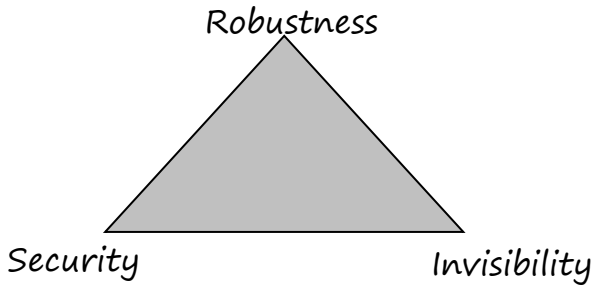


Fig-2

That is the way the algorithm changes the vessel and the severity of such an operation determines with no doubt the delectability of the message, since delectability is a function of file characteristics deviation from the norm, embedding operation attitude and change severity of such change decides vessel file delectability.

A typical triangle of conflict is message Invisibility, Robustness, and Security. Invisibility is a measure of the in notability of the contents of the message within the vessel.

Security is sinominous to the cryptographic idea to message security, meaning inability of reconstruction of the message without the proper secret key material shared.

Robustness refers to the endurance capability of the message to survive distortion or removal attacks intact. It is often used in the watermarking

field since watermarking seeks the persistence of the watermark over attacks, steganographic messages on the other hand tend to be of high sensitivity to such attacks. The more invisible the message is the less secure it is (cryptography needs space) and the less robust it is (no error checking/recovery introduced).The more robust the message is embedded the more size it requires and the more visible it is.

2.5 STEGANOGRAPHY TECHNIQUES

Over the past few years, numerous steganography techniques that embed hidden messages in multimedia objects have been proposed. There have been many techniques for hiding information or messages in images in such a manner that alteration made to the image is perceptually indiscernible. Commonly approaches are include LSB, Masking and filtering and Transform techniques.

Least significant bit (LSB) insertion is a simple approach to embedding information in image file. The simplest steganography techniques embed the bits of the message directly into least significant bit plane of the cover-image in a

deterministic sequence. Modulating the least significant bit does not result in human perceptible difference because the amplitude of the change is small. In this technique, the embedding capacity can be increased by using two or more least significant bits. At the same time, not only the risk of making the embedded message statistically detectable increase but also the image fidelity degrades. Hence a variable size LSB embedding schema is presented, in which the number of LSBs used for message embedding/extracting depends on the local characteristics of the pixel. The advantage of LSB-based method is easy to implement and high message pay-load.

Although LSB hides the message in such way that the humans do not perceive it, it is still possible for the opponent to retrieve the message due

to the simplicity of the technique. Therefore, malicious people can easily try to extract the message from the beginning of the image if they are suspicious that there exists secret information that was embedded in the image.

Therefore, a system named Secure Information Hiding System (SIHS) is proposed to improve the LSB scheme. It overcomes the sequence-mapping problem by embedding the massage into a set of random pixels, which are scattered on the cover-image.

Masking and filtering techniques, usually restricted to 24 bits and gray scale image, hide information by marking an image, in a manner similar to paper watermarks. The technique perform analysis of the image, thus embed the information in significant areas so that the hidden message is more integral to cover image than just hiding it in the noise level.

Transform techniques embed the message by modulating coefficient in a transform domain, such as the Discrete Fourier Transform, or Wavelet Transform. These methods hide messages in significant areas of the cover image, which make them more robust to attack. Transformations can be applied over the entire image, to block throughout the image, or other variant.

2.6 IMAGE STEGANOGRAPHY AND BITMAP PICTURES

Using bitmap pictures for hiding secret information is one of most popular choices for Steganography. Many types of software built for this purpose, some of these software use password protection to encrypting information on picture. To use these software you must have a ‘BMP’ format of a pictures to use it, but using other type of pictures like “JPEG”, “GIF” or any other types is rather or never used, because of algorithm of “BMP” pictures for Steganography is simple. Also we know that in the web most popular of image types are “JPEG” and other types not “BPM”, so we should have a solution for this problem.

This software provide the solution of this problem, it can accept any type of image to hide information file, but finally it give the only “BMP” image as an output that has hidden file inside it.

2.7 BITMAP STEGANOGRAPHY

Bitmap type is the simplest type of picture because that it doesn’t have any technology for decreasing file size. Structure of these files is that a bitmap image created from pixels that any pixel created from three colors (red, green and blue said RGB) each color of a pixel is one byte information that shows the density of that color. Merging these three color makes every color that we see in these pictures. We know that every byte in computer science is created from 8 bit that first bit is Most-Significant-Bit (MSB) and last bit Least-Significant-Bit (LSB), the idea of using Steganography science is in this place; we use LSB bit for writing our security information inside BMP pictures. So if we just use last layer (8st layar) of information, we should change the last bit of pixels, in other hands we have 3 bits in each pixel so we have 3*hight*width bits memory to write our information. But before writing our data we must write name of data(file), size of name of data & size of data. We can do this by assigning some first bits of memory (8st layer).

(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011)

Using each 3 pixel of picture to save a byte of data.

CHAPTER 3
PROPOSED MODEL

This project is developed for hiding information in any image file. The scope of the project is implementation of steganography tools for hiding information includes any type of information file and image files and the path where the user wants to save Image and extruded file.

3.1 METHODOLOGY

User needs to run the application. The user has two tab options – encrypt and decrypt. If user select encrypt, application give the screen to select image file, information file and option to save the image file. If user select decrypt, application gives the screen to select only image file and ask path where user want to save the secrete file.

This project has two methods – Encrypt and Decrypt.

In encryption the secrete information is hiding in with any type of image file.

Decryption is getting the secrete information from image file.

3.2 LIMITATIONS OF THE SOFTWARE

This project has an assumption that is both the sender and receiver must have shared some secret information before imprisonment. Pure steganography means that there is none prior information shared by two communication parties.This assumption should be introduced as no prior connection between the hosts doesn’t allow the application to proceed and this limitation may be advanced in future enhancements as it is

already being focused on.The most scrumptious future enhancement would be to make it a pure steganography applicaton wherein the hosts doesn't need a prior connection to access each other and process towards the encryption and decryption of the related file.

3.3 SYSTEM ANALYSIS AND DESIGN

Steganography system requires any type of image file and the information or message that is to be hidden. It has two modules encrypt and decrypt.
Microsoft .Net framework prepares a huge amount of tool and options for programmers that they simples programming. One of .Net tools for pictures and images is auto-converting most types of pictures to BMP format. I used this tool in this software called "Steganography" that is written in C#.Net language and you can use this software to hide your information in any type of pictures without any converting its format to BMP (software converts inside it).
The algorithm used for Encryption and Decryption in this application provides using several layers lieu of using only LSB layer of image. Writing data starts from last layer (8st or LSB layer); because significant of this layer is least and every upper layer has doubled significant from its down layer. So every step we go to upper layer image quality decreases and image retouching transpires.
The encrypt module is used to hide information into the image; no one can see that information or file. This module requires any type of image and message and gives the only one image file in destination.
The decrypt module is used to get the hidden information in an image file. It take the image file as an output, and give two file at destination folder, one is the same image file and another is the message file that is hidden it that.

Before encrypting file inside image we must save name and size of file in a definite place of image. We could save file name before file information in LSB layer and save file size and file name size in most right-down pixels of image. Writing this information is needed to retrieve file from encrypted image in decryption state.

The graphical representation of this system is as follows:

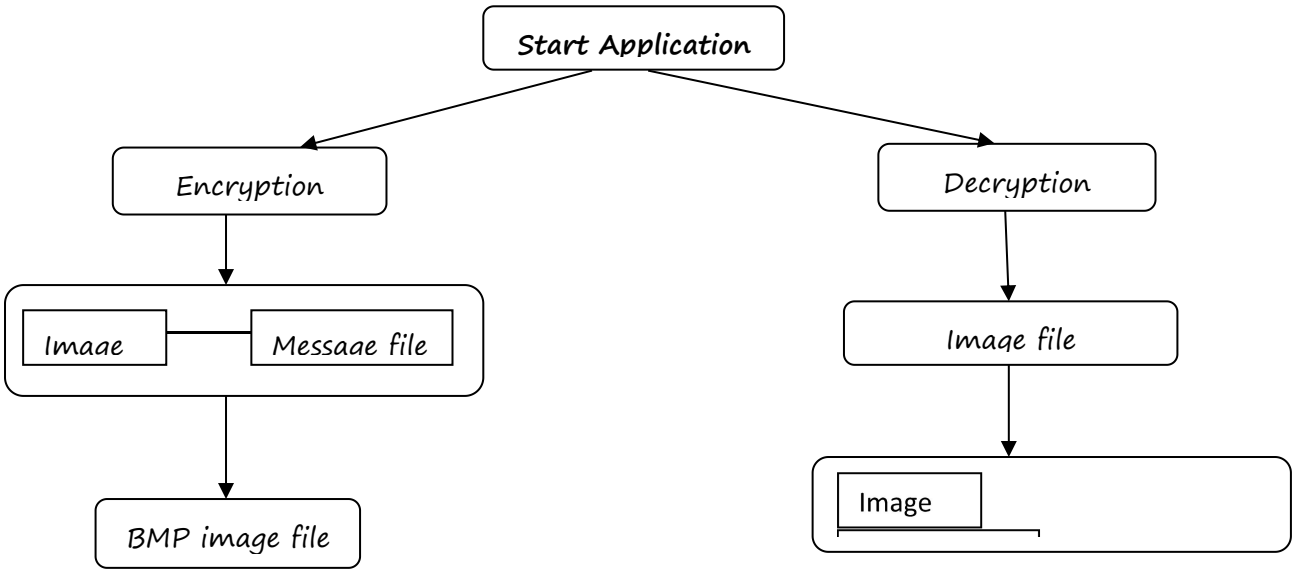
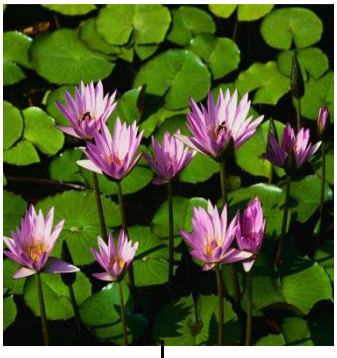


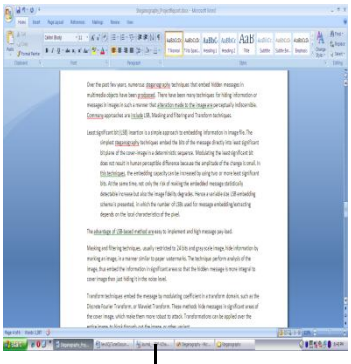
Fig-3

3.4 ENCRYPTION PROCESS

IMAGE FILE



INFORMATION FILE

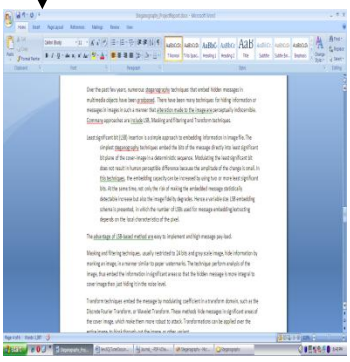


BMP FILE (Fig-4)

3.5 DECRYPTION PROCESS

BMP FILE

IMAGE FILE



INFORMATION FILE

Fig-5

3.6 USER MANUAL

This is the first screen which has two tab options – one is Encrypt Image for encryption and another is Decrypt image for decryption. In right – top panel is displays the information about the image such as size, height and width.

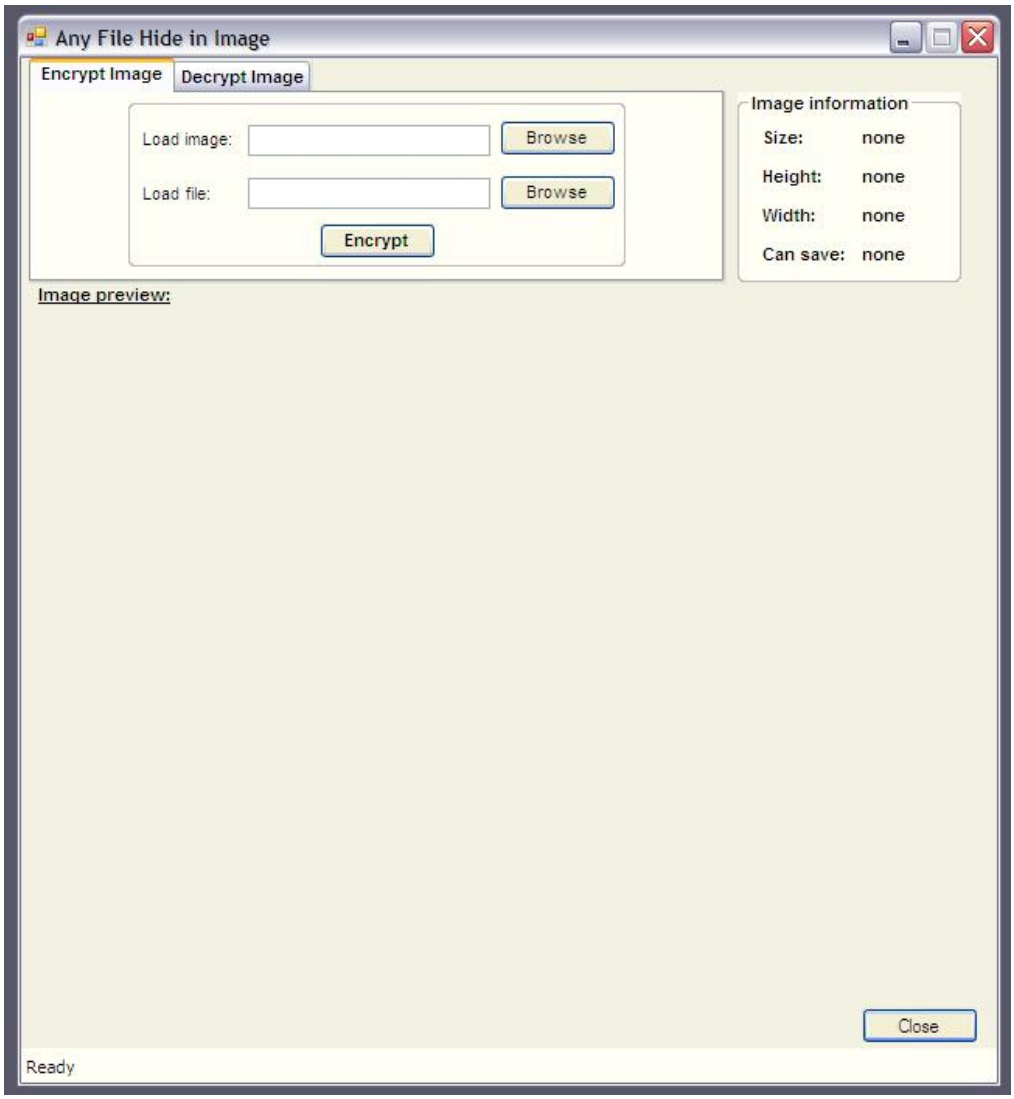


Fig-6

3.7 FOR ENCRYPTION:

1.For Encryption select Encrypt Image tab option from the notification bar on top.

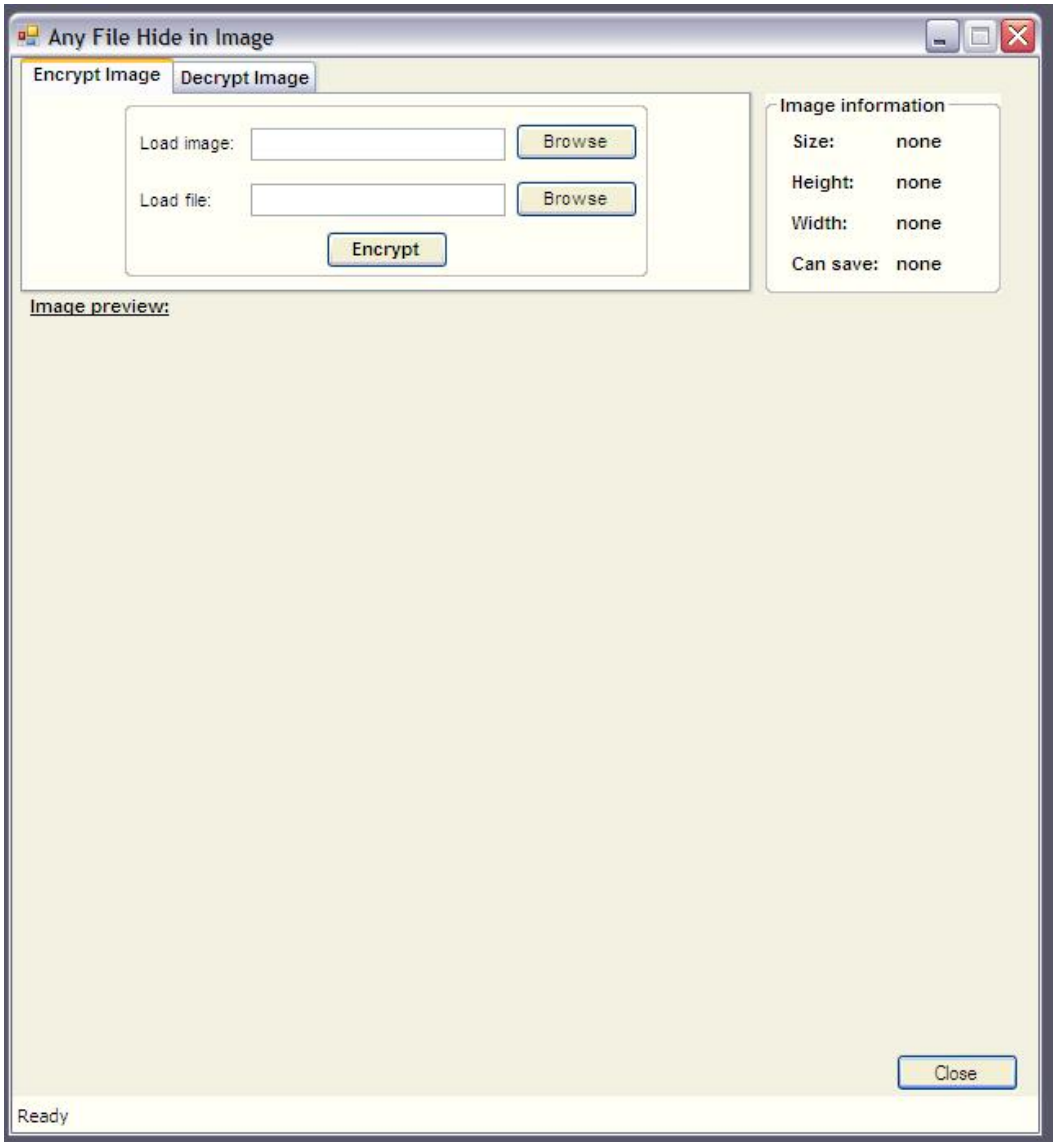


Fig-7

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.

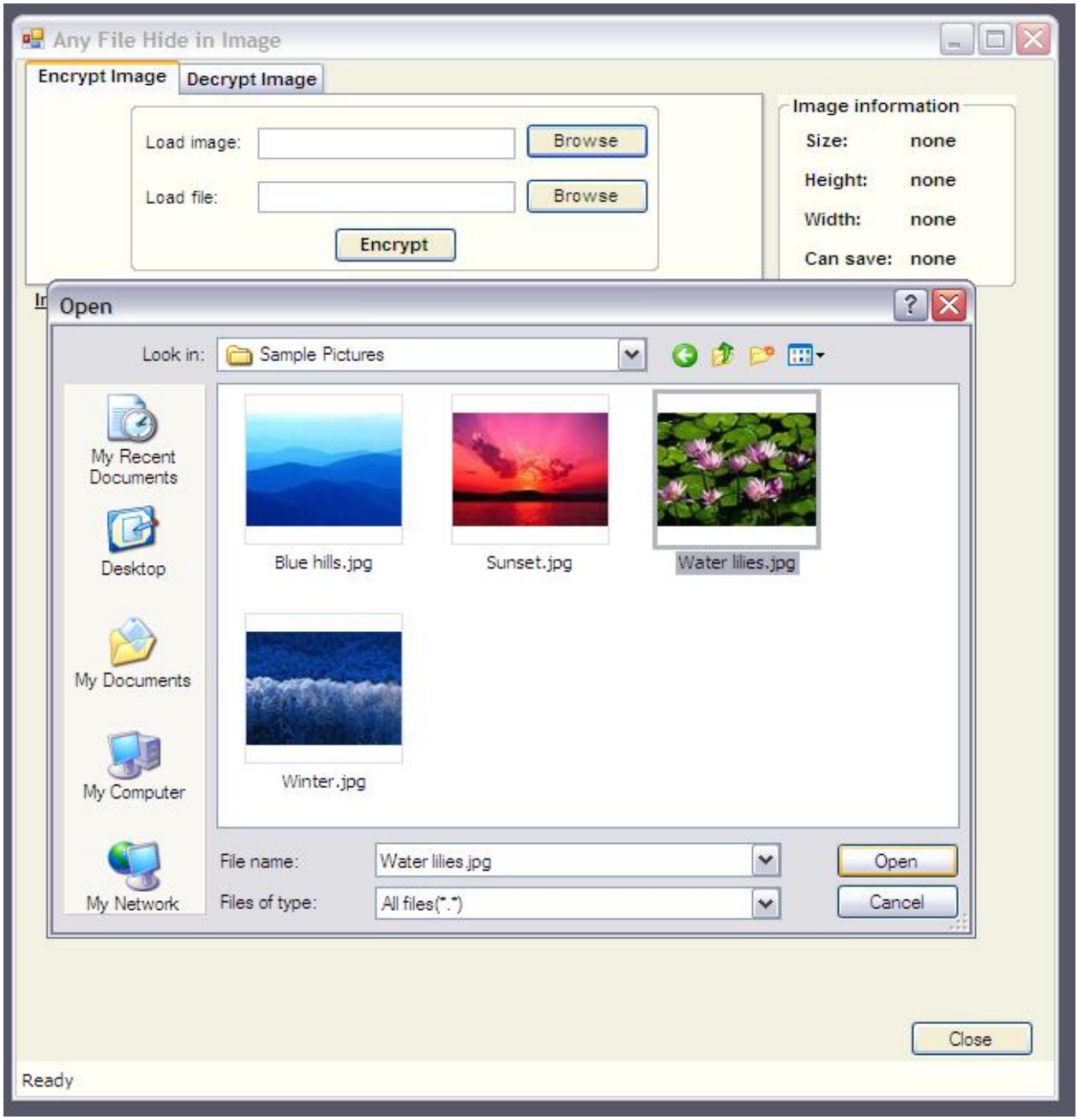


Fig-8

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

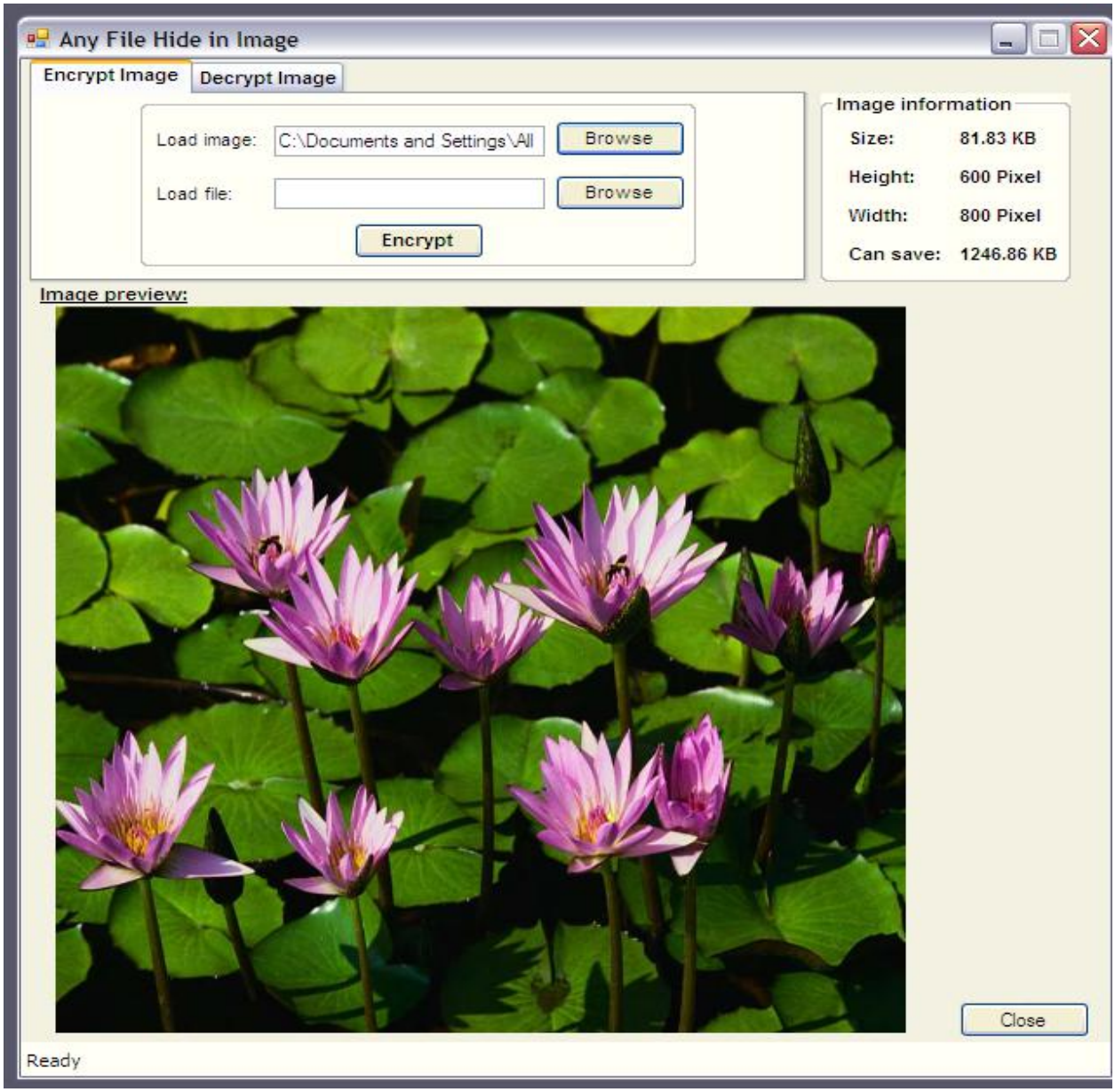


Fig-9

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.

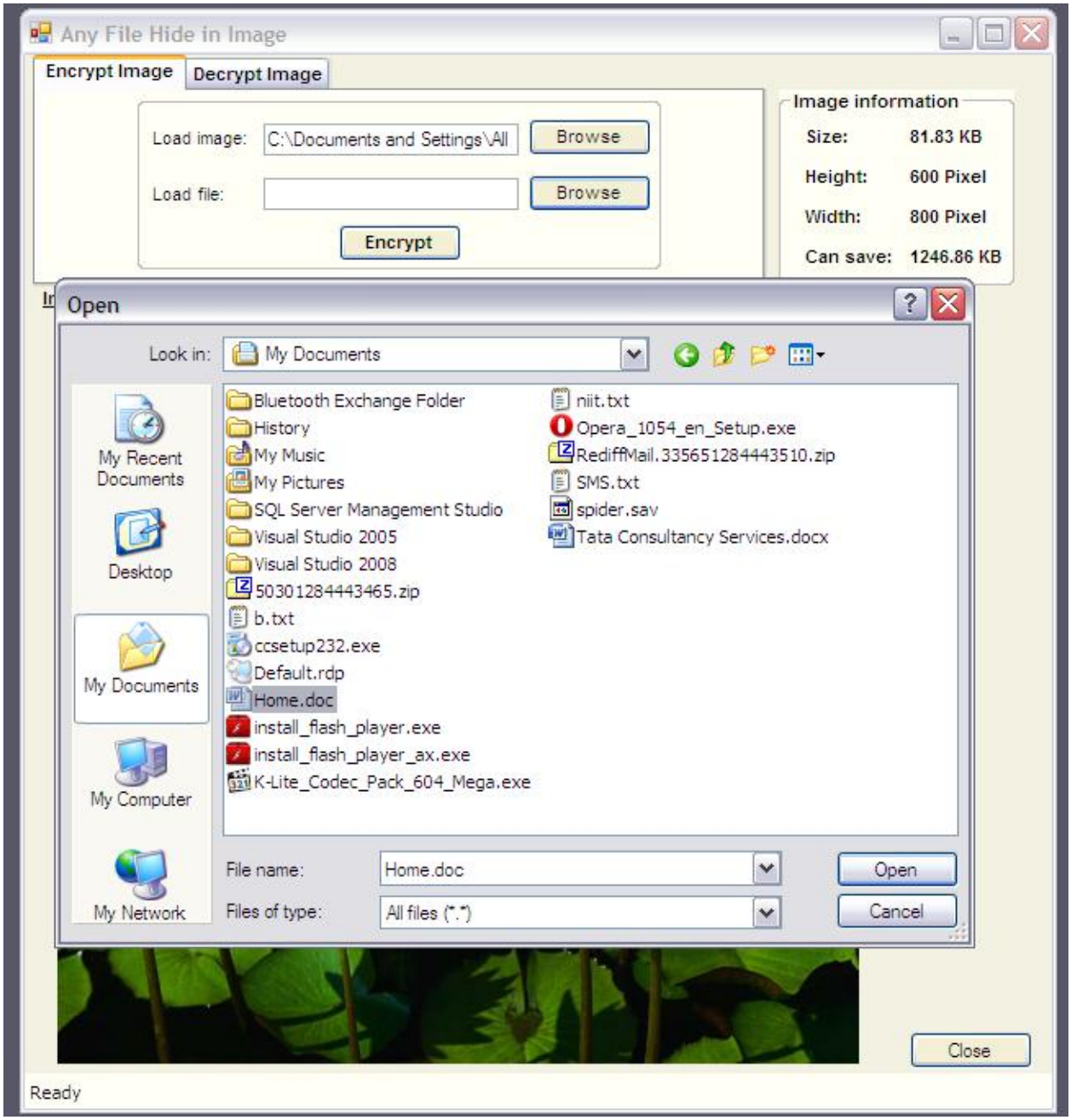


Fig-10

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.

Fig-11

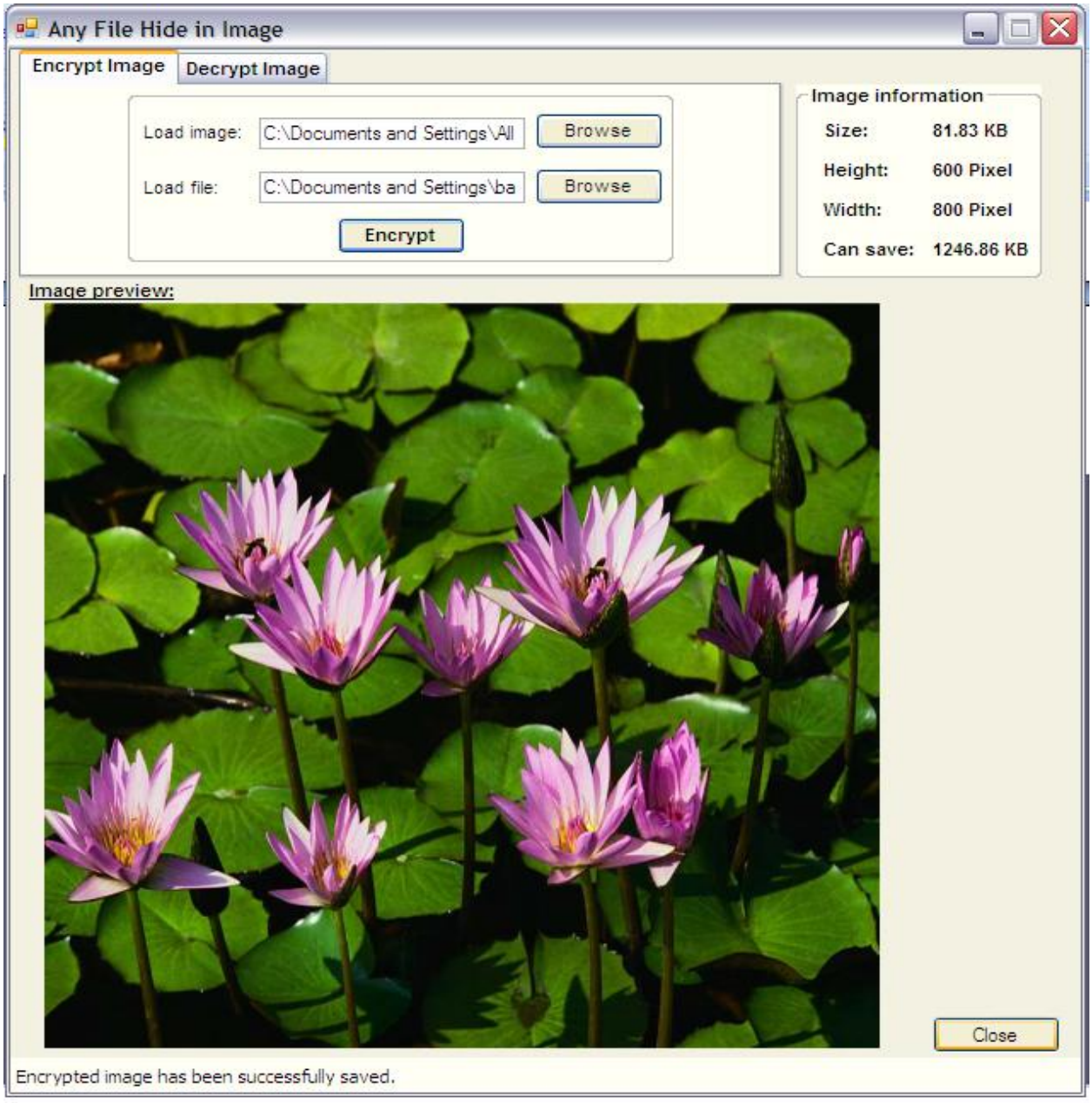


Fig-12

3.8 FOR DECRYPTION:

1. Select the Decryption Image tab option.

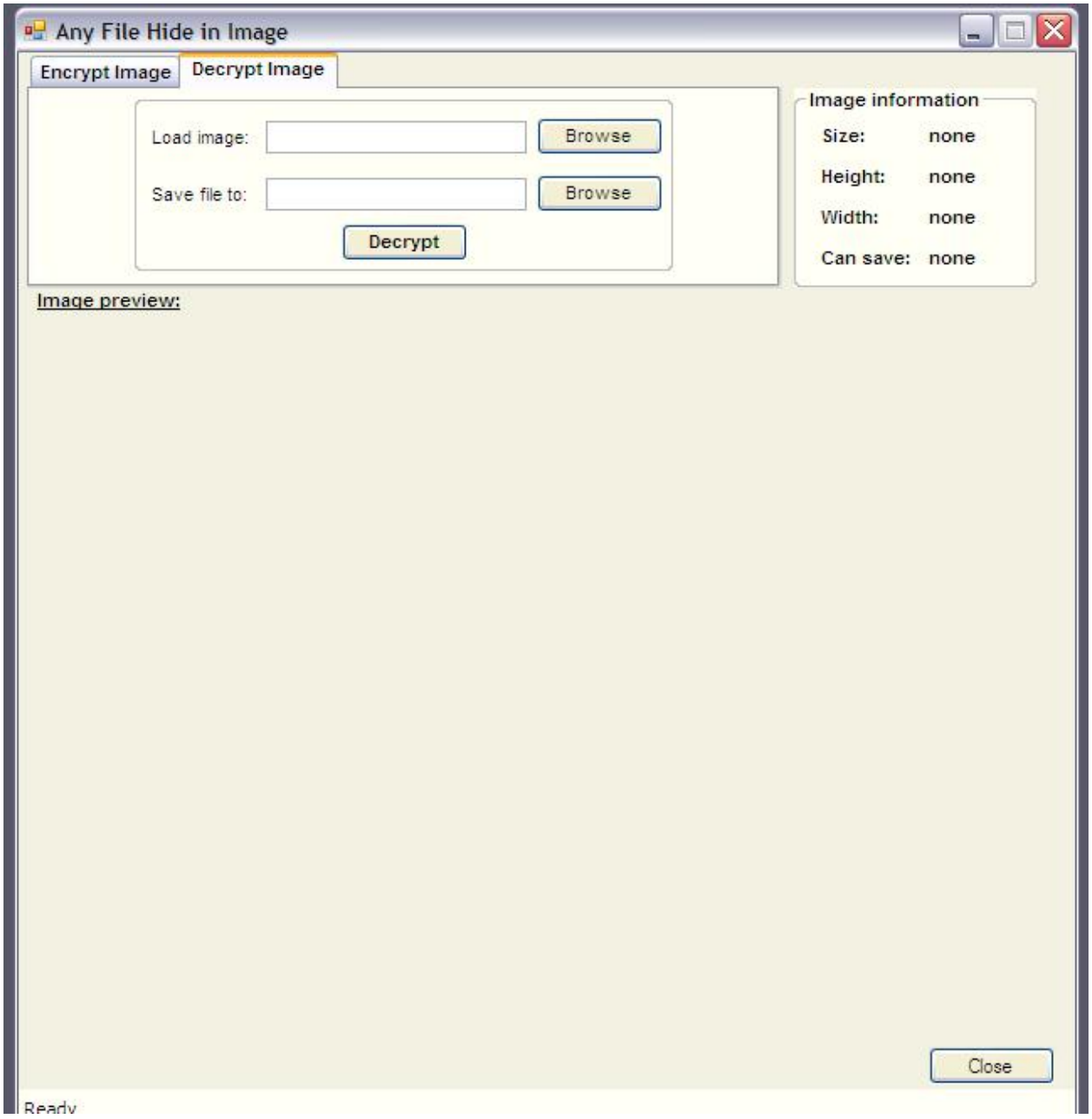


Fig-13

2. 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.

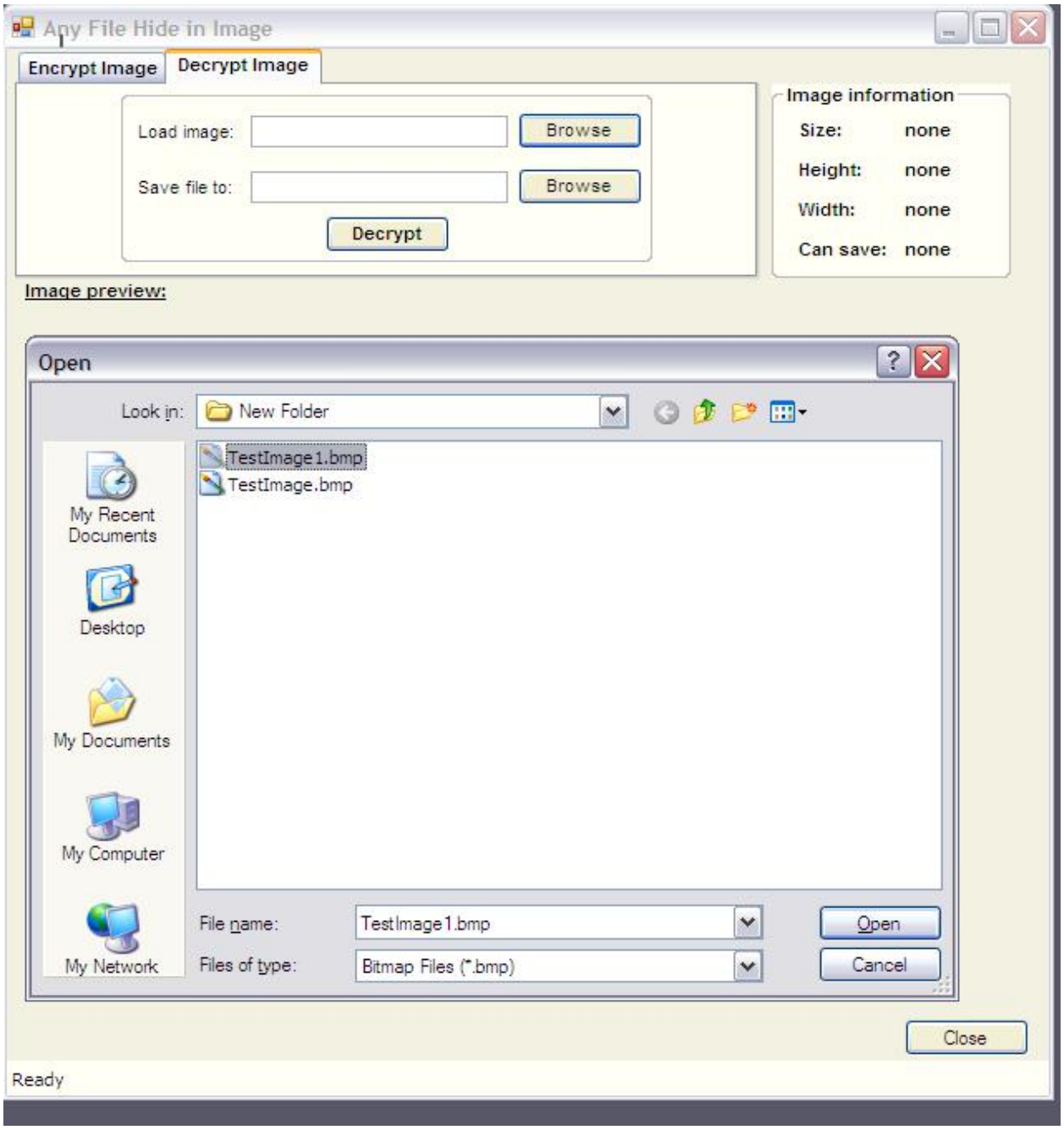


Fig-14

3.The image file displayed as follows:

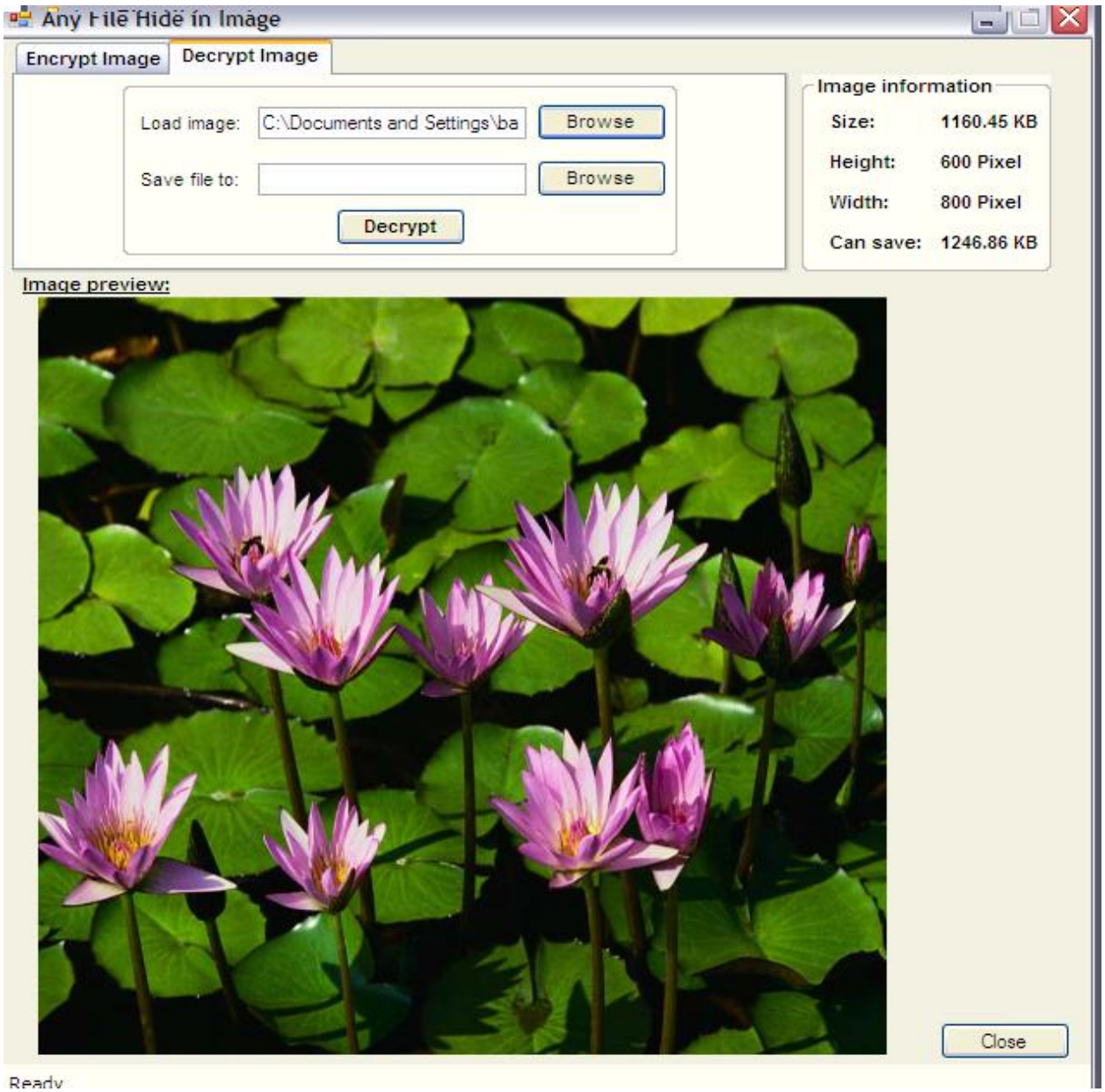


Fig-15

4. 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.

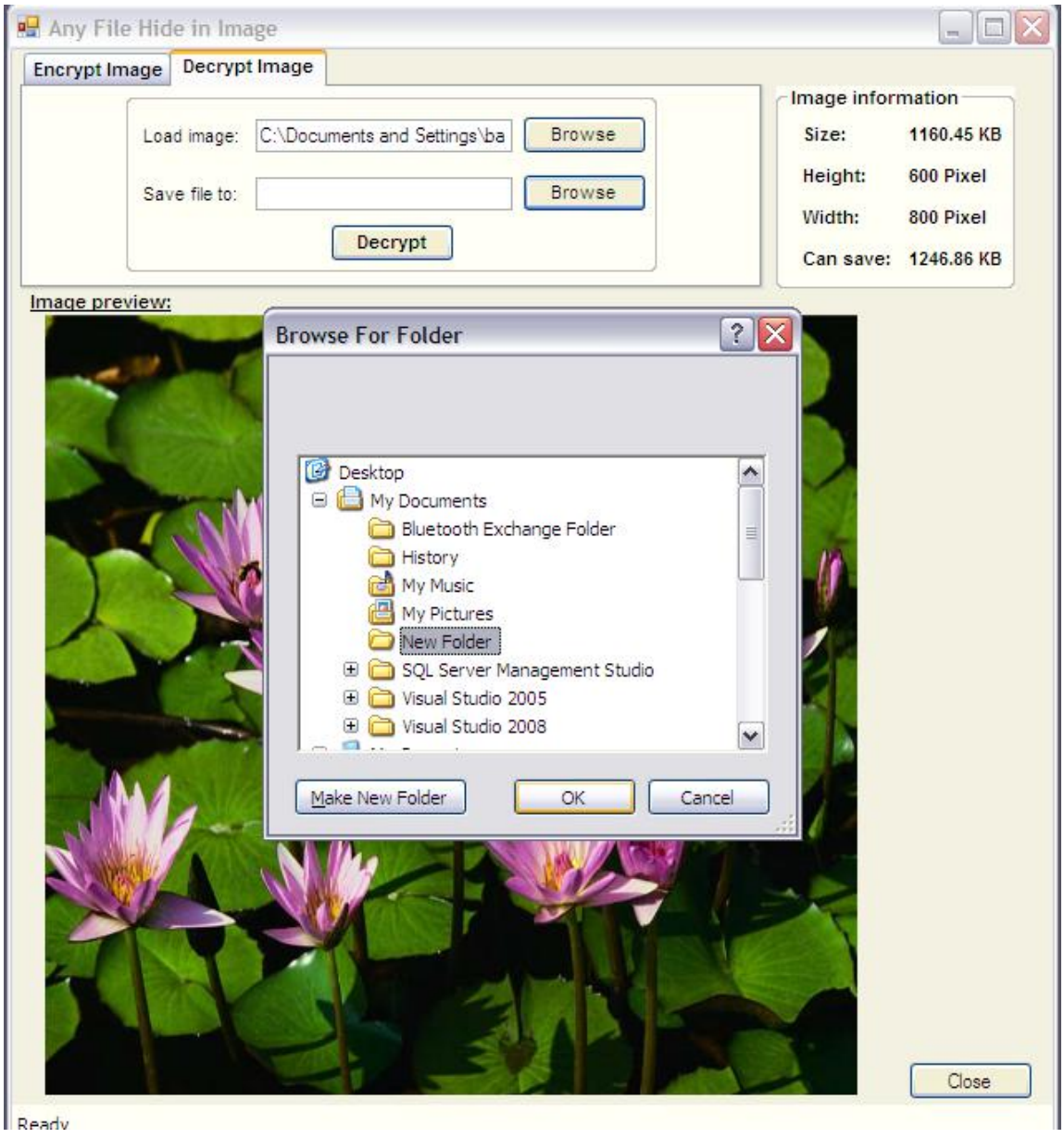


Fig-16

5.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.

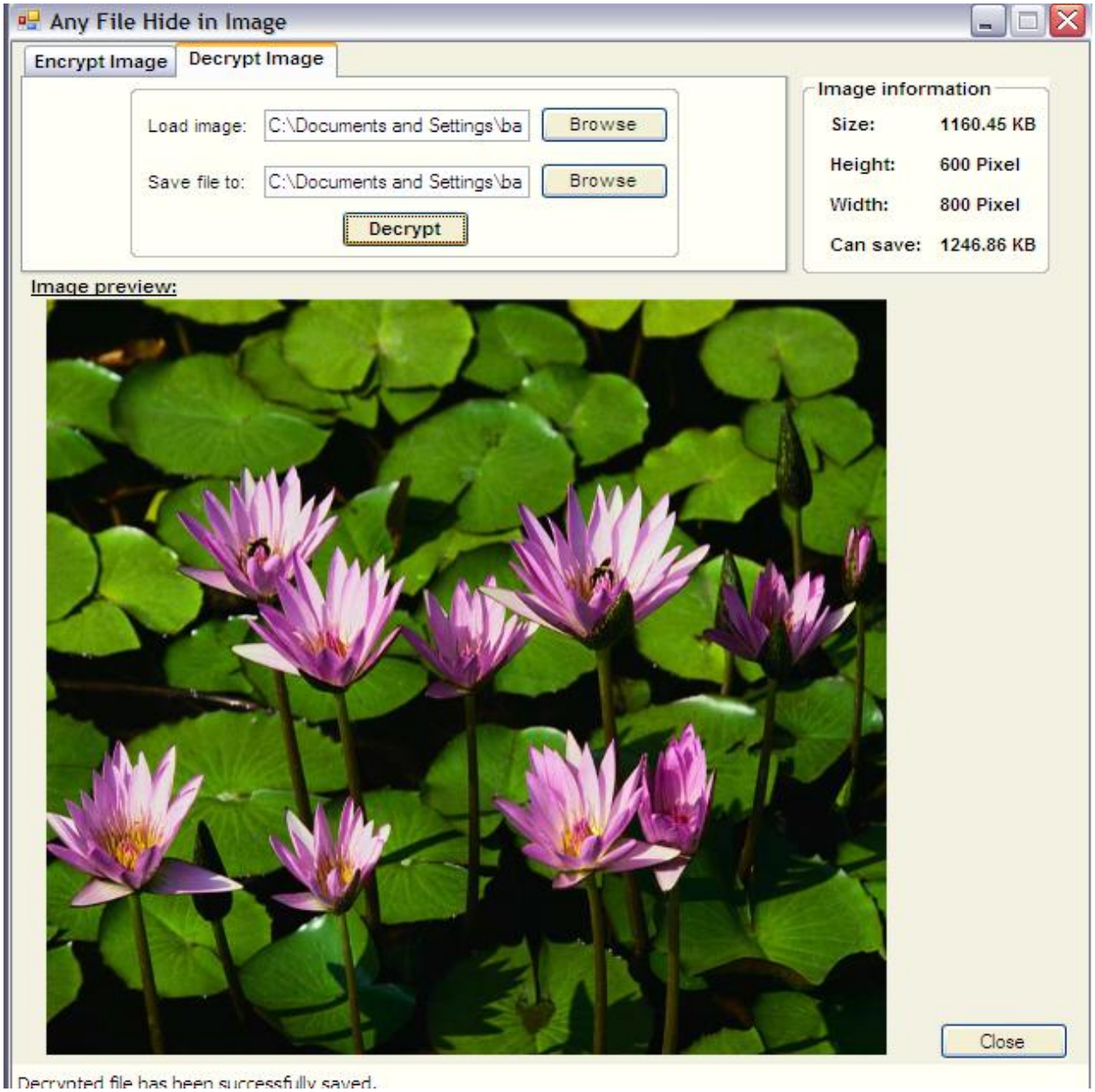


Fig-17

CHAPTER 4
SUMMARY AND CONCLUSION

Steganography is a really interesting subject and outside of the mainstream cryptography and system administration that most of us deal with day after day.

Steganography can be used for hidden communication. We have explored the limits of steganography theory and practice. We printed out the enhancement of the image steganography system using LSB approach to provide a means of secure communication. A stego-key has been applied to the system during embedment of the message into the cover image.

This steganography application software provided for the purpose to how to use any type of image formats to hiding any type of files inside their. The master work of this application is in supporting any type of pictures without need to convert to bitmap, and lower limitation on file size to hide, because of using maximum memory space in pictures to hide the file.

Since ancient times, man has found a desire in the ability to communicate covertly. The recent explosion of research in watermarking to protect intellectual property is evidence that steganography is not just limited to military or espionage applications. Steganography, like cryptography, will play an increasing role in the future of secure communication in the "digital world".

REFERENCES

1. Catrin Burrows ; Pooneh Bagheri Zadeh
   2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security)

2. A Comparative Evaluation of Jpeg Steganography
Dipti Watni ; Sonal Chawla
2019 5th International Conference on Signal Processing, Computing and Control (ISPCC)

3. Linguistic Steganography Detection Based on Perplexity
Peng Meng ; Liusheng Huang ; Zhili Chen ; Wei Yang ; Dong Li
2008 International Conference on MultiMedia and Information Technology

4. Data hiding on web using combination of Steganography and Cryptography
Lipi Kothari ; Rikin Thakkar ; Satvik Khara
2017 International Conference on Computer, Communications and Electronics (Comptelix)