International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958 (Online), Volume-9 Issue-4, April, 2020

Information Hiding using Steganography

Ritu Sindhu, Pragati Singh

Abstract: ***The process of hiding data and information is known to be steganography it is done to provide secure communication, in present world there is a demand of sending and displaying data in a hidden format especially when the exchange of information and data is taking place publically, and this is the reason because of which many methods have been proposed for data and information hiding. In this paper data and information are being hidden in digital image format, as it is mostly in demand on the internet. For data hiding there are so many techniques developed some are easy, some are bit tedious as compared to the other and all of these techniques have their own benefits, use and limitation. This paper mainly focuses to present Steganography overview, its demand, advantages and the techniques involved in it. In this paper there is also an attempt to identify which Steganography techniques are more useful and what are their requirements and also it shows which application will have more compatibility with which steganography technique.***

Keywords: Digital Image, Data hiding, Information hiding.

I. INTRODUCTION

Steganography has been derived from two greek words firstly Steganos (covered) and Graptos (Writing) that means "covered writing" which basically mean to hide data and information into a plain sight. In today's world everyone is sharing data and information with one another, the development in electronic information and data sharing gadgets and with their increased use, the data security issue has became essential. For this information and data security there have been different methods available such as Steganography, cryptography etc. People often gets confused between steganography and cryptography because both these methods are used for data and information hiding, but there is difference between these two, Steganography is a way of data and information hiding, in this method a person is not able to known that whether there is a hidden data or information is available or not, steganography basically exploits the perception of humans. The hidden data and information are not visible directly. Steganography is mainly done to hide files inside other files whereas cryptography is the way of protecting data, which can be known through decryption, the message in cryptography is given in an encrypted form, and there are encryption key which is shared between the authorized persons, by knowing this encryption key anyone can get the data and information, in cryptography there is nothing like hiding up of data it's just a way of protecting the data, no human exploitation of human sense are done in cryptography as people know that there is some information available the only trick is to get the encryption key, so as to overcome this issues steganography is introduced. Steganography involves audio, video, image, text, etc.

1.1 Steganography Mediums

There are many Steganography techniques available relying on the kind of item to be protected in a way to achieve security.

1.1.1. Image Steganography: To hide the information use of pixel intensities is done, if the cover object taken is image then it is known as image steganography.

1.1.2. Video Steganography: Digital video format is use to hide any type of information in video steganography. In this technique for hiding information in images in the video the discrete cosine transform (DCT) adjusts the value (example: 7.667 to 8), which is not conspicuous through human eye. Mp4, AVI, etc video formats are used by video steganography.

1.1.3. Audio Steganography: Audio steganography is one of the most significant medium due to demand of Voice Over Internet Protocol (VOIP). As in this technique audio is chosen for information hiding, that's why it is called Audio Steganography. WAVE,MPEG, etc. digital audio formats are used in audio steganography.

1.1.4. Network Steganography: In this technique the cover object chosen is as network protocol, such as UDP, ICMP etc and these protocols are used as carrier.

1.1.5. Text Steganography: In this technique, for information hiding, capital letters, white spaces, number of tabs and many others are used.

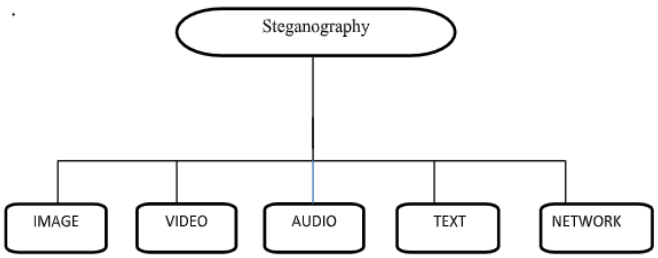


Figure 1: Different Mediums to achieve steganography

II. STEGANOGRAPHY METHODS SHOULD HAVE FOLLOWING:

a) Accuracy: Data or information gained from the medium should be reliable and accurate.

b) Volume: The data implanting volume should be maximum.

c) Strength: The data implanted must be able to survive any kind of processing action that the host signal goes through.

d) Privacy: Without the prior permission of main userwho have the password, hidden data should not release.

III. STEGANOGRAPHY STANDARDS

Revised Manuscript Received on April 25, 2020.
* Correspondence Author
Ritu Sindhu*, Senior Professor, Computer Science and Engineering department in Galgotias University, Gautam Budhh Nagar, U.P
Pragati Singh, Student B.Tech, Computer Science and Engineering department in Galgotias University, Gautam Budhh Nagar, U.P.

a) Loading Capacity: It shows the amount of hidden information that the cover image can implant in it. The rate of implantation is given in complete amount such as the secret message length.

b) Secured: A steganographic system is said to be secured when there is invisibledifference between cover image and steganographic image.

c) Cost effective: The two parameters used to figure out cost effectiveness are data hiding and data retrieval of any steganography approach.

d) Analytical Attacks: Analytical attacks are the attacks in which the embedded secret messages are extracted. The steganography algorithm used must show robustness to analytical attacks.

e) Quality: Increment in data amount decreases the quality, an appropriate amount of data and a valid approach should be done in order to not degrade the quality of data.

f) Indistinct: When the cover image and the steganographic image are not distinguished by human eye, then it is indistinguishable and perfect.

IV. THE TERMINOLOGIES USED IN IMAGE STEGANOGRAPHY ARE FOLLOWING:

1. **Covered Image:** Real image acting as a carrier for the hidden file.
2. **SteganographicImage:**The embedded information inside the cover image issteganographic image.
3. **Message:** Information which is actually hidden into images, it can be a image or a plain text.
4. **Steganographickey:**For getting the message from steganographic image, steganographic key is used.
5. **Implanting Algorithm:** For hiding the information inside the image,an algorithm is used.
6. **Detaching Algorithm:**For getting the information from stegonagraphic image, an algorithm is used.

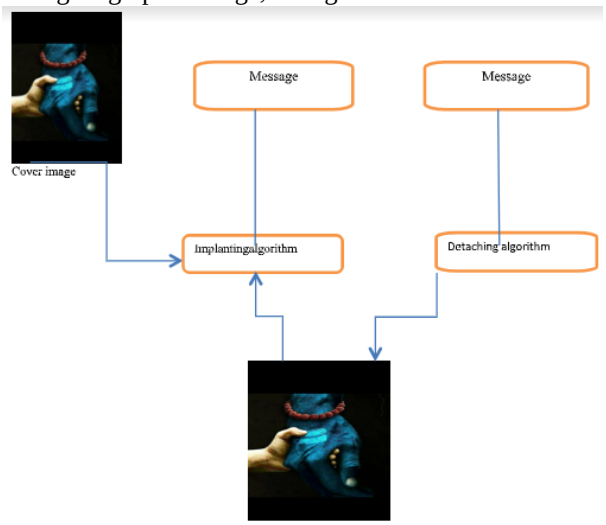


Figure 2: Steganography using Image.

Basically in an image steganography information is hidden in a cover image and this cover image results into a steganographic-image. The receiver receives the steganographic-image by a known medium and a third person involved in this processdon't even have the idea that there is a message hidden in the steganographic image. When the receiver receives the steganographic image, the message hidden in it can be known either by using steganographic key or simply without steganographickey(it depends upon the algorithm used) by the receiver. In figure 2 a diagram of digital image steganography is shown, in which steganographic key is not used, the implanted algorithm just requires the cover image and message for hiding data and information, and gives a result in the form of steganographic image, which is then send to the detaching algorithm which gives the message from the steganographic image.

V. STEGANOGRAPHY TECHNIQUES

Following are the domains in which steganography techniques are divided:

a) Frequency Domain Technique: In this technique use of various algorithms and modifications are done to hide information, it a zone of embedded methods on which number of algorithms is suggested, this technique is a bit tedious and is classified as follows:

- Discrete cosine transformation technique: For the conversion of a signal into elementary frequency components discrete cosine transform (DCT) is used.
- Discrete Wavelet transformation technique: When the wavelets are discretely sampled, it is a discrete wavelet transform (DWT).
- Discrete Fourier transformation technique: The use of this technique is done to get frequency component of every pixel value.

b) Spatial Domain Methods: In this method few bits of image pixel are directly changed in order to hide data. This technique is classified as follows:

- Pixel value differencing: In this technique a quantization range table is designed,payload is determined and maintenance of the countability of steganography is done.
- Edge based data embedding method: In this method, in an image every edge pixel is used. Firstly we calculate the masked image and identify edge pixels through canny edge detection method. In LSB bits of the edge pixel the data is hidden and receiver receives the steganographic object.
- Least significant Bit:In a string LSB is the lowest bit, it is the rightmost key in thestring, example, in the binary number: 110100101001, the far right 1 is LSB. In LSB of image, secret information is stored.
- Random pixel embedding method: This method is employed to implant and transmit steganography object.

LSB technique Benefits:

1. Quality of main image is maintained.
2. Enhancement in capacity for information storage.

LSB technique disadvantages:

1. Low strength, image data might get lost.
2. Attacks can easily destroy hidden data.

VI. BITMAP PICTURES AND IMAGE STEGANOGRAPHY

For Steganography, bitmap pictures are very popular choice for hiding secret information.

There are different kinds of software available for this; password protection is used by some of the software for encrypting information. A 'BMP' format of pictures is required for using these software, and the use of other type of pictures like "GIF", "JPEG" etc are notused because "BMP" picture algorithm for steganography are a bit easy. But on internet most of the pictures types have "JPEG"not "BPM", so there is a need for this problem.

This solution for this kind of problem is given by this software,different kind of image file can be accepted by this software for information hiding,but in end it gives "BMP" image file in which data is hidden.

Bitmap Steganography Technique:

One of the simplest type of picture is the Bitmap type as for decreasing file size it have no technologies.A bitmap image created from pixels is the structure of these files,three colors(green,red and blue say GRB) are used for pixel creation, one byte information is contained in every color of pixel and it shows the color's destiny. The colors which we see in these pictures are made by merging these three colors. 1 Byte is equivalent to 8 bit, and the first bit is calledas Most-Significant-Bit (MSB) and last bit is called Least-Significant-Bit (LSB), now here for writing security information in BMP picture we use LSB bit. Now if the (8st layer) that is the last layer of information is need to be changed then we only need to change last bits of pixel,3 bits are there in each pixel so the bits memory for writing our data is equivalent to 3*height*width. Data name and data file name should be written properly and it can be done by assigning first bit of memory.

(01110101 01010101 11101100)

(11010010 10010101 00010100)

(10110010 10011100 01101011)

3 pixels are used for saving one byte data.

Analysis of System and desigining

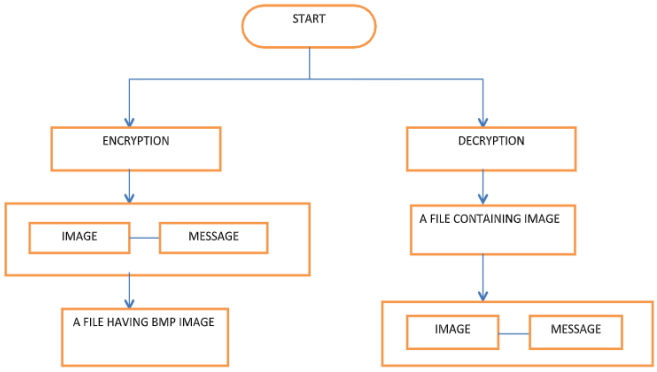
Any kind of image is taken in this system for data hiding and then encryption and decryption technique is done.

In this application the algorithm employed for encoding and decoding is several layers lieu of using only image of LSB. The beginning of data writing is from (8st or LSB layer) that is from the last layer, because this layer has least significance as comparison to other layers.

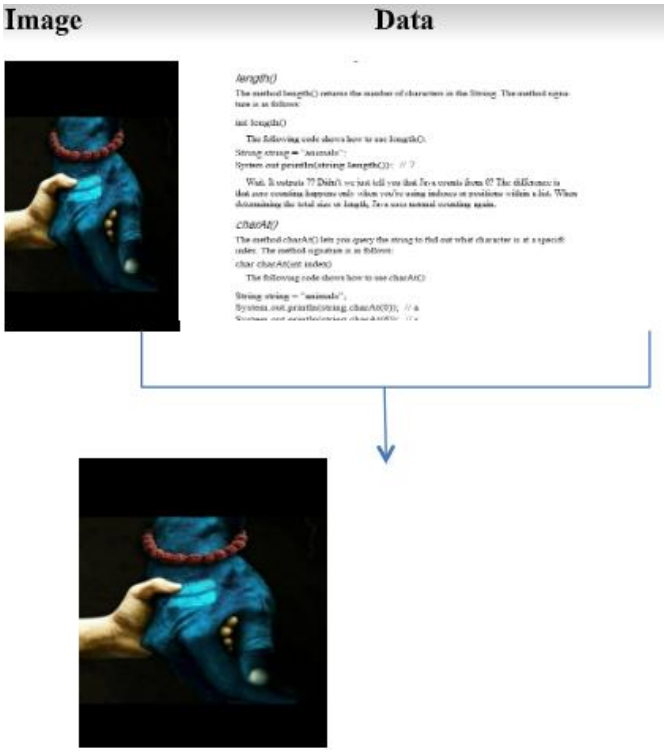
To hide file and information the encrypt module is used inside the image in a waysuch that no one is able to see that information or file. Only one image file is given in output, and also this modulecan have any type of image as input.

For having the hidden information the decrypt module is given, as output it extracts the image file and at destination folder two files are given, a hidden file(having hidden message in it) and the original image file.The name and size of file must be stored in a specified place of image before encrypting them. File information can be savedafter file information in LSB layer and save file name size and file name of image in most right-down pixels.Information is indeed needed to be written for the extraction of files from encoded to decoded state.

System's diagrammatic depiction:



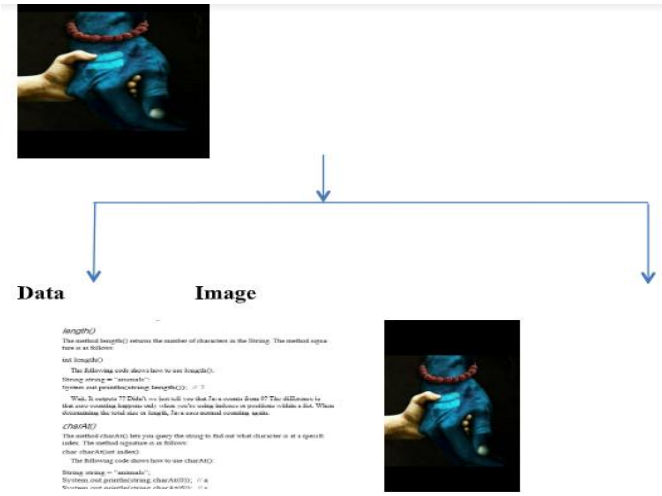
Encoding:



A BMP File

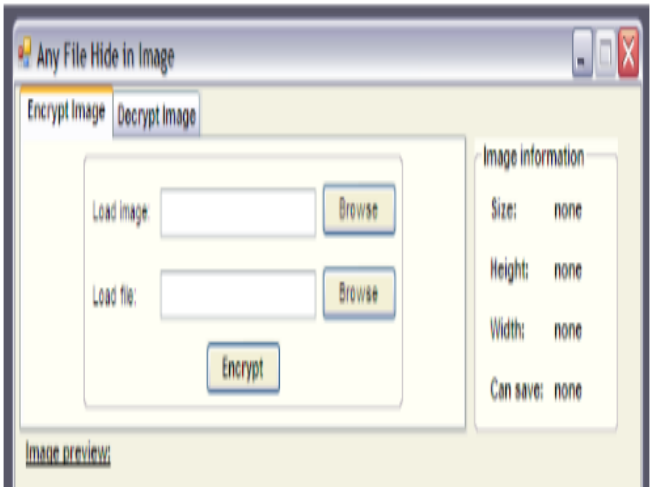
Decoding:

A BMP File



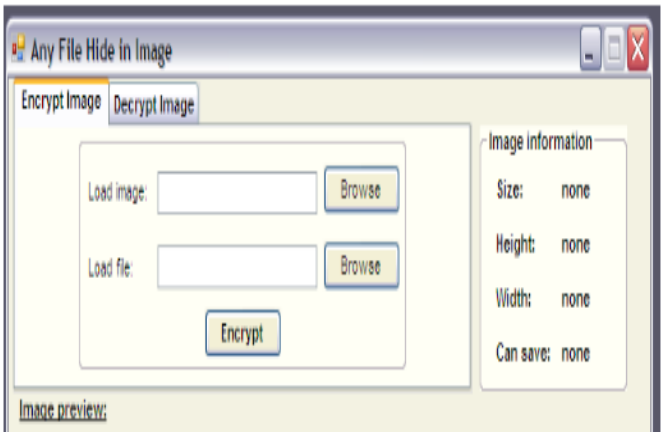
VII.RESULT ANALYSIS AND INSTRUCTIONS:

There are two tab optionon the very first screen the first oneEncrypt image for encoding and the other one decrypt image for decoding. The image information like size, height and width are displayed at top-right panel.



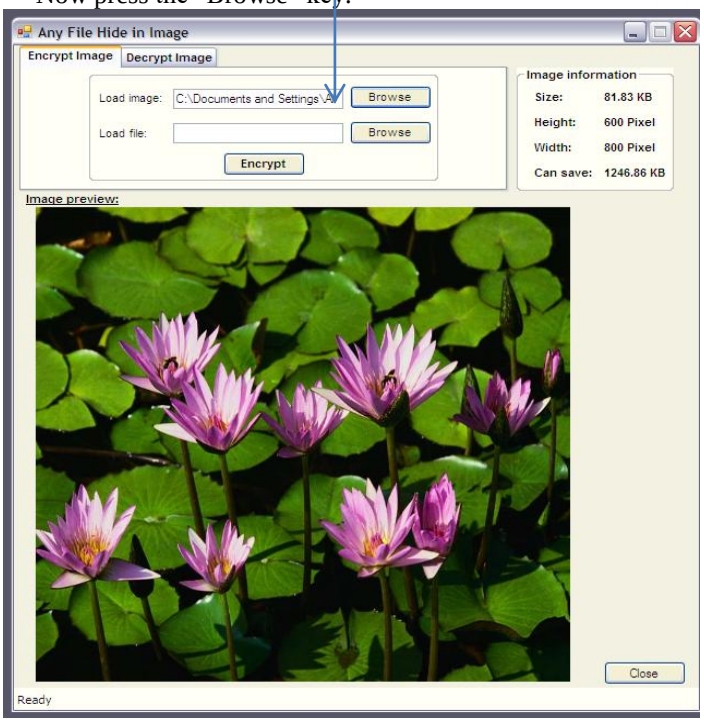
Encoding Process

1. Select Encrypt Image tab option for Encryption.

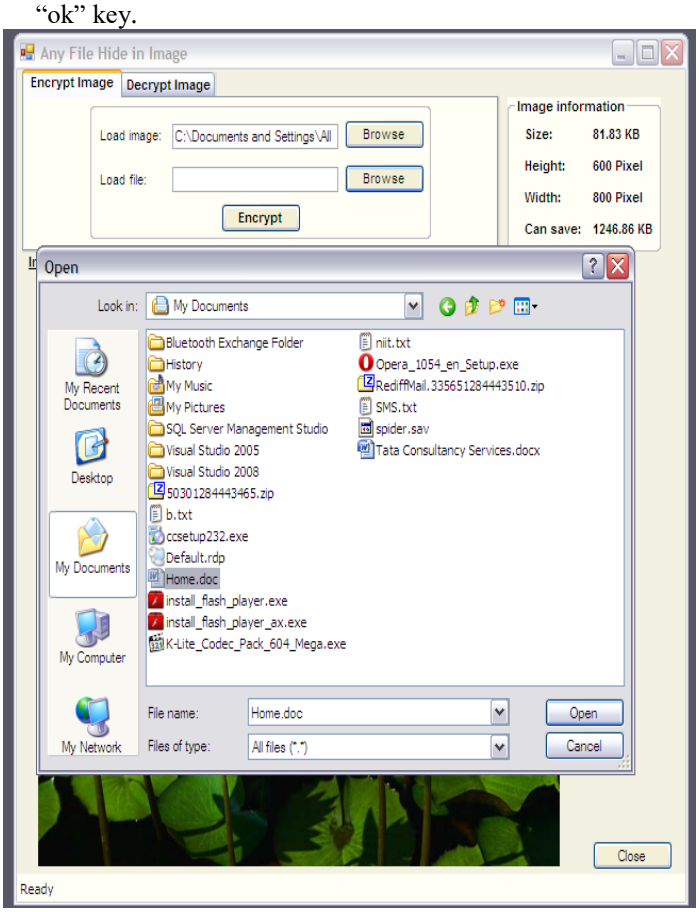


2. Next to load image textbox there is a “Browse” button,click on that buttonA open window is displayednow choose the image filein which information is going to be hidden and then press the Open key.

3. Open the image file, a window is displayed as follows. Now press the “Browse” key.



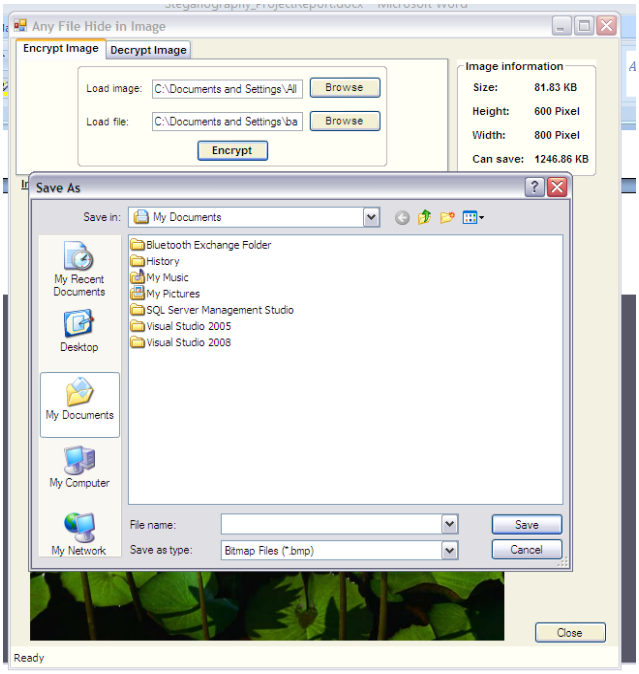
4. Open window will be displayed again, choose whatever file type you have to hide with the image and press the “ok” key.



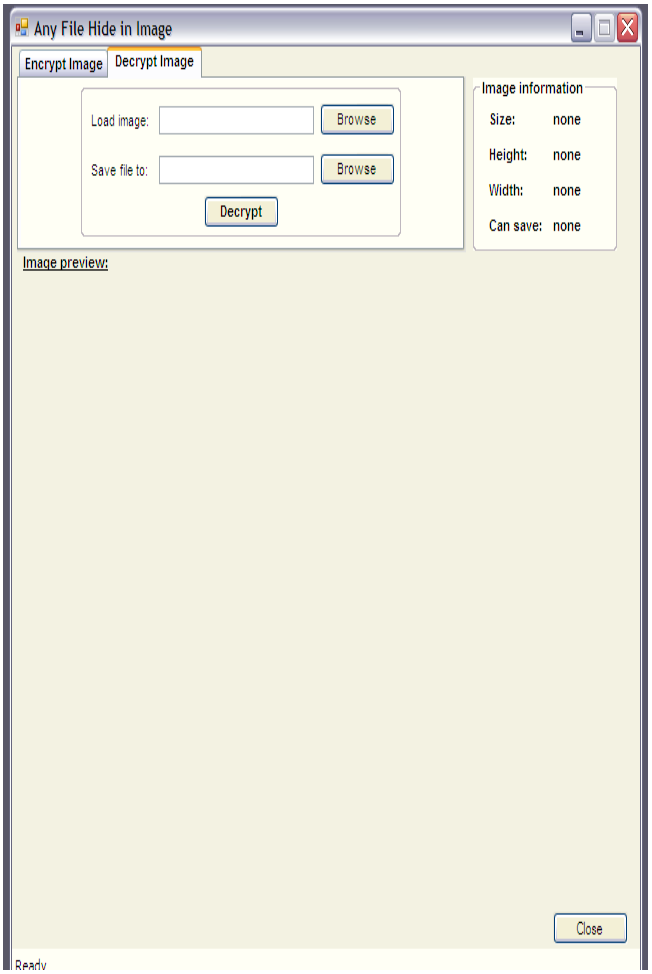
5. Encrypting file is the other step. Click onthe“Encrypt” key, a save window is displayed it will request to choose the path for saving new image file and its name. BMP is the default format for the image files.

Retrieval Number: D8760049420/2020©BEIESP
DOI: 10.35940/ijeat.D8760.049420
Journal Website: www.ijeat.org

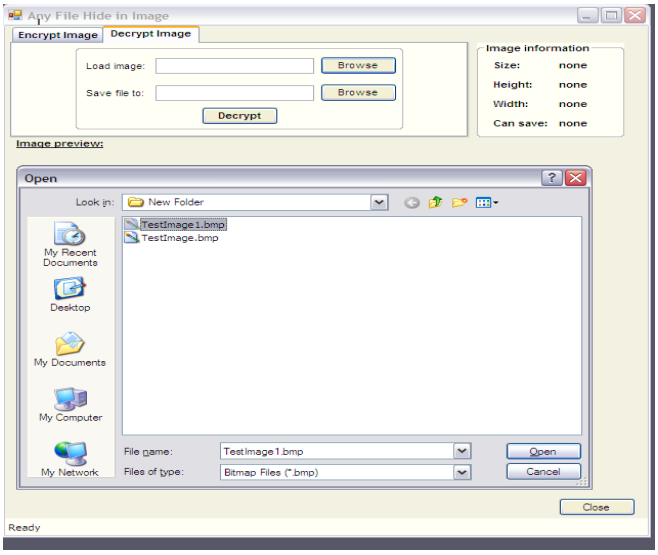
Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication



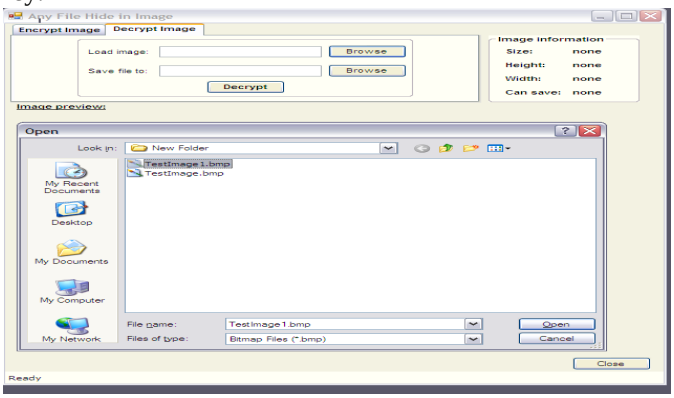
Decoding Process: Tap on the decryption tab.



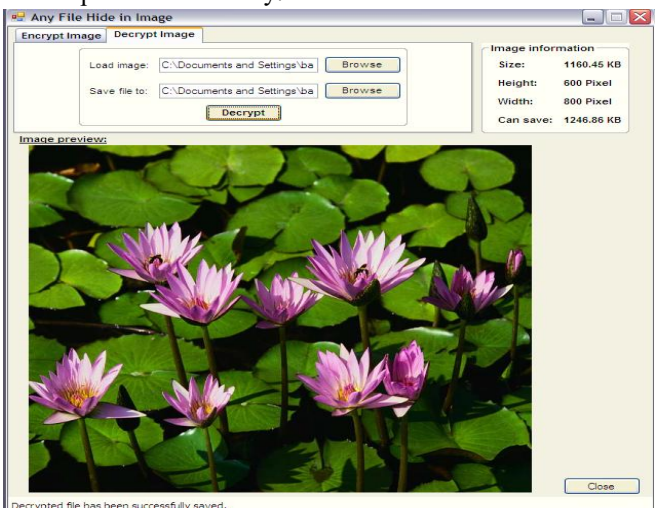
Choose “Browse” button, after choosing Browse button a Open file window will appear,now choose the encrypted image having hidden information and is encrypted. Now choose the image file and tap the Open key.



1. Now close to “Savefileto” textbox there appears “Browse” button click on that button. A dialog box “Browse for folder” will appear. The path for extraction of hidden file is selected here. Now choose the folder and press the “ok” key.

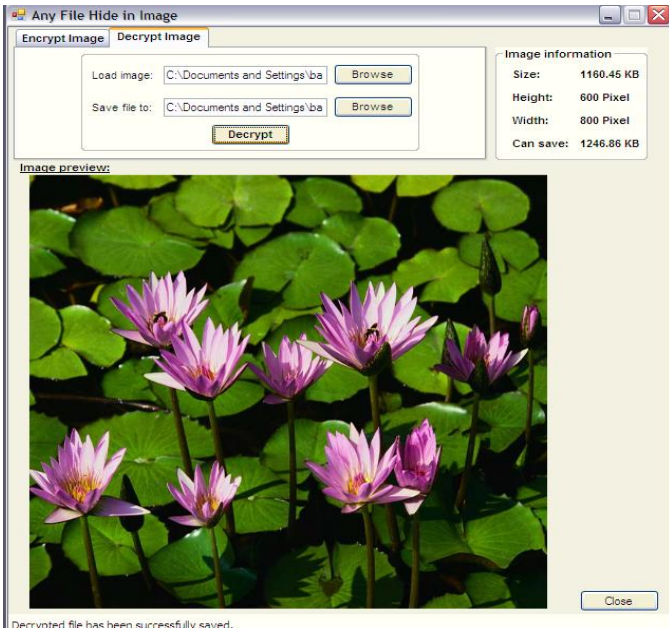


2. Now close to “Savefileto” textbox there appears “Browse” button click on that buttonA dialog box “Browse for folder” will appear. The path for extraction of hidden file is selected here. Now choose the folder and press the “ok” key.



3. For decrypting the image choose the Decrypt button, the image and the hidden file are stored inthe selected folder.

4. A successful decryption of message is displayed at screen bottom.



VIII. CONCLUSION

A survey of distinct steganography techniques, methods, standards, advantages, disadvantages and major types are givenin the paper and a method is explained which can take any kind of image file without converting it into bitmap and also using maximum memory space to hide files in pictures.

REFERENCES

1. An Overview of Different Type of Data Hiding Scheme in Image using Steganographic Techniques MukeshGarg* A.P. GurudevJangraM.Tech. Scholar H.O.D in CSE Department Jind Institute of Engineering & Technology Jind Institute of Engineering &Technol, Volume 4, Issue 1, January 2014 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Research Paper is Available online at: www.ijarcsse.com
2. International Refereed Journal of Engineering and Science (IRJES) ISSN (Online) 2319-183X, (Print) 2319-1821 Volume 6, Issue 1 (January 2017), PP.68-71, Survey Paper on Steganography Namrata Singh Computer Science and engineering ABES Engineering College, Ghaziabad A.K.T.U.
3. American Journal of Engineering Research (AJER) e-ISSN : 2320-0847 p-ISSN : 2320-0936 Volume-02, Issue-11, pp-122-128 www.ajer.org
   Steganography: A Review of Information Security Research and Development in Muslim World YunuraAzuraYunus, SalwaAbRahman, Jamaludin Ibrahim Kuliyyah of Information and Communication Technology International Islamic University Malaysia
4. International Journal of Innovative Research in Computer and Communication Engineering Vol. 4, Issue 1, January 2016,A Survey Paper on Steganography Techniques Dr. Rajkumar L Biradar1, Ambika Umashetty2 Associate Professor, Dept. of Electronics and Telematics, G. Narayanamma Institute of Technology & Science, Hyderabad, India1 Dept. of Computer Science & Engineering, Appa Institute of Engineering & Technology, Kalaburagi.
5. T. Morkel , J.H.P. Eloff and M.S. Olivier “An Overview of Image Steganography”.
6. SamerAtawneh, Ammar Almomani1 and Putra Sumari, “Steganography in Digital Images: Common Approaches and Tools,”IETE Technical Review, Vol 30, Issue 4, Jul-Aug 2013.
7. Mastering C# (Paperback), SQL Server Bible (Paperback) ,.NET Black Book (Paperback) books.

AUTHORS PROFILE

Dr.RituSindhu, She is a researcher and a senior professor in the Computer Science and Engineering department in Galgotias University, Gautam Budhh Nagar, U.P. who has published more than 60 research papers in various reputed popular journals and conferences like SCOPUS, Springer etc.

Pragati Singh, She is a final year student of B.Tech Computer Science and Engineering department in Galgotias University, Gautam Budhh Nagar, U.P.