International Journal of Computational Intelligence Research
ISSN 0973-1873 Volume 13, Number 10 (2017), pp. 2289-2295

http://www.ripublication.com

Steganography for Secure Data Transmission

Niveditha Shetty

Department of Computer Science,
NMAM Institute of Technology, Nitte. India.

Abstract

Information security is an essential factor while transmitting secret information between two entities. The methods used for this purpose are Steganography and cryptography. Although Cryptography scrambles the information, it discloses its existence. Steganography hides the existence of the secret information. In steganography the secret message to be communicated is embedded within a carrier, hence it is hidden from the malicious users. In this work a combination of Cryptography and Stegonography technique is proposed to hide the secret data in a carrier such as image, audio or video file.

Keywords: Steganography, Cryptography, Encryption, Decryption

INTRODUCTION:

Steganography can be defined as the study of embedding sensitive information in another medium known as the cover medium. It is just as old as cryptography[8]. Steganography involves hiding of the information to avoid detection of the secret information. The objects used to hide the secret information are called cover objects. The hidden information plus the cover object is known as stego object. The cover object can be multimedia files such as audio, video or image file. Images are popularly used as cover objects. Gary scale images or color images can be used as cover objects. Color images steganography is more popular than grey scale image steganography as it has more space for data hiding. HSV(Hue, Saturation, Value), RGB(Red, Green, Blue) are few formats in which the color images can be represented[1]. MP3, WAV file formats are among the various file formats used to

store audio files. MP3 is the most commonly used audio file format. M.I Khalil is one among the few researches who chose to hide an audio file in an image. He embedded a short audio message in the least significant bits of all the bytes in a pixel[2].Many algorithms have been introduced in Steganography to safeguard the sensitive information regarding research, work politics, military etc. Literature survey indicates that there is a huge scope for development in audio encryption[7].

Ki-Hyun Jung et.al worked on increasing the image quality and payload capacity in steganography using techniques such as edge detection and image interpolation[3]. Ali Kanso et.al used steganalytic attacks such as RS attack, Histogram test, PSNR test to test his algorithm used for steganography[4]. Dr Dinesh Singh and Taruna suggested a technique using keyless randomization to embed sensitive data in variable and multiple LSB's[9]. Text steganography is a method in which secret information is hidden in the nth character of each word in a text message. Text steganography is not very trendy, as text files have very less redundant data[10]. Images provide an excellent medium for data hiding. The more comprehensive an image, lesser constraints there are on how much information it can embed before it becomes a suspect. The packages such as JPHide/JPSeek use the coefficients in a JPEG to conceal secret information[8].

Another technique is used in which information is embedded in visually insignificant areas of the image. Nevertheless, image degradation can be explored using different images and messages of different lengths. An alternative approach which is specific to GIF images is to manipulate the image's palette so as to hide information. The image itself is not altered in any noticeable way using GifShuffle, rather Gifshuffle permutes the GIF image's color map, keeping the original image fully intact.

In this work an attempt is made to develop a system which provides multilayered security for secure data transfer. LSB coding is used to embed secret information in the cover objects such as image, audio or video file. In LSB coding the least significant bit of each sampling point is substituted with a binary message. Ideal data transmission rate of 1kbps per 1 kHz is used for LSB coding. Sometimes to increase the amount of data to be embedded the two Least Significant bits of the sample are replaced with two message bits.

STEGANOGRAPHY CHARACTERISTICS:

- Imperceptibility: As the secret data is hidden in the cover object, it goes undetectable.
- Security: It is measured in terms of Universal Image Quality Index(UIQI), Color Image Quality Measure(CQM), Peak Signal to Noise Ratio(PSNR) for images. Squared Pearson Correlation Coefficient (SPCC), Signal to Noise

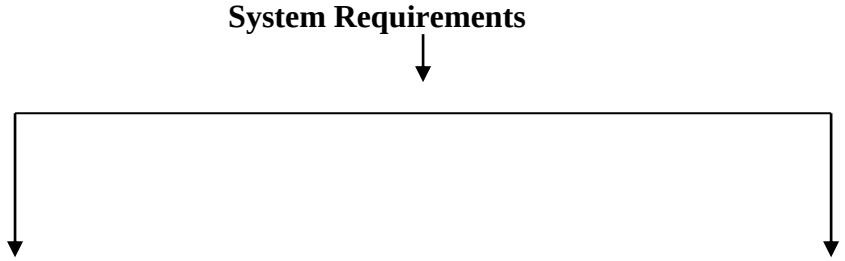
Ratio(SNR) etc are used to measure audio[5,6].

- Capacity: It is the measure of size of the secret information. It can be measured in samples or bits or bytes.

Working principle:

The proposed system provides multilayered security for secure data transfer. LSB coding is used to embed secret information in the cover objects such as image, audio or video file. In LSB coding the least significant bit of each sampling point is substituted with a binary message. Ideal data transmission rate of 1kbps per 1 kHz is used for LSB coding. Sometimes to increase the amount of data to be embedded the two Least Significant bits of the sample are substituted with two message bits.

The softwares used in this work are Core java, jdk1.6.0_12, Computer with a Pentium ||| processor, 256 MB RAM and about 2GB(approx) of hard disk space. The user has to make the interactions to the system through the user screens developed as part of the system using Java Frames. The software runs on any Operating System which has java virtual machine. 256 MB RAM and disk space of 2GB (approx) is required for this purpose. Since this software is primarily based on JAVA, the most basic system configuration as specified will most likely work. For performance reasons a possible minimal system requirement would be a Pentium ||| class processor, 256 MB RAM and disk space of 2GB (approx).



Software Requirements	**Hardware Requirements**
JDK1.3 and above	Processor : Pentium III
Any O.S	Memory : min 128MB
	Disk Space : depends on AVI File

Design procedure:

These are the steps followed in data hiding while transmitting and receiving the Stego object:

1. Obtain a cover image (Any available image)
2. Get the secret information to be sent (image or message)
3. Combine cover image with the information to be hidden(LSB algorithm is used)
4. During transmission it will be compressed to minimize congestion.
5. Data can be encrypted so that malicious users will not be able to access it..
6. Additional security can be provided by giving password facility.
7. Password check can be provided during extraction of data.
8. The hidden message can be extracted only if the passwords match.

Procedure to embed the message into the master file:

Inputs:

Message: The message to be embedded in the stego object.

Master_file: The stego object in which the message will be hidden.

Compressed: Variable indicating whether the message should be compressed.

Encryption: Variable indicating whether the message should be encrypted.

Algorithm:

1. Create a byte array of size equal to the input file.

2. Copy the contents of the input file into the byte array.

3. Embed the input file size, features and version information into the byte array.

4.Compress the message if the compression variable is set and embed the compression ratio into the output file.

5. Encrypt the message if required.

6. Embed the message size and the message into the output file.

Procedure to retrieve the embedded message from the master file:

Algorithm:

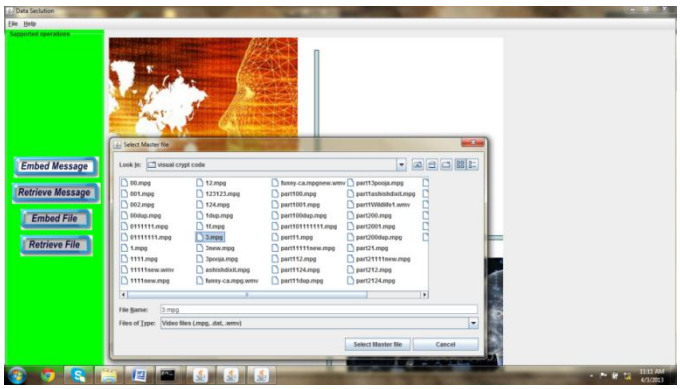
1. Retrieve the output file from the Stego object.

2. Retrieve the byte array from the output file.

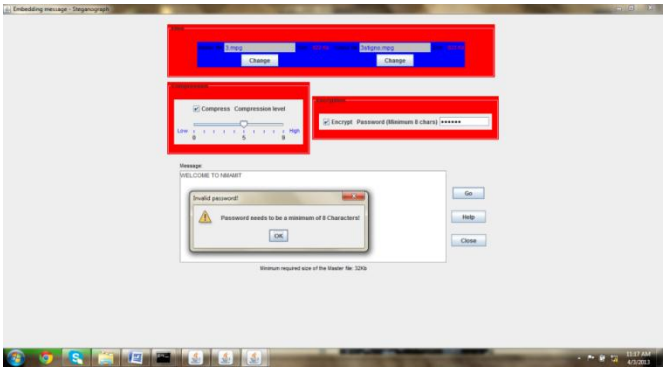
2. Uncompress the message if the compression flag is set.
3. Decrypt the message if the embedded message is encrypted.

1. **Home Page**

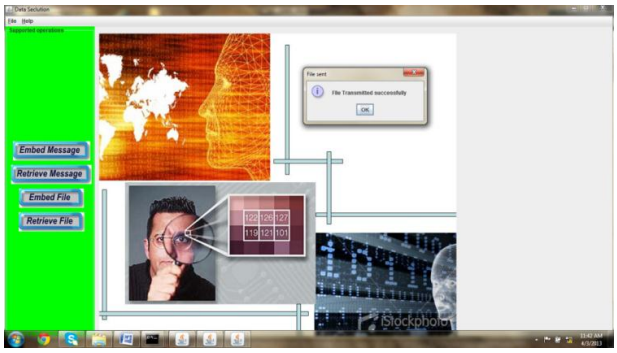
2. Selecting the input video file, in which the Message will be embedded.



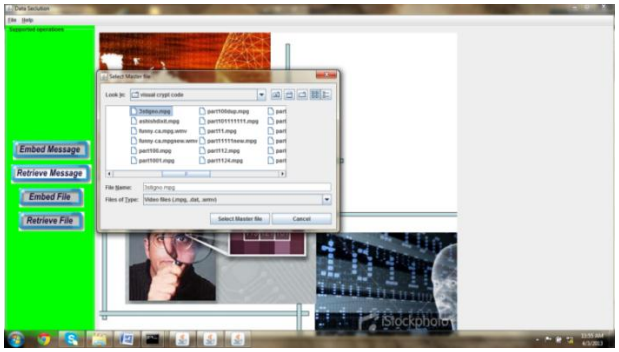
3. Embedding the message



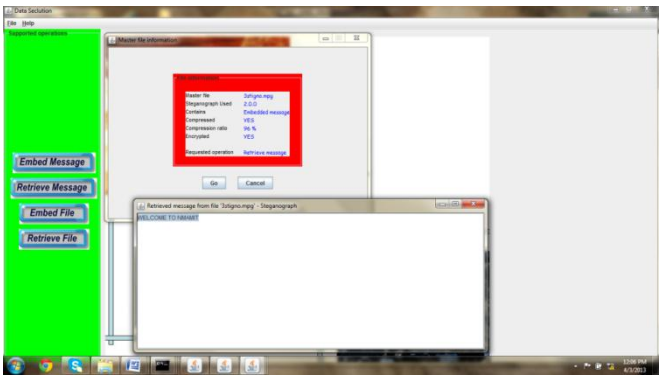
4. Sending the Stego object(Video File) containing the embedded secret message



5. Retrieving the message from the video file



6. Message retrieved successfully



CONCLUSIONS

This paper proposes a robust and secure steganography technique. It provides an efficient way of transmitting data in media files without exposing its existence. This technique involves low cost and is reliable. This approach needs to be examined against steganography attacks such as cropping and histogram equalization.

REFERENCES

[1] Shejul, A. A., Kulkarni, U.L. A Secure Skin Tone based Steganography (SSTS) using Wavelet Transform. International Journal of Computer Theory and Engineering, Vol.3, No.1, 2011. pp. 16-22.

[2] M. I. Khalil. Image steganography: Hiding short messages within digital images. JCS&T, Vol.11, No. 2. pp 68-73.

[3] Ki-Hyun Jung, Kee-Young Yoo. Data hiding using edge detector for scalable images, Springer 2012.

[4] Ali Kanso, Hala S. Own. Steganographic algorithm based on a chaotic map. Communication Nonlinear Science Numerical Simulation, 17, 2012. pp 3287–3302.

[5] Zhou Wang, Alan Conrad Bovik, Hamid Rahim Sheikh, Eero P. Simoncelli. Image Quality Assessment: From Error Visibility to Structure Similarity. IEEE Transactions on image processing, Vol. 13, No. 4, 2004. pp. 600-612.

[6] C.Sasi varnan, A. Jagan, Jaspreet Kaur, Divya Jyoti, Dr.D.S.Rao. Image Quality Assessment Techniques in Spatial Domain. IJCST Vol. 2, Issue 3, 2011. pp 177-184.

[7] Prabir Kr. Nasar Hari Narayan Khan, Ujjal Roy, Ayan Chaudhuri, Atal Chaudhuri. Shared Cryptography with embedded session key for secret audio. International Journal of computer applications(0975-8887, Volume 20- No 8, Jully 2011)

[8] Billiam A. An Introduction to Steganography and its uses. 2014. Available from: http://null-byte.wonderhowto.com/how-to/introduction-steganography-its-uses-0155310/.

[9] Taruna, Singh D. Message Guided Random Audio Stegano graphy Using Modified LSB Technique. International Journal of Computers & Technology. 2014 Jan; 12(5): 3464–8.

[10] Pratap Chandra Mandal, "Modern Steganographic technique: A Survey", International Journal of Computer Science & Engineering Technology (IJCSET).