IFERP
connecting engineers... developing research

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 3, Issue 3, March 2016

Information Hiding within Image File Using Steganography Technique

[1] K.Vinay Kumar [2] N Pushpalatha, [3] Prasad B
[1]II/IV, [2][3]Associate Professor
[1][2][3] Department of CSE, Marri Laxman Reddy Institute of Technology and Management (MLRITM)
Hyderabad
[1] vinayvinnu908@gmail.com [2] pushpalatha523@gmail.com[3]bprasad@gmail.com

Abstract: **Steganography is the art and science of sending covert messages such that the existence and nature of such a message is only known by the sender and intended recipient. The process of hiding the information in other information without altering is known as Steganography. It is the art of hiding message inside a multimedia block. Attacks, misuse or unauthorized access of information is of great concern today which makes the protection of documents through digital media is a priority problem. Digital images are widely used in order to store the information. For hiding secret information in images, there exists a large variety of techniques. Some applications may require absolute invisibility of secret information, while some require 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.**

Keywords: Steganography, Hiding secret information, Intruders, Cryptography.

I. 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.

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.

Why This Steganography?

This technique is chosen, because this system includes not only imperceptibility but also un-delectability by any steganolysis tool.

II. SYSTEM ANALYSIS

Project Scope:

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.

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. So we prepare this application, to make the information hiding more simple and user friendly.

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

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.

III. METHODOLOGY

Steganography system requires any type of image file and the information or message that is to be hidden. 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. The graphical representation of this system is shown in fig1.

Encryption Process:

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 as shown in the fig 2 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.

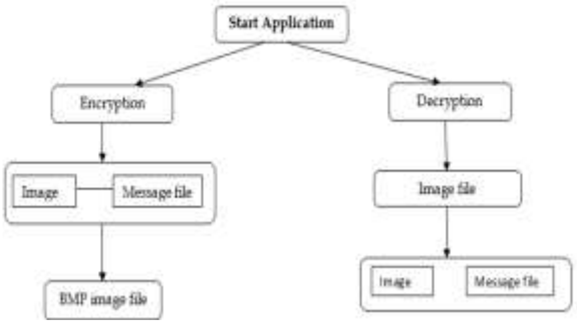


Fig 1: ***Graphical representation of the system***

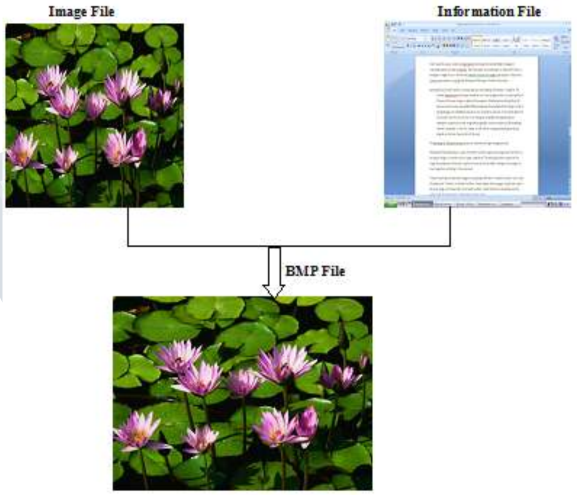


Fig 2 : Encrypt Module

Decryption Process:

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.

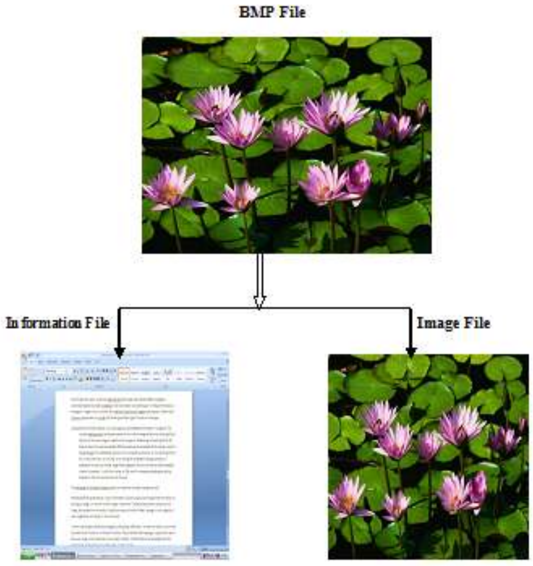


Fig 3 : Decrypt Module

IV. SYSTEM DESIGN

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.

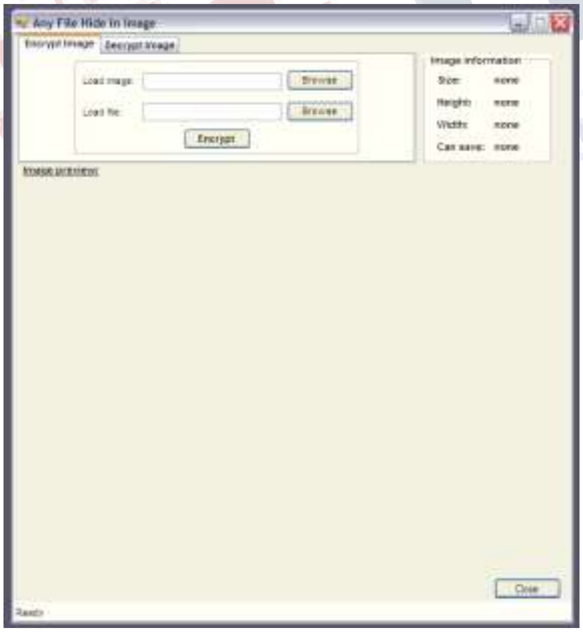


Fig 4: User Manual

Encryption:

For Encryption select Encrypt Image tab option as shown in fig 5.

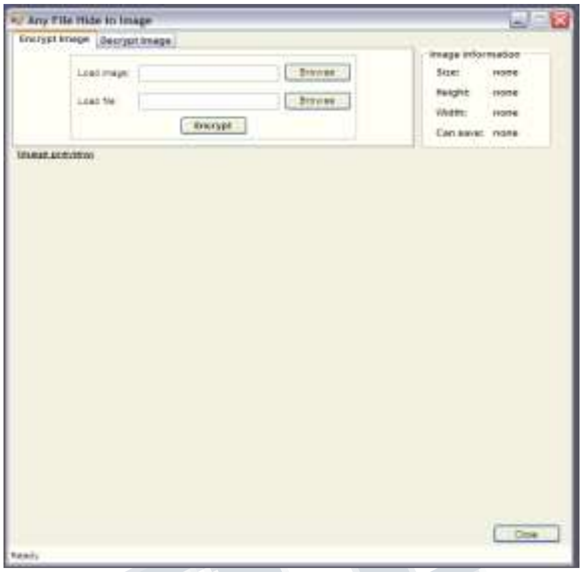


Fig 5 : Selection for Encryption

For load image as shown in fig 6 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.

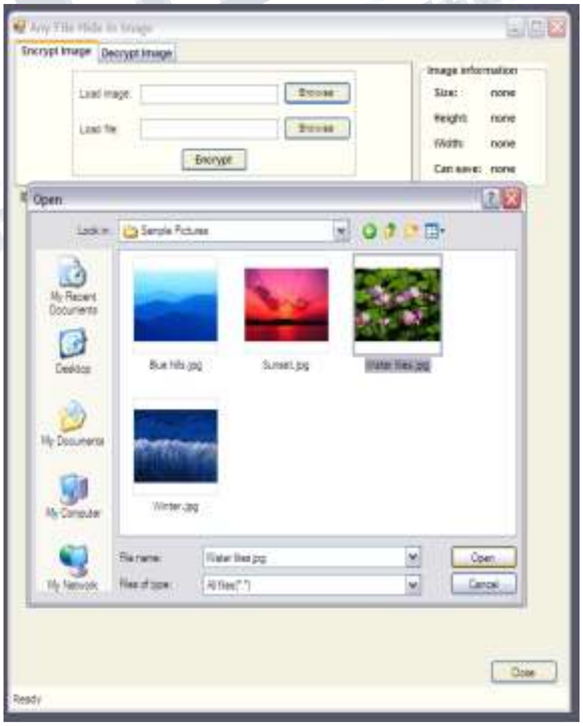
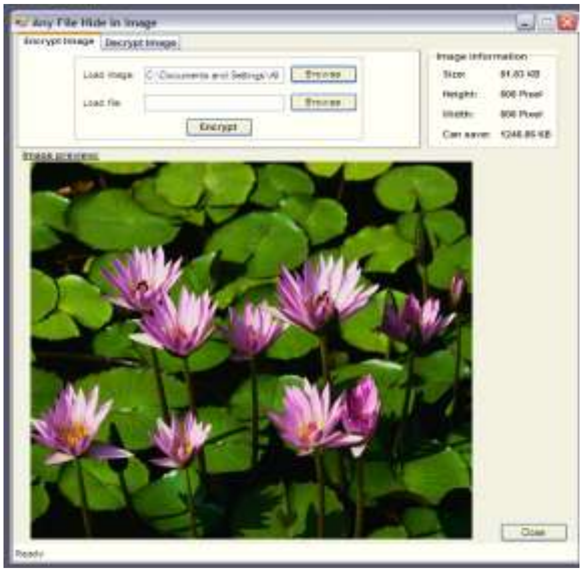


Fig 6 : Load Image

The image file will opened and is displays as shown in the fig 7. Next, click on "Browse" button that is next to the Load File textbox.



Load image: C:\Documents and Settings\All

Load file:

Image information

Size: 81.83 KB

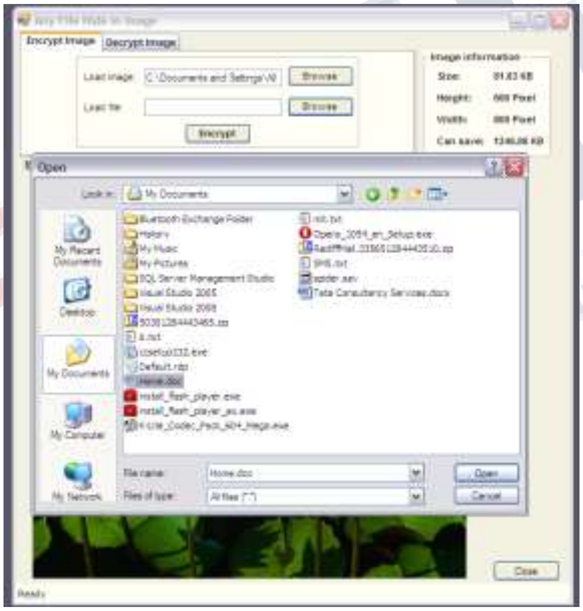
Height: 800 Pixel

Width: 800 Pixel

Can save: 1246.86 KB

Fig 7 : Load File

Again the file open dialog box will appear as shown in the fig 8, select any type of file whatever you want to hide with the image and click on ok button.



Load image: C:\Documents and Settings\All

Load file:

Image information

Size: 81.83 KB

Height: 800 Pixel

Width: 800 Pixel

Can save: 1246.86 KB

Look in: My Documents

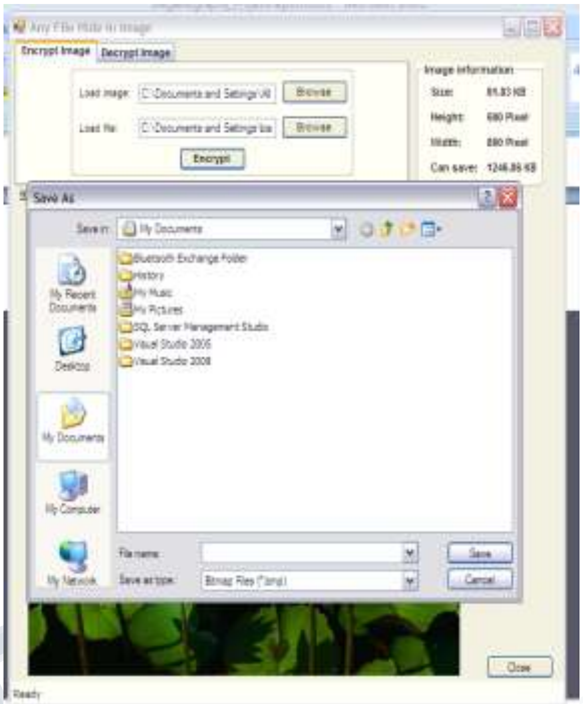
Bluetooth Exchange Folder
History
My Music
My Pictures
SQL Server Management Studio
Visual Studio 2005
Visual Studio 2008
50381284443465.zip
a.txt
cdsetup132.exe
Default.rdp
Home.doc
install_flash_player.exe
install_flash_player_ax.exe
K-Lite_Codec_Pack_404_Mega.exe
mb.txt
Opera_1054_en_Setup.exe
Rediffmail.3356512844435.10.zip
SMS.txt
spider.sav
Tata Consultancy Services.docx

File name: Home.doc

Files of type: All files (*.*)

Fig 8 : File open dialog box for hiding image

The next step is to encrypt the file. Now click on "Encrypt" button as shown in fig 9, 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.



Load image: C:\Documents and Settings\All

Load file: C:\Documents and Settings\ba

Image information

Size: 81.83 KB

Height: 800 Pixel

Width: 800 Pixel

Can save: 1246.86 KB

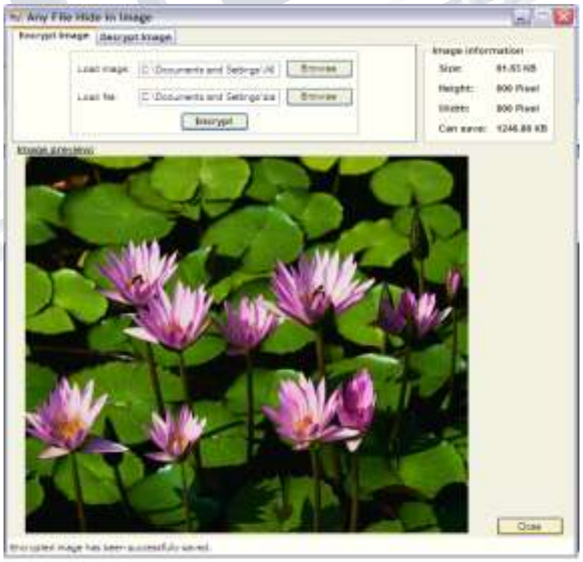
Save in: My Documents

Bluetooth Exchange Folder
History
My Music
My Pictures
SQL Server Management Studio
Visual Studio 2005
Visual Studio 2008

File name:

Save as type: Bitmap Files (*.bmp)

Fig 9 : To save the New image file and the Image file name



Load image: C:\Documents and Settings\All

Load file: C:\Documents and Settings\ba

Image information

Size: 81.83 KB

Height: 800 Pixel

Width: 800 Pixel

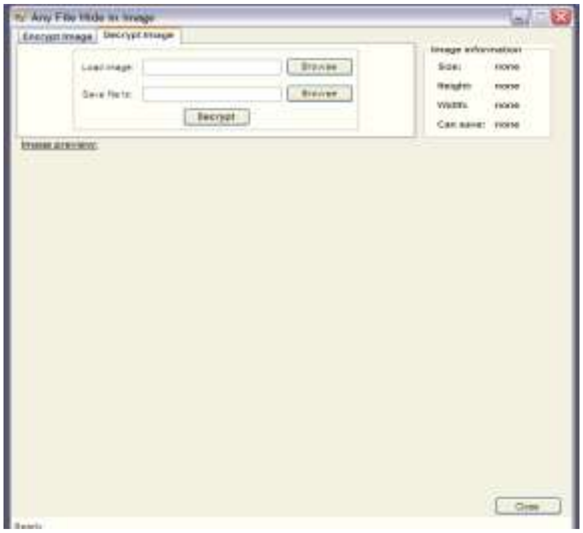
Can save: 1246.86 KB

Encrypted image has been successfully saved.

Fig 10 : Successful Saving of Image

Decryption:

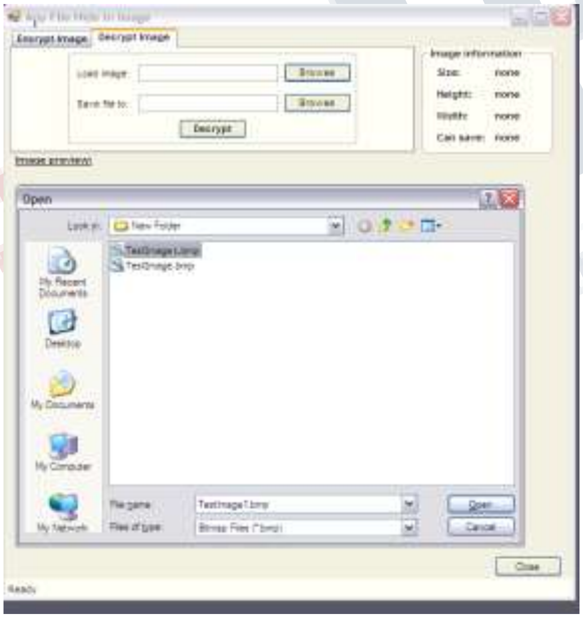
Select the Decryption Image tab option as shown in fig11.



Size: none
Height: none
Width: none
Can save: none

Fig 11 : Decryption Image tab option.

Next click on the "Browse" button as shown in fig 12, 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.



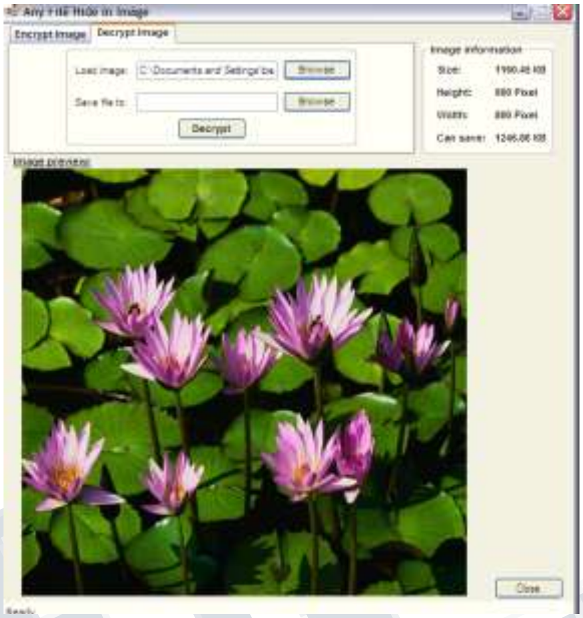
Size: none
Height: none
Width: none
Can save: none

Look in: New Folder
TestImage1.bmp
TestImage.bmp
File name: TestImage1.bmp
Files of type: Bitmap Files (*.bmp)

Fig 12 : Image selection

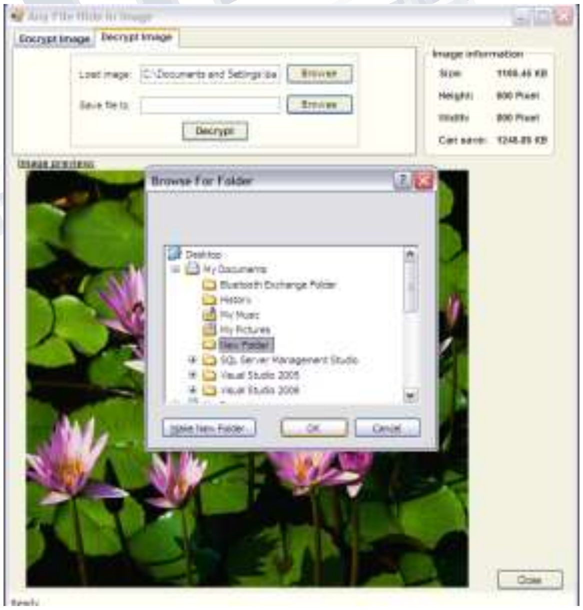
The selected image file is displayed as shown in fig 13.

Now click on "Browse" button as shown in fig 14 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.



Load image: C:\Documents and Settings\ba
Size: 1190.46 KB
Height: 880 Pixel
Width: 880 Pixel
Can save: 1246.66 KB

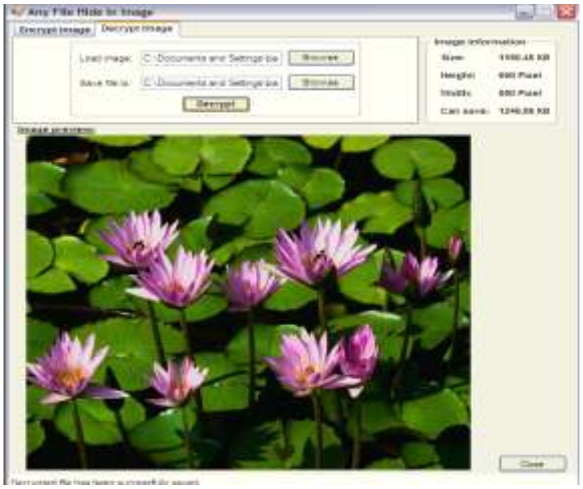
Fig 13 : Image display



Load image: C:\Documents and Settings\ba
Size: 1166.46 KB
Height: 800 Pixel
Width: 800 Pixel
Can save: 1248.89 KB

Fig 14 : Browse for folder

Now click on Decrypt button as shown in fig 15, 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.



Load image: C:\Documents and Settings\ba

Save file to: C:\Documents and Settings\ba

Size: 1100.45 KB
Height: 600 Pixel
Width: 800 Pixel
Can save: 1240.88 KB

Decrypted file has been successfully saved.

Fig 15 : Decrypt the image

V. 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] M. Chen, N. Memon, E.K. Wong, Data hiding in document images, in: H. Nemati (Ed.). Premier Reference Source–Information Security and Ethics: Concepts, Methodologies, Tools and Applications, New York: Information Science Reference, 2008, pp. 438-450.

[2] D.C. Lou, J.L. Liu, H.K. Tso, Evolution of information –hiding technology, in H. Nemati (Ed.), Premier Reference Source–Information Security and Ethics: Concepts, Methodologies, Tools and Applications, New York: Information Science Reference, 2008, pp. 438-450.

[3] Schneider, Secrets & Lies, Indiana:Wiley Publishing,2000.

[4] E. Cole, Hiding in Plain Sight: Steganography and the Art of Covert Communication, Indianapolis: Wiley Publishing, 2003.

[5] T. Jahnke, J. Seitz, (2008). An introduction in digital watermarking applications, principles and problems, in: H.Nemati (Ed), Premier Reference Source–Information Security and Ethics: Concepts, Methodologies, Tools and Applications, New York: Information Science Reference,2008, pp. 554-569.

[6] M. Warkentin, M.B. Schmidt, E. Bekkering, Steganography and steganalysis, Premier reference Source–Intellectual Property Protection for Multimedia Information technology, Chapter XIX, 2008, pp. 374-380.

[7] N.N. El-Emam, Hiding a large amount of data with high security using steganography algorithm, Journal of Computer Science 3 (2007) 223-232

[8] P.Y. Chen, W.E. Wu, A modifed side match scheme for image steganography, International Journal of Applied Science & Engineering 7 (2009) 53-60

[9] C.C. Chang, H.W. Tseng, A steganographic method for digital image using side match, Pattern Recognition Letters 25 (2004) 1431-1437

[10] P.C. Wu, W.H. Tsai, A steganographic method for images by pixel-value differencing, Pattern Recognition Letters 24 (2003) 1613-1626

[11] R. Ibrahim and T.S. Kuan, Steganography imaging system (SIS): hiding secret message inside an image, Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering and Computer Science 2010, San Francisco, USA, 2010, pp. 144-148.