IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 3, Ver. II (May-Jun. 2016), PP 38-43
www.iosrjournals.org

A Technique To Hide Information Within Image File For Secure Transmission

Anita Khanal[1], Anup Pradhan[2], Mingur Namgyal Gurung[3], Rinchen Doma Bhutia[4] Rajeev Sharma[5]
[1,2,3,4,5] *Department Of Computer Science And Technology*
Centre For Computers And Communication
Chisopani, South Sikkim, India

Abstract:- *In today's world lots of data are being corrupted so, for a secure message transfer we need Steganography .It is the method of hiding information in other information. Other file formats such as of audio or video format can also be used, but because of their frequency on the internet, digital images are more popular. There are variety of steganography technique that are used for hiding secret information and are more complex than others while 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 use and techniques. It also helps to choose which stegnographic technique are suitable for which application and also attempts to identify the requirements of a good steganography algorithm.*
Keywords*: - Steganography, Cryptography, plain text, encryption, decryption, transposition cipher.*

I. Introduction

The use of steganography is the solution to the problem of information being leaked by the intruders. One solution to this problem is, through the use of steganography.]It is a technique of hiding information in digital media. In contrast to cryptography, rather than keeping others from knowing the hidden information, it is to keep others from thinking that the information even exists.

Steganography becomes more valuable as more people join the cyberspace revolution. Steganography is the way of concealing information in manner that prevents the detection of hidden messages. It 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 for the information and data has become an important issue. Besides cryptography, steganography can also be employed to keep information more secure. In cryptography, before passing message through the network, the encrypted message is embedded in a digital host, keeping the existence of the message 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 need of special means of security especially on a computer network is growing due to the growth in modern communication. As the number of data /information exchange on the internet increases, the importance of network security is increasing. Therefore, for the protection against unauthorized access and use of data, the confidentiality and data integrity are require. Thus it 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.

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.

II. Literature Survey

Privacy must be kept secure at all cost. Information security is the factor that keeps information safe and protects the systems and hardware that use, store, and transmit that information. Information security can be defined as measures adopted to prevent the unauthorized use or modification of applied data or capabilities.

A. Steganography vs. Watermarking

Steganography focus on the degree of invisibility while watermarking pay most of its parameters to the robustness of the message and its ability to withstand attacks of removal, such as image operations, audio operations in the case of images and audio files being watermarked respectively.

It is a non-questionable fact that delectability of a vessel with an stenographic message or a watermark is a function of the changeability function of the algorithm over the vessel.

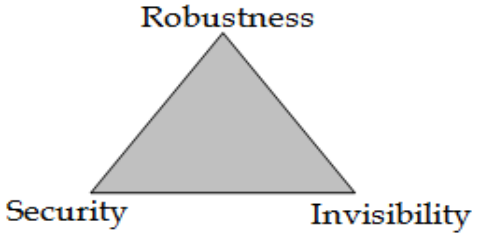

Fig 1: A typical triangle of conflict.

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

Invisibility, Robustness, and Security are a typical triangle of conflict. Invisibility can be define as the amount of the notability of the contents of the message within the vessel. Security is similar to the cryptographic idea for message security, which means inability of reconstruction of the message without the proper secret key material shared.

Robustness refers to the durability of the message to survive disturbance or to remove attacks intact. It is usually used in the watermarking field since watermarking seems to have 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 and the less robust it is. Whereas, if the more robust the message is embedded then, the more size it requires and also the more visible it is.

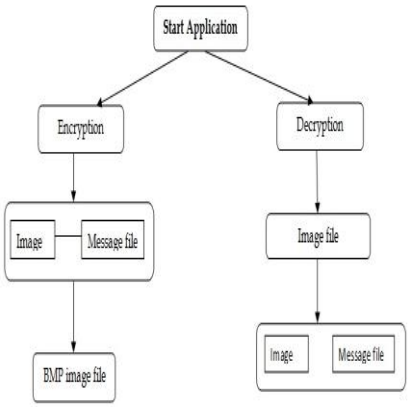

Fig 2: The graphical representation the system.

B. Detecting Steganography

Steganalysis is the art of detecting Steganography . It involves identifying the use of Steganography inside of a file. It does not deal decrypt the hidden information inside of a file, rather it just discover it.

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

"Selecting and comparing the image file with the other image file. Multiple copies of images are on the internet, so one can try and compare the image file that look suspicious. For example, if you download a PNG image and your suspect file is also a PNG image, both the files may look almost similar apart from the fact that one is larger and blur than the other one, thus it is most obvious that your suspect file has hidden information/data inside of it.

III. Proposed System

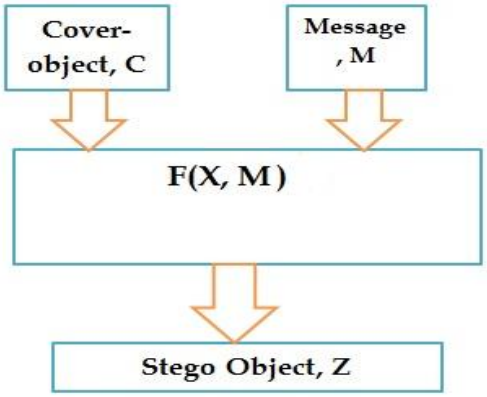

Fig.3: The model for steganography

The proposed system for steganography is friendly user interface where the user needs to specify or select the inputs which may be text, audio or any other file. After the operation(extracting or embedding) is done, the user can open or just save the output of that particular operation according to their own wish. As for security to avoid an intruder to extract the embedded data, a security key is used while extracting and embedding message (data).

Least significant bit(LSB)is the simplest process to embed message in a digital file. LSB coding also allows a huge amount of data to be encoded, by substituting the LSB of a each single point with a binary message. The normal data transmission rate in LSB coding is 1kbps per 1 kHz.

However, in some cases of LSB coding, one or more than one least significant bit are replaced with two message bits. This may result in the increase of amount of data that can be encoded whereas, it also increases the amount of disturbance in file as well.

IV. Methodology Used

The method used to hide the information in the cover file is LSB Bit Substitution Technique.

Using this approach, the least significant bits of information that determine the meaningful content of the original file can be replaced with new data in a way such that causes the least amount of distortion.

The advantage of using this method is that the cover file size does not change after the execution of the algorithms.

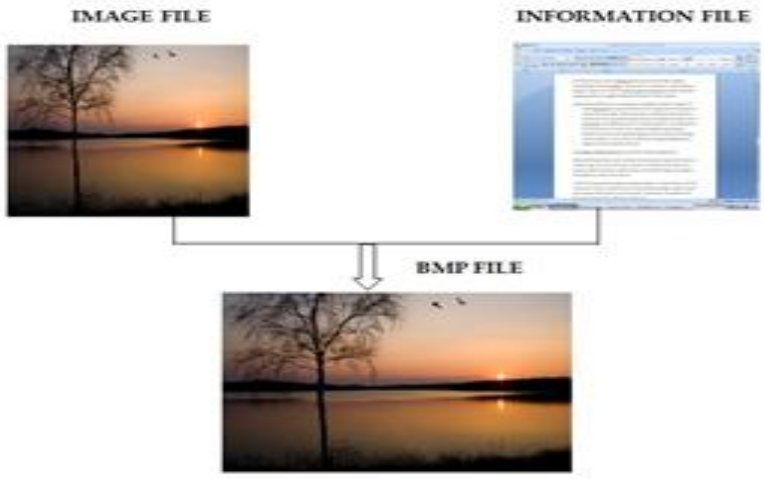

Fig 4: Process of encryption

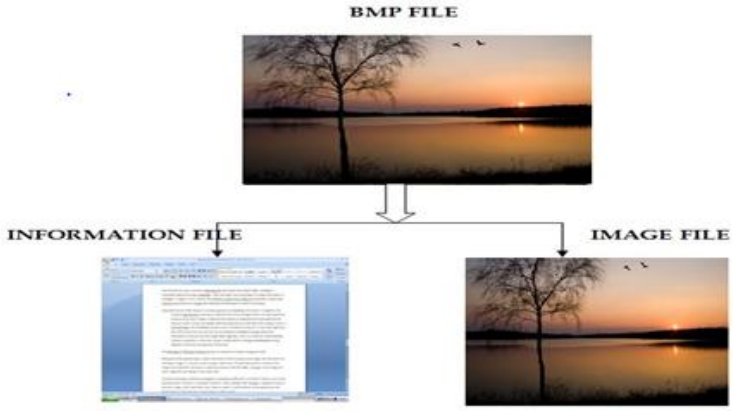

Fig 5: Process of decryption

V. procedure

The fig 6 given below which has two tab options – one is for encryption and another is for decryption. In the right side, top panel shows the information about the size, height, and width of the image.

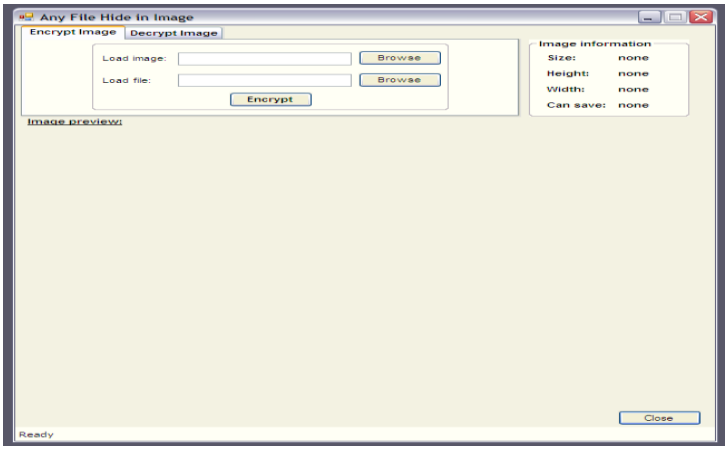

Fig6: Tab option for encryption and decryption

A. Encryption

1. Select encrypt image from tab option for the encryption process.
2. For selecting the image, click on browse. The dialog box will appear. Then, select the Image file, which you want to use hide information and click on Open button.
3. The image file will open and will be displayed as given below. Next, click on "Browse"

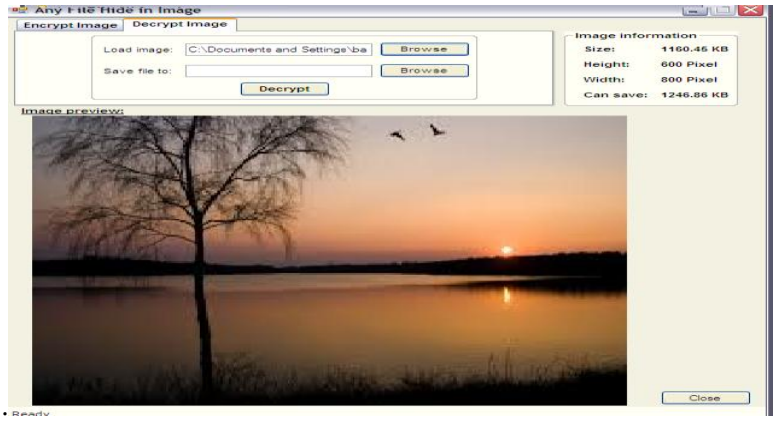

Fig7: Encryption

4. Again the same dialog box will appear, now select the type of file you want to hide within the image and then, click on ok button.
5. Click on "Encrypt" button, to encrypt the file. The save dialog box will appear, then select the path to save the New image file and the Image file name.

B. Decryption

1. Select the Image tab option for decryption process.
2. Click on the "Browse" button, to open the dialog box, now select the image which is Encrypted. Select the image file and click on Open button.
3. The image displayed as follows:

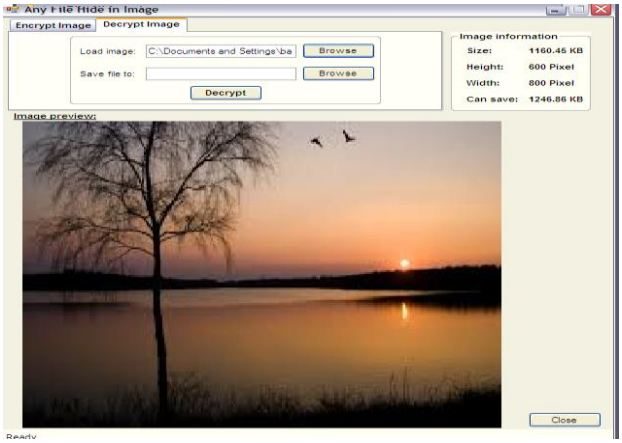

Fig8: Decryption

4. Now click on "Browse" button. It will open a dialog box i.e. for browsing a folder. Then, select the path or folder, where you want to extract the hidden file. Select the folder and click on Ok button.
5. Now click on Decrypt button, to decrypt the image. Then the hidden file and image file will be saved into a selected folder. The alert or message for successful decryption will be displayed on the status bar.

VI. Analysis

A. Image size

The size of an image file, is, directly related to the number of pixels it contains and the granularity of the color definition. A image of 640*480 pix, using a palate of 256 colours would require a file about 307 KB in size (640*480 bytes) whereas a image having high-resolution of 1024*768 pix and 24-bit color would result in a 2.36MB file(1024*768*3 bytes).

B. Cover Image

The cover image should be in Graphic Interchange Format (GIF), Bitmap (BMP) and Joint Photographic Experts Group (JPEG). GIF and 8-bit BMP file allows the software to reconstruct the original image, know as lossless compression.

Table1. PSNR comparison for the proposed System

Size of *Image*	Original Image	Stego Image	PSNR
200X200			89
300X300			91
500X500			92

PSNR or Peak-Signal-To-Noise –Ratio is an term used by the engineers for the ration between the power of corrupting noise that influence its representation and the maximum possible power of a signal. The signal in case is the real data and the corrupted noise is an error introduced by algorithms.

When comparing image PSNR is an approximation to human perception. A higher usually indicates that the reconstruction is of better quality. It is valid only when it is used for the corruption of a result from the same content and data. MSE or Mean Squared Error
can be used for defining PSNR. In a given method K, MSE is defined as:

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

$$\begin{aligned} PSNR &= 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right) \\ &= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \\ &= 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE) \end{aligned}$$

VII. Conclusion

The Steganography is an interesting subject and outside of the mainstream cryptography and system administration that most of us deal in day to day life. Steganography can be used for hiding information. We used the LSB technique to provide a means of secure communication. A stage-key has been applied to the system during embedment of the message into the cover image. This steganography application software is provided for the purpose to hide any type of files in the host file. The application supports any file format of an image, without converting it to any other format. Since ancient times, man has found a desire in the ability to communicate covertly. The recent research in watermarking is evidence that, beside military use or espionage application, steganography can be used in other areas where hiding of data or information security is required. Steganography, like cryptography, will play an major role in the future of secure communication in the "digital world" because of its unique properties of encrypting and decrypting of information.

Reference

[1]. N.F. Johnson and S.C. Katzenbeisser, "A survey of steganographic techniques", in: S. Katzenbeisser and F.A.P. Petitcolas, (ed.) (2000) Information hiding techniques for steganography and digital watermarking, Norwood: Artech House, INC.

[2]. N. Johnson and S. Jajodia. Steganalysis of images created using current steganography software. Workshop on Information Hiding, 1998.

[3]. N. Johnson and S. Jajodia. Exploring Steganography: Seeing the Unseen. Computer, vol. 31, no. 2, pp. 2634, 1998.

[4]. K. Lee, A. Westfeld, and S. Lee. Generalised category attack: improving histogram-based attack on jpeg lsb embedding.In Proceedings of the 9th international conference on Information hiding, IH'07, pages 378–391, Berlin, Heidelberg, 2007.Springer-Verlag.

[5]. E. T. Lin and E. J. Delp. A review of data hiding in digital images. Proceedings of the Image Processing, Image Quality, Image.Fridrich ,J, M. Goljan, and R. Du, ―Detecting LSB steganography in color and grayscale images,‖ IEEE Multimedia Special Issue on Security, pp. 22–28, October- November 2001.

[6]. S.B. Sadkhan, Cryptography: Current status and future trends, in: Proceedings of IEEE International Conference on Information & Communication Technologies: From Theory to Applications, Damascus. Syria, April 19-23, 2004, pp. 417-418.

[7]. T. Morkel, J. H. P. Eloff, M. S. Olivier, "An Overview of Image Steganography", Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria, SA.

[8]. C. C. Lin andW. H. Tsai, "Secret image sharing with steganography and authentication," Journal of Sys- tems and Software, vol. 73, pp. 405–414, Nov. 2004.