Journal of Signal and Image Processing
ISSN: 0976-8882 & E-ISSN: 0976-8890, Volume 3, Issue 3, 2012, pp.-111-113.
Available online at http://www.bioinfo.in/contents.php?id=48

DESIGN AND IMPLEMENTATION OF IMAGE STEGANOGRAPHY

CHINCHOLKAR A.A.* AND URKUDE D.A.

Department of Computer Science, Jawaharlal Darda Institute of Engineering & Technology, Yavatmal, MS, India.
*Corresponding Author: Email- anaghachincholkar@gmail.com, amiturkude24@gmail.com

Received: April 24, 2012; Accepted: May 03, 2012

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 steganographic techniques some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of the steganography technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden. This paper intends to give an overview of design and implementation of image steganography,it uses the Microsoft visual studio.net framework as a platform where the coding is written in the c#.net and when debugged the respective output in the form of forms will be created as shown further. its uses LSB techniques to hide the data inside the image. It also attempts to identify the requirements of a good steganographic algorithm and briefly reflects on which steganographic techniques are more useful, this paper is of design and implementation of image steganography will use Microsoft visual studio.net framework for coding and later n using LSB techniques at background for encryption and decryption of message inside the image.

Keywords- capacity, security, robustness

Citation: Chincholkar A.A. and Urkude D.A.(2012) Design and Implementation of Image Steganography. Journal of Signal and Image Processing, ISSN: 0976-8882 & E-ISSN: 0976-8890, Volume 3, Issue 3, pp.-111-113.

Introduction

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message; this is in contrast to cryptography, where the existence of the message itself is not disguised, but the content is obscured. The advantage of steganography over cryptography alone is that messages do not attract attention to themselves, to messengers, or to recipients.

Steganographic messages are often first encrypted by some traditional means and then a covertext is modified in some way to contain the encrypted message, resulting in stegotext. For example, the letter size, spacing, typeface, or other characteristics of a covertext can be manipulated to carry the hidden message; only the recipient (who must know the technique used) can recover the message and then decrypt it. Steganography uses in electronic communication include steganographic coding inside of a transport layer, such as an MP3 file, or a protocol, such as UDP.

The paper 'Steganography' provides means for secure data transmission and secure data storage network. Hereby, important files carrying confidential information can be stored in the server in an encrypted form. Access to these files is limited to certain authorized people only. Transmission also takes place in an encrypted form so that no intruder can get any useful information from the original file during transit. Further, before trying to access important files, the user has to login to the system using a valid username and password, which is allotted to him by the system administrator.

Objectives

The paper has the following objectives-

- To create a tool that can be used to hide data inside a 24 bit color image.
- The tool should be easy to useand should use a graphical user interface.
- The tool should work cross-platform.
- The tool should effectively hide a message using an image degradation approach and should be able to retrieve this message afterwards.
- The tool should take into account the original content, to theoretically more effectively hide the message.
- The tool should be able to provide some information as to the effectiveness of the hiding i.e. it should be able to evaluate the degradation of an image. The analysis used will consist of existing watermarking measures, re- implemented for this tool.
- The technique should fall under the category of Secret Key Steganography -where without the key the hidden message cannot be retrieved.
- The tool should be able to encrypt the message before embedding it.

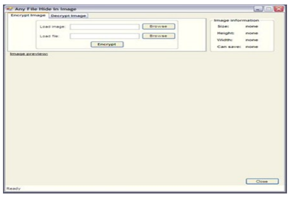
Related work

The paper 'Steganography' provides means for secure data transmission and secure data storage network. Hereby, important files carrying confidential information can be stored in the server in an encrypted form. Access to these files is limited to certain authorized people only. Transmission also takes place in an encrypted form so that no intruder can get any useful information from the original file during transit. Further, before trying to access important files, the user has to login to the system using a valid username and password, which is allotted to him by the system administrator.

As shown in the experimental results of implementation of image steganography we had provided the coding in Microsoft visual studio.net framework in c#.net and the forms shown in the figures 1 to 11 respectively will be created when we will debug the code from the c#.net file. and further shown in figure 1 it is the encryption phase of the image steganography.as shown in figure1 it ask for the path of the image to browse by clicking on browse button where the particular message is to be hidden. further shown in the figure 2 the image folder will opened when clicked on browse button from where the image is to be selected and loaded into the load image section, further in figure 3 the image preview will be shown. Also we have to provide the path for the doc, text file to be hidden into the respective image in the load file section.and as the file is loaded in the particular section click on open as shown in figure 4.then the next form will get appeared and we have to click on encrypt button and then it will ask us for the location where the image with the hidden message to save shown in figure 5.when clicked on save button on figure 5, the message ”encrypted image has been successfully saved ” will appear shown in figure 6 form with the respective image.

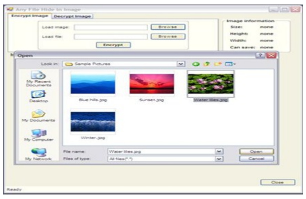
Then the next phase is the decryption phase here the message is to be decrypted from the image will done. As shown in figure 7 form we have to click on decrypt image menu and then the ‘load image’ and ‘save file to’ sections ares provided. shown in figure 8 the testimage1.bmp (bitmap image) image path is provided from which we have to decrypt the message, then we have to provide the folder where the file is to be stored by providing the address of the particular folder in the ‘save file to’ section in the form of figure 9 then click on browse then the destination folder will be asked where the image file to be saved,click on ok button to save the image in the destination folder shown in figure 10.Finally click on the ‘Decrypt’ button then the message will appear “decrypted file has been successfully saved”.

Implementation of image steganoghraphy
Experimental Results



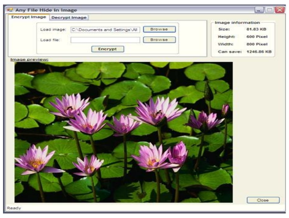
Size: none
Height: none
Width: none
Can save: none
Ready

Fig. 1-



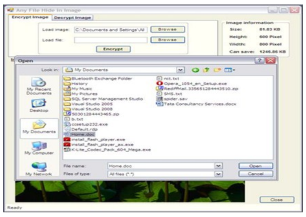
Size: none
Height: none
Width: none
Can save: none
File name: Water lilies.jpg
Files of type: All files(*.*)
Ready

Fig. 2-



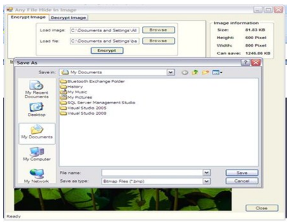
Load image: C:\Documents and Settings\All
Size: 81.83 KB
Height: 600 Pixel
Width: 800 Pixel
Can save: 1246.86 KB
Ready

Fig. 3-



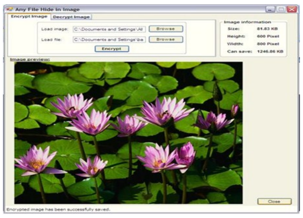
Load image: C:\Documents and Settings\All
Size: 81.83 KB
Height: 600 Pixel
Width: 800 Pixel
Can save: 1246.86 KB
File name: Home.doc
Files of type: All files (*.*)
Ready

Fig. 4-



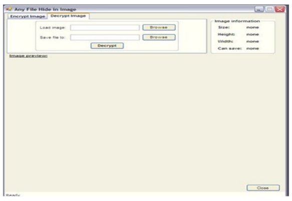
Load image: C:\Documents and Settings\All
Load file: C:\Documents and Settings\ba
Size: 81.83 KB
Height: 600 Pixel
Width: 800 Pixel
Can save: 1246.86 KB
Save as type: Bitmap Files (*.bmp)
Ready

Fig. 5-



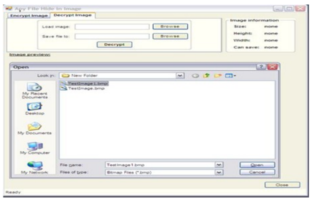
Load image: C:\Documents and Settings\All
Load file: C:\Documents and Settings\ba
Size: 81.83 KB
Height: 600 Pixel
Width: 800 Pixel
Can save: 1246.86 KB
Encrypted image has been successfully saved.

Fig. 6-



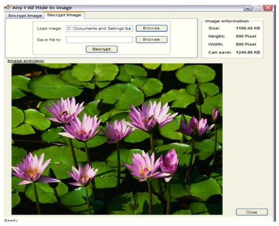
Size: none
Height: none
Width: none
Can save: none
Ready

Fig. 7-



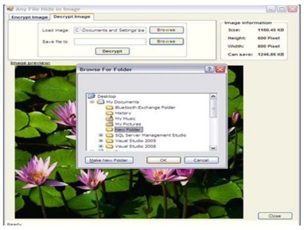
Size: none
Height: none
Width: none
Can save: none
File name: TestImage1.bmp
Files of type: Bitmap Files (*.bmp)
Ready

Fig. 8-



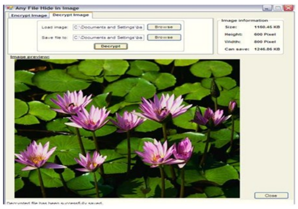
Load image: C:\Documents and Settings\ba
Size: 1160.45 KB
Height: 600 Pixel
Width: 800 Pixel
Can save: 1246.86 KB
Ready

Fig. 9-



Load image: C:\Documents and Settings\ba
Size: 1160.45 KB
Height: 600 Pixel
Width: 800 Pixel
Can save: 1246.86 KB
Ready

Fig. 10-



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

Image information
Size: 1160.45 KB
Height: 600 Pixel
Width: 800 Pixel
Can save: 1246.86 KB

Decrypted file has been successfully saved.

Fig. 11-

Application

- Image Steganography has many applications, especially in today's modern, high-tech world. Privacy and anonymity is a concern for most people on the internet.
- Image Steganography allows for two parties to communicate secretly and covertly. It allows for some morally-conscious people to safely whistle blow on internal actions. One of the other main uses for Image Steganography is for the transportation of high-level or top-secret documents between international governments.
- While Image Steganography has many legitimate uses, it can also be quite nefarious. It can be used by hackers to send viruses and Trojans to compromise machines and also by terrorists and other organizations that rely on covert operations to communicate secretly and safely.
- Image Steganography also used in military purpose for transporting important data.

Conclusion

Steganography is not a threat in general and Steganography is hardly something that is used by Terrorists and I seriously doubt that it will be used by Terrorists. I think that Steganography is a potential threat. However I do not believe it will be used for purposes that are being pushed by the media. The most probable use of Steganography is probably to hide illegal material such as child pornography. I believe that Steganography may also be used to hide sensitive information and transfer it from one place to another. For example a foreign military may have a double agent working inside the US Military, the agent steals some sensitive documents and he wants to copy them onto CD to take home and email to his superiors. He knows that if he burns the documents to the disk there is a disk of the disk being checked. So what could he do? Simple, hide the documents inside picture files that look nothing out of the ordinary. People should be focusing on the important aspects of Steganography, such as what it is really used for, instead of believing propaganda put out by the media.

References

[1] Ahsan K. and Kundur D. *Practical Internet Steganography: Data Hiding in IP* http://www.ece.tamu.edu/~deepa/pdf/txsecwrksh03 pdf.

[2] Anderson R.J. and Petitcolas F.A.P. (1998) *J. Selected Areas in Comm.*, 16 (4) 474-481.

[3] Curran K. and Bailey K. (2003) *International Journal of Digital Evidence.*

[4] Chapman M., Davida G. and Rennhard M. *A Practical and Effective Approach to Large-Scale Automated Linguistic Steganography* <http://www.nicetext.com/doc/isc01.pdf>

[5] Dai Y., Liu G. and Wang Breaking Z. (2006) *International Journal of Computer Science and Network Security*, 6 (3b).

[6] Fidrich J., Golijan M. and Du R. *Reliable Detection of LSB Steganography in Color and Grayscale Images*,

[7] <http://www.ssie.binghamton.edu/fridrich/Research/acmwrkshp_version.pdf>

[8] Handel T. and Sandford M. (1996) *International Workshop on Information Hiding*.

[9] Herodotus (1996) *The Histories, Penguin Classics*.

[10] International Telecommunication Union (1992) *Information Technology - Digital Compression and Coding of Continuous-Tone Still Images - Requirements and Specifications Recommendation T.*81.

[11] Jackson J. T., Gregg H., Gunsch G. H., Claypoole R. L. and Lamont G. B. (2003) *International Journal of Digital Evidence.*

[12] Johnson N. *Digital Image Steganography and Digital Watermarking Tool Table.* http://www.jjtc.com/Steganography/toolmatrix.htm