Analysis and Design of 3 LSB Techniques for Secure Audio Steganography

*Laxmi Kumari, *Dinesh Goyal

*Suresh Gyan Vihar University, Jaipur

Abstract: Information hiding has evolved since 1970's and has become an integral part of internet in present century. This has been a keystone in the field of Information communication, as it saves data from losses, attacks and any other malicious practices. There have been many techniques of information hiding which can be classified into information modification (Cryptography) & information embedding (steganography).

Steganography is an art of hiding one message file into another cover file so that during communication of the data the attacker will not have the idea of secret data which is travelling. Audio steganography is an art in which the message data is embedding in the audio file by using techniques like LSB, Parity, phase, spread spectrum and Echo embedding. Till now LSB techniques has been implemented for embedding text file in audio up to 4th & 5th LSB.In this research paper we will attempt to embed image file in an audio file using 3rd LSB technique and try to analyze the quality of audio after embedding process is completed.

I. Introduction

A. Steganography:-

Steganography is the most advanced communications areas, hidden information and other information, to conceal the fact. Many different vector file formats can be used, but the digital image is the most popular because of their frequency on the Internet. Hide secret information for the image, there is a wide variety of steganographic techniques, some of which are more complex than others; they all have their own strengths and weaknesses. Different applications have different requirements, the use of steganography. For example, some applications may require absolute invisibility of the secret information, while others require larger secret information is hidden. This paper addressed a hidden picture overview of its uses and technologies. It is also trying to find a good steganography requirements briefly reflect steganographic techniques more suitable for which applications.[1]

The general idea of hiding some information in digital content has a wider class of applications. The techniques involved in such applications are collectively referred to as *information hiding*. For example, an image printed on a document could be annotated by metadata that could lead a user to its high resolution version. In general, metadata provides additional information about an image.

Although metadata can also be stored in the file header of a digital image, this approach has many limitations. Usually, when a file is transformed to another format (e.g., from TIFF to JPEG or to BMP), the metadata is lost. Secondly, cropping or any other form of image manipulation destroys the metadata. Finally, metadata can only be attached to an image as long as the image exists in the digital form and is lost once the image is printed. Information hiding allows the metadata to travel with the image regardless of the file format and image state (digital or analog).

B. Types of Steganography:-

Almost all digital file formats can be used for steganography, but more suitable format, are those with a high degree of redundancy. Redundancy can be defined as an object, which provides the necessary accuracy is much greater than the use of objects, and display. Redundant bits are an object can be changed easily without changing those bits to be detected. Image and audio files, especially to meet this requirement, but also found in other file formats can be used for information hiding.

Hidden text information is secret history of the most important methods. One obvious way is a message in every word of every n-th letter hidden secret messages.[2]

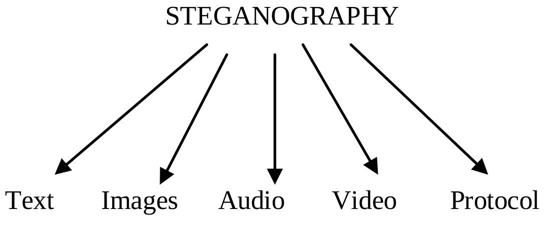


Fig1. Types of Steganography

C. Applications:-

Steganography is applicable to, but not limited to, the following areas.

1) Confidential communication and secret data storing

2) Protection of data alteration

3) Access control system for digital content distribution

4) Media Database systems [6]

D.Modern Steganography

At sender site, the message to be hidden (*emb*) is hiding in some cover data. The cover data may be some digital image, text file, video file, binary file, etc.. A key is associated with the hiding process. The message thus obtained is called is called stego which is transmitted to the receiver. The same process is repeated at receiver site but in reverse order to obtain the original message as shown in below given Figure.

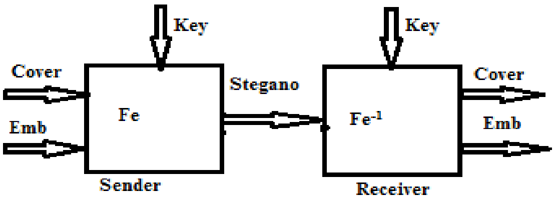


Fig 2. Modern Steganography

Where,

Fe - steganographic function “embedding”.

Fe^{-1} - steganographic function “extracting”.

Cover - cover data in which emb will be hidden.

Emb - message to be hidden.

Key - parameter of fe.

Stegano - cover data with the hidden message.[3]

II. AUDIO STEGANOGRAPHY:-

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. Steganography works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text, HTML, or even floppy disks) with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images.

In a computer-based audio Steganography system, secret messages are embedded in digital sound. The secret message is embedded by slightly altering the binary sequence of a sound file. Existing audio Steganography software can embed messages in WAV, AU, and even MP3 sound files. Embedding secret messages in digital sound is usually a more difficult process than embedding messages in other media, such as digital images. These methods range from rather simple algorithms that insert information in the form of signal noise to more powerful methods that exploit sophisticated signal processing techniques to hide information.

Types of Audio Steganography:-

- LSB coding
- Parity coding
- Phase coding
- Spread spectrum
- Echo hiding

Technique Used:-

1. LSB(Least Significant Bit)

This is the simplest of the Steganography methods based in the use of LSB, and therefore the most vulnerable. The embedding process consists of the sequential substitution of each Least Significant Bit (LSB-1) of the image pixel for the bit message.

This method is probably the easiest way of hiding information in an image and yet it is surprisingly effective. It works by using the least significant bits of each pixel in one image to hide the most significant bits of another. So in a JPEG image for example, the following steps would need to be taken

a. First load up both the host image and the image you need to hide.

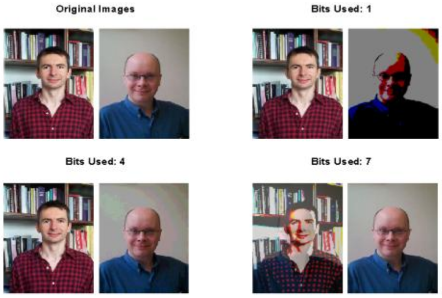
b. Next chose the number of bits you wish to hide the secret image in. The more bits used in the host image, the more it deteriorates. Increasing the number of bits used though obviously has a beneficial reaction on the secret image increasing its clarity.

c. Now you have to create a new image by combining the pixels from both images. If you decide for example, to use 4 bits to hide the secret image, there will be four bits left for the host image. (PGM - one byte per pixel, JPEG - one byte each for red, green, blue and one byte for alpha channel in some image types)

Host Pixel: 10110001
Secret Pixel: 00111111
New Image Pixel: 10110011

d. To get the original image back you just need to know how many bits were used to store the secret image. You then scan through the host image, pick out the least significant bits according the number used and then use them to create a new image with one change - the bits extracted now become the most significant bits.

Host Pixel: 10110011
Bits used: 4
New Image: 00110000



This method works well when both the host and secret images are given equal priority. When one has significantly more room than another, quality is sacrificed. Also while in this example an image has been hidden, the least significant bits could be used to store text or even a small 1amount of sound. All you need to do is change how the least significant bits are filled in the host image. However this technique makes it very easy to find and remove the hidden data. [4]

III. Evaluation of Audio Steganography

ADVANTAGES:

1. Audio based Steganography has the potential to conceal more information:
   a. Audio files are generally larger than images
   b. Our hearing can be easily fooled
   c. Slight changes in amplitude can store vast amounts of information
2. The flexibility of audio Steganography is makes it very potentially powerful :
3. Another aspect of audio Steganography that makes it so attractive is its ability to combine with existing cryptography technologies.
4. Many sources and types makes statistical analysis more difficult :

DISADVANTAGES:

1. Embedding additional information into audio sequences is a more tedious task than that of images, due to dynamic supremacy of the HAS over human visual system.
2. Robustness: Copyright marks hidden in audio samples using substitution could be easily manipulated or destroyed if a miscreant comes to know that information is hidden this way.
3. Commercialized audio Steganography have disadvantages that the existence of hidden messages can be easily recognized visually and only certain sized data can be hidden.[5]

IV. Proposed Work

Problem domain:-

1. There are many techniques for text embedding in Audio which goes up to 7LSB also.
2. There is no technique of embedding JPEG images in Audio cover.
3. All the JPEG images normally are encrypted and transmitted without any cover.

Solution domain:-

1. Flow chart for Proposed Model is as follows

SENDER:-

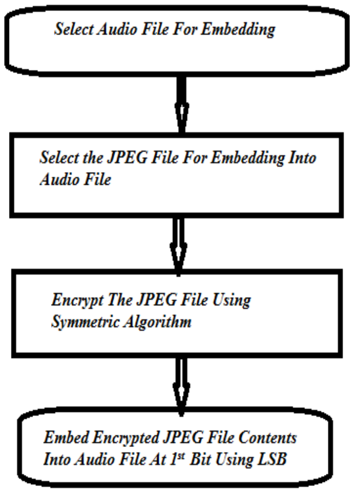

Select Audio File For Embedding
Select the JPEG File For Embedding Into Audio File
Encrypt The JPEG File Using Symmetric Algorithm
Embed Encrypted JPEG File Contents Into Audio File At 1st Bit Using LSB

Fig. 4 Audio Steganography at Sender end

RECEIVER:-

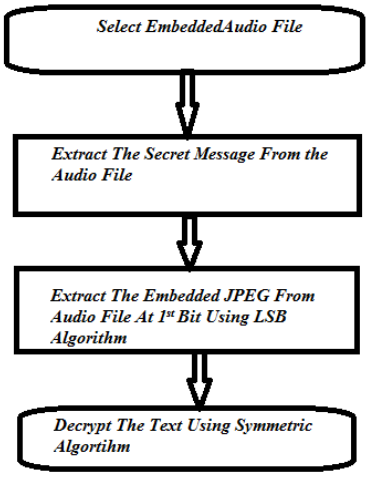

Select EmbeddedAudio File
Extract The Secret Message From the Audio File
Extract The Embedded JPEG From Audio File At 1st Bit Using LSB Algorithm
Decrypt The Text Using Symmetric Algortihm

Fig. 5 Audio Steganography at Receiver end

V. Analysis

a. Technical analysis:-

Comparison of results (SNR) to analyze the performance of the proposed Model.

Table 1

S. No.	Name of Image	Size of Image(KB)	Dimension of Input Image	Image Status	PSNR (after and before embedding)
1	Flower	16.8	259*194	Normal Image	31.740
				Encrypted Image	28.1194
2	Radhe Krishna	26.5	480*480	Normal Image	32.2911
				Encrypted Image	31.2163
3	quote	43.90	420*317	Normal Image	29.4341
				Encrypted Image	27.8544
4	Rose	106	1280*1024	Normal Image	30.9266
				Encrypted Image	29.4214
5	Poster	67.9	720*540	Normal Image	28.9979
				Encrypted Image	27.5416

b. Graphs of FFT Analysis of Audio Files

1. INPUT AUDIO FILE

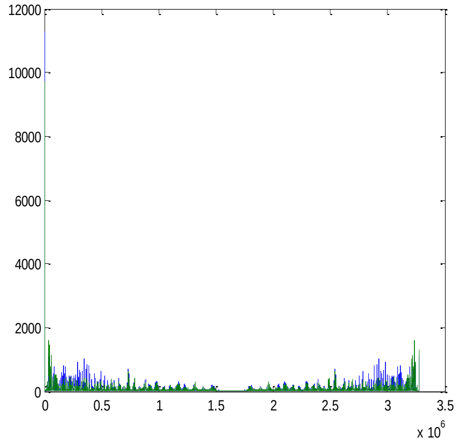


Fig. 6 Audio Steganography INPUT File

2. EMBEDDED AUDIO FILE

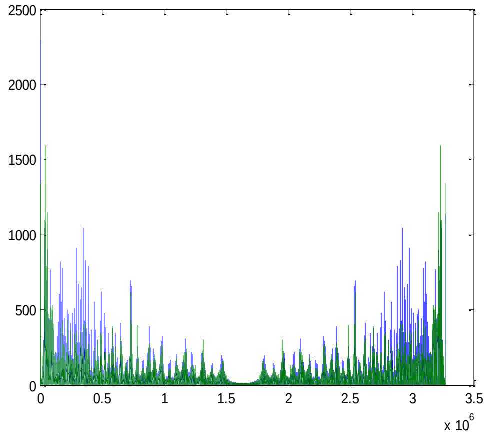


Fig. 7 Audio Steganography OUTPUT File

VI. Conclusion

Many currently used technologies are not strong enough to prevent the embedded data detection and removal. The use of benchmarking techniques become more common, the need for a more robust standard definition, in order to help overcome this.

While studying audio Steganography it was found that lot of work already done on this technique. Text, video, Image, audio can hide inside the audio and one can use audio as a cover file and also as a secret message but did not get anything done on encrypted images.

Here we have tried to perform audio steganography using encrypted image (encrypted using AES).

The results prove that most of the images are having PSNR more than 28 which shows that the loss in the image data is quite low. While in case of FFT analysis of audio file their is big difference in the both audio(before and after embedding)

VII. Future Work

Even though our work increases the security of image message by encryption and then embedding, still, In future the work may be improved so that we get similar audio quality after and before embedding, It may also be tried to perform audio steganography of encrypted images using DCT.

IX. References

1. Moerland,T., “Steganography and Steganalysis”, Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/privtech.pdf.

2. IJEIT1412201210_35.pdf.

3. Khan, M.M.; “Steganography”, http://www.neiu.edu/~ncaftori/355/Steganography.ppt.

4. AN OVERVIEW OF IMAGE STEGANOGRAPHY
T. Morkel 1, J.H.P. Eloff 2, M.S. Olivier 3

5. “Steganography FAQ” - Aelphaeis Mangarae

[Zone-H.Org] March 18th 2006,

http://www.infosecwriters.com/text_resources/pdf/

Steganography_AMangarae.pdf

6. A Proposed Algorithm for Steganography in Digital Image Based on Least Significant Bit
BY A. E.Mustafa, A.M.F.ElGamal, M.E.ElAlmi, Ahmed.BD