International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org, editorijettcs@gmail.com
Volume 2, Issue 3, May – June 2013 **ISSN 2278-6856**

EVALUATING OVERHEADS OF LSB BASED AUDIO STEGANOGRAPHY

Digvijay Singh Mankotia[1], Kuldeep Sharma[2]

[1&2] Electronics & communication engg.
RIET,Phagwara,
PTU ialandhar

Abstract: ***A Steganographic method for embedding textual information in audio signal is deliberated here. A new fast algorithm is proposed which will use DCT base audio compression to speed up the audio steganography algorithm. In the proposed method each audio signal will be transformed into bits and then the textual information will be embedded in it. In embedding process, first the message character is transformed into its equivalent binary form. The last 4 bits of this binary is taken into deliberation and applying redundancy of the binary code the prefix either 0 or 1 is used. To identify the uppercase, lower case, space, and number the control symbols in the form of binary is used. By using proposed LSB based algorithm, the capacity of stego system to hide the text increases. The performance evaluation will be prepared by comparing the output of proposed strategy with well-known existing algorithms.***

Index terms: Audio signals, Audio Steganography, Overheads and LSB.

I. Introduction

Information embedding [1]-[5] refers to the embedding of data within a cover object (also referred to as cover text) such as image, video, audio, graphics, text, or packet transmission times. Applications include copyright protection, database annotation, transaction tracking, traitor tracing, timing channels, and multiuser communications.

These applications often impose the requirement that embedding only slightly perturb the cover text. The name watermarking has been widely used to describe information embedding techniques that are perceptually transparent, i.e., the marked object (after embedding) is perceptually similar to the cover object. In some applications, the presence of the embedded information should be kept secret. Then perceptual transparency is not sufficient, because statistical analysis could reveal the presence of hidden information.

The problem of embedding information that is hard to detect is called steganography, and the marked object is called stegotext [3]. Steganography differs from cryptography in that the presence of the message needs to remain secret, rather than the value of the message. The dual problem to steganography is steganalysis, that is, detection of hidden information within a stegotext.

Several application scenarios for steganography

1) Steganography may be used to communicate over public networks such as the Internet. One may embed bits into inconspicuous files that are routinely sent over such networks: images, video, audio files, etc. Users of such technology may include intelligence and military personnel, people that are subject to censorship, and more generally, people who have a need for privacy.

2) Steganography may also be used to communicate over private networks. For instance, confidential documents within a commercial or governmental organization could be marked with identifiers that are hard to detect. The purpose is to trace unauthorized use of a document to a particular person who received a copy of this document. The recipient of the marked documents should not be aware of the presence of these identifiers.

3) Timing channels can be used to leak out information about computers. A pirate could modify the timing of packets sent by the computer, encoding data that reside on that computer. The pirate wishes to make this information leakage undetectable to avoid arousing suspicion. To disrupt potential information leakage, the network could jam packet timings - hence the network plays the role of an active warden. The channel over which the stegotext is transmitted could be noiseless or noisy, corresponding to the case of a passive and an active warden, respectively.

Moreover, the steganographer's ability to choose the cover text is often limited if not altogether nonexistent. In the private-network application above, the cover text is generated by a content provider, not by the steganographer (i.e., the authority responsible for document security).

Research motivation

A literature survey of the existing solutions to the problem of audio steganography leads to the following conclusions:

a. Solutions that provide accurate audio steganography are slow.

b. Solutions that reduce the required time result in lesser accuracy in audio steganography.
So a trade-off between space and time complexity is the motivation for the work. And to reduce the time and space complexity we have used dct based audio compression.

Research methodology

To attain the objective, step-by-step methodology is use in this research work.Figure1 illustrate the audio steganography process which is based on least significant bit modification. The flowchart of the algorithm is given as shown in Figure 1. IT is showing the different steps that will be followed in order to encode the text into the digital signal.

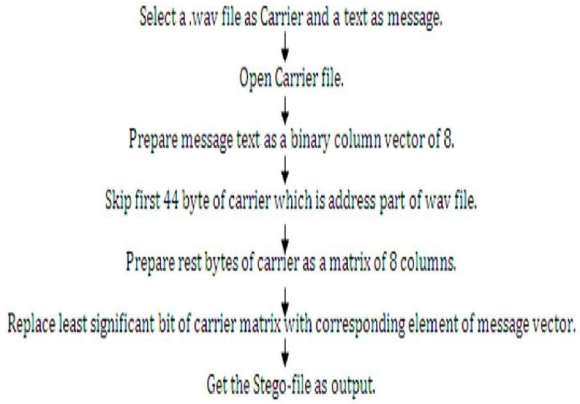

Fig 1 Flowchart of LSB modification Technique for audio steganography.

After executing the program the procedure can showed with the help of original data as shown in Figure 2

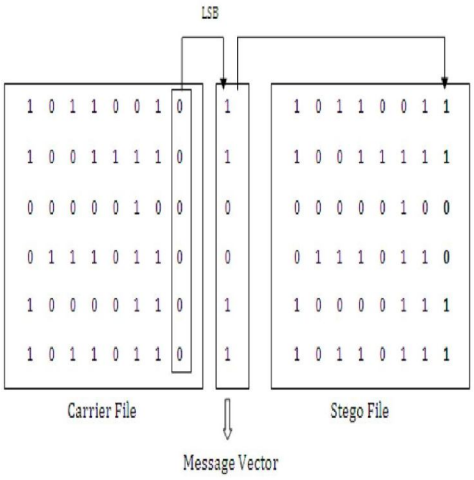

Fig2 LSB modification procedure for Audio Steganography.

Least Significant Bit (LSB) Encoding

Least significant bit (LSB) coding is the simplest way to embed information in a digital audio file. By substituting the least significant bit of each sampling point with a binary message, LSB coding allows for a large amount of data to be encoded. In LSB coding, the ideal data transmission rate is 1 kbps per 1 kHz. In some implementations of LSB coding, however, the two least significant bits of a sample are replaced with two message bits. This increases the amount of data that can be encoded but also increases the amount of resulting noise in the audio file as well.
To extract a secret message from an LSB encoded sound file, the receiver needs access to the sequence of sample indices used in the embedding process. Normally, the length of the secret message to be encoded is smaller than the total number of samples in a sound file. One must decide then on how to choose the subset of samples that will contain the secret message and communicate that decision to the receiver.
One trivial technique is to start at the beginning of the sound file and perform LSB coding until the message has been completely embedded, leaving the remaining samples unchanged. This creates a security problem, however in that the first part of the sound file will have different statistical properties than the second part of the sound file that was not modified. One solution to this problem is to pad the secret message with random bits so that the length of the message is equal to the total number of samples.
There are two main disadvantages associated with the use of methods like LSB coding. The human ear is very sensitive and can often detect even the slightest bit of noise introduced into a sound file, Second disadvantage however, is that this is not robust. If a sound file embedded with a secret message using either LSB coding was resample, the embedded information would be lost. Robustness can be improved somewhat by using a redundancy technique while encoding the secret message. However, redundancy techniques reduce data transmission rate significantly.

Problem formulation

The goal of this research work is to explore audio steganography and its applications in secure, real-time voice communication. Steganography is the process of hiding a secret message within a larger one such that the presence of the secret message cannot be detected. In this case, user authentication information will be embedded in raw audio data in a voice chat application.
This can be accomplished by using the least significant bit of an audio sample to store one bit of an encoded message. With a proper decoder, the secret message can be extracted from an audio sample while the normal listener would have no idea that it exists. For an 8-bit

sample, this process will result in fairly low distortion, around 23dB.

In order to provide authentication information about the sender, the encoded message will be a cryptographic hash value computed from a prior set of audio samples. The audio stream will be divided into frames of a specific size, such as 512 samples. Each new frame will contain the information required to authenticate the previously sent frame, thus providing real-time sender verification. The deliverables for this research work will be a series of sender/receiver programs. The sender program will take in audio stream data, along with a key, and embedded some authentication data steganographically. The receiver program will receive and playback the transmitted audio data while decoding and displaying the decoded authentication information. Ultimately, these techniques could be used in a bidirectional voice chat application that provides user authentication that is undetectable in its network traffic. Stretch goals include the implementation of audio compression and plug-in development for existing voice chat applications.

Problem definition

Classification of audio documents as bearing hidden information or not is a security issue addressed in the context of steganalysis. A cover audio object can be converted into a stego-audio object via steganographic methods. In this research work a statistical methods will be proposed which will calculate the effect of steganography on audio signals.

The emphases are to propose a technique which put minimum effect on audio signals. As every steganography technique comes up with some overheads and also results in increasing the size of audio signals so overheads and optimality is also considered in this research work. Different metrics will be calculated which will be used to compare proposed optimal technique with available methods.

To do performance comparison the result of proposed algorithm will be compared with some well known audio recognition algorithm.

Literature review

Sridevi et al. (2009) [1] have been researched in the efficient method of audio steganography by modified LSB algorithm and strong encryption key with enhanced security. In the current internet community, secure data transfer is limited due to its attack made on data communication. So more robust methods are chosen so that they ensure secured data transfer. One of the solutions which came to the rescue is the audio Steganography. But existing audio steganographic systems have poor interface, very low level implementation, difficult to understand and valid only for certain audio formats with restricted message size.

Enhanced Audio Steganography (EAS)[1] is system which is based on audio Steganography and cryptography, ensures secure data transfer between the source and destination. EAS uses most powerful encryption algorithm in the first level of security, which is very complex to break. In the second level it uses a more powerful modified LSB (Least Significant Bit) Algorithm to encode the message into audio. It performs bit level manipulation to encode the message.

The basic idea behind this research has to provide a good, efficient method for hiding the data from hackers and sent to the destination in a safer manner. Though it is well modulated software it has been limited to certain restrictions. The quality of sound depends on the size of the audio which the user selects and length of the message. Though it shows bit level deviations in the frequency chart, as a whole the change in the audio cannot be determined.

Nedeljko et al. (2004) [2] has been studied in the increasing robustness of LSB audio steganography using a novel embedding method. This research has presented a novel high bit rate LSB audio watermarking method. The basic idea of the proposed LSB algorithm is watermark embedding that causes minimal embedding distortion of the host audio. Using the proposed two-step algorithm, watermark bits are embedded into higher LSB layers, resulting in increased robustness against noise addition or MPEG compression. Listening tests showed that the perceptual quality of watermarked audio is higher in the case of the proposed method than in the standard LSB method.

Jayaram et al.(2011) [3] has researched the information hiding using audio steganography. Today's large demand of internet applications requires data to be transmitted in a secure manner. Data transmission in public communication system is not secure because of interception and improper manipulation by eavesdropper. So the attractive solution for this problem is Steganography, which is the art and science of writing hidden messages in such a way that no one, apart from the sender and intend recipient, suspects the existence of the message, a form of security through obscurity.

Audio steganography [3] is the scheme of hiding the existence of secret information by concealing it into another medium such as audio file. This research has mainly discussed different types of audio steganographic methods, advantages and disadvantages.

Gadicha et al. (2011) [4] has described the audio wave steganography. This research has explored a new 4th bit rate LSB audio Steganography method that reduces embedding distortion of the host audio. Using the proposed algorithm, Message bits are embedded into 4th LSB layers, resulting in increased robustness against noise addition. In addition, listening tests showed that perceptual quality of audio is higher in the case of the proposed method than in the standard LSB method.

Divya et al.(2012) [5] has studied on the hiding text in audio using multiple LSB steganography and provide security using cryptography. Steganography is an art and science of writing hidden messages in such a way that no one apart from the intended recipient knows the existence of the message. The maximum number of bits that can be used for LSB audio steganography without causing noticeable perceptual distortion to the host audio signal is 4 LSBs, if 16 bits per sample audio sequences are used.

The research has proposed two novel approaches of substitution technique of audio steganography that improves the capacity of cover audio for embedding additional data. Using these methods, message bits are embedded into multiple and variable LSBs. These methods utilize up to 7 LSBs for embedding data. Results showed that both these methods improve capacity of data hiding of cover audio by 35% to 70% as compared to the standard LSB algorithm with 4 LSBs used for data embedding. And using encryption and decryption techniques performing cryptography. So for this RSA algorithm used.

Gunjan et al. (2012) [6] has studied a detailed look of audio steganography techniques using LSB and genetic algorithm approach. This research has study of various techniques of audio steganography using different algorithms like genetic algorithm approach and LSB approach. It has tried some approaches that help in audio steganography. It has 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.

In steganography, the message used to hide secret message is called host message or cover message. Once the contents of the host message or cover message are modified, the resultant message is known as stego message. In other words, stegomessage is combination of host message and secret message. Audio steganography requires a text or audio secret message to be embedded within a cover audio message. Due to availability of redundancy, the cover audio message before steganography, stego message after steganography remains same for information hiding.

Malviya et al.(2012) [7] has studied audio steganography by different methods. Information hiding technique is a new kind of secret communication technology. Steganography has been proposed as a new alternative technique to enforce data security. A perfect audio Steganographic technique aim at embedding data in an imperceptible, robust and secure way and then extracting it by authorized people.

Hence, up to date the main challenge in digital audio steganography is to obtain robust high capacity steganographic systems. Leaning towards designing a system that ensures high capacity or robustness and security of embedded data has led to great diversity in the existing steganographic techniques. A current state of art literature on audio steganographic techniques and how it's performed by different way.

In this section different issue related to this research work has been evaluated. A perfect audio Steganographic technique aim at embedding data in an imperceptible, robust and secure way and then extracting it by authorized people. However there does not exist any standard method or metric which will evaluate the performance of encoded signals.

Proposed algorithm

Figure 3 is demonstrating that how message is hiding takes place using LSB method. However as proposed algorithm is DCT based so what is demanded is to compress every signal by using DCT compression before it is passed to LSB based steganography technique.

a. Embedded data in songs

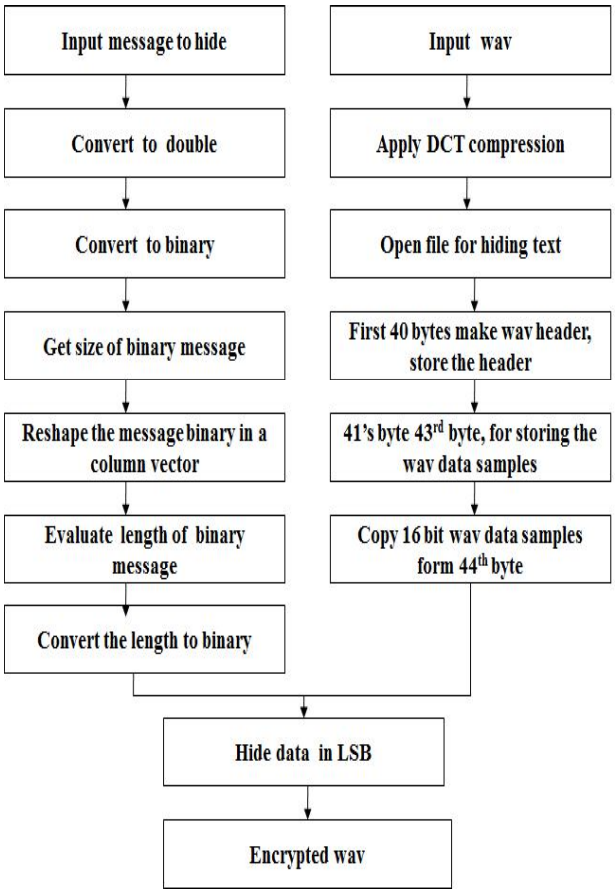

Fig. 3 Proposed algorithm

Figure 4 is demonstrating that how message is extraction takes place using LSB method. However as proposed algorithm is DCT based but no inverse DCT is preformed

to reconvert signal is in its original form as it not the area of interest in audio steganography.

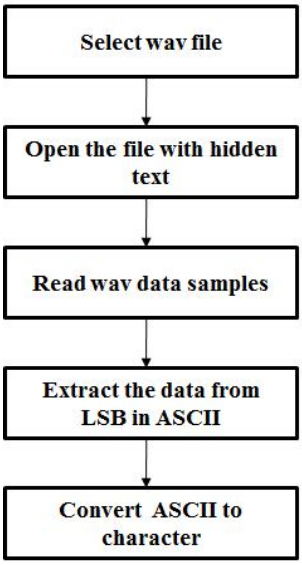

Fig. 4 Extraction of data

Experimental setup

A suitable simulation is done in MATLAB by considering proposed strategy. A set of 100 audio signals in .wav format is taken and passed one by one to the proposed simulator and results are taken. The set detail is shown in Table 1.

Table 1 Experimental data

Name *.wav*	Size in kb's
Waheguru.wav	56
Water.wav	78
Train.wav	101
Air.wav	178
IPL.wav	223
- - -	- - -
Gurbani.wav	2130
Arty.wav	2267
Micromax.wav	2289

Performance analysis

This section provides the comparison between proposed and existing strategy. Figure 5 is demonstrating the effect of DCT compression on the original signal and it is clearly showing the effect of compression on the audio spectrum as shown in the Figure.

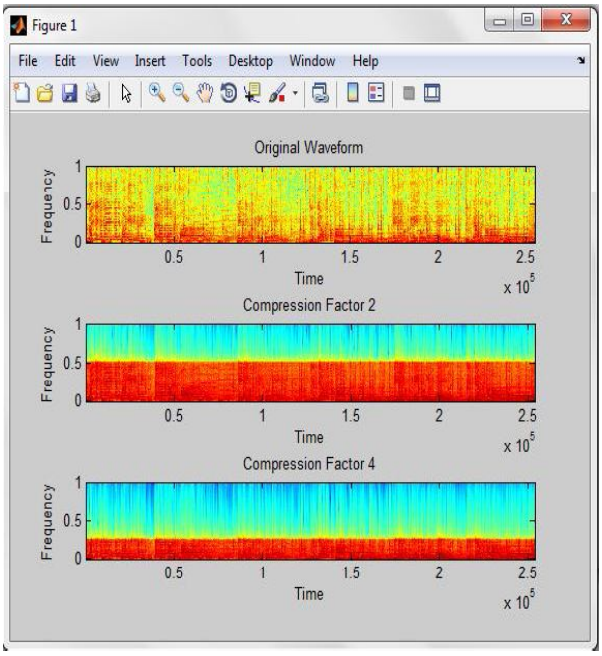

Fig. 5 DCT based compressed wav signal

Table 2 is showing the outcome of the proposed algorithm over the existing algorithm.

Original size	Proposed size	Stego size of proposed technique	Stego size of Existing technique	Time of proposed technique	Time of Existing technique
200	56	56	200	1.2	1.9
300	78	78	300	1.4	2.1
412	101	101	412	1.8	2.3
556	178	178	556	1.9	2.4
676	223	223	676	2.1	2.6
712	243	243	712	2.2	2.9
810	267	267	810	2.4	3.0
924	317	317	924	2.4	3.0
1024	378	378	1024	2.8	3.1

Figure 6 is showing the performance graph of proposed algorithm over existing algorithm by considering the size of original wav with the wav output of DCT based compression.

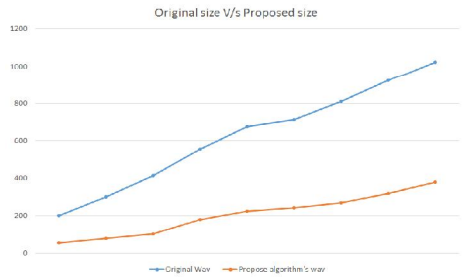

Fig. 6 Original wav V/s DCT based compression.

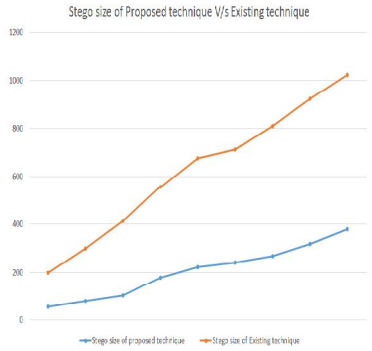

Fig. 7 Embedded wav using existing V/s DCT based technique

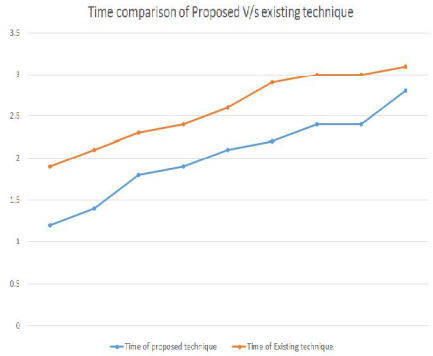

Fig 8 Time comparison between proposed and existing technique

Conclusion

This paper has evaluated the different gaps in existing research and techniques. It has been found that existing methods do work well but they are slow in nature as audio size always vary and when size become more they take too much time to hide the message in the audios same at decoding time. Therefore in-order to provide improved and fast results, a new integrated improved audio steganography algorithm is proposed in this research work. In order to improve the efficiency and prevent audio steganography algorithm from becoming the bottleneck of encoded audios, overheads are also calculated in this research work. To reduce overheads and embedding time DCT based compression is used to reduce the size of the audio signals. By doing performance comparison it is shown that the proposed strategy provide better results.

Reference

[1] R Sridevi, Dr. A Damodaram and Dr.Svl. Narasimham, "Efficient Method of Audio Steganography by Modified LSB Algorithm and Strong Encryption Key With Enhanced Security", Journal of Theoretical and Applied Information Technology, pp. 771-778, 2009.

[2] NedeljkoCvejic, TapioSeppanen, "Increasing Robustness Of LSB Audio Steganography Using A Novel Embedding Method ", The International Conference on Information Technology, 2004.

[3] Jayaram P, Ranganatha H R and Anupama H S, "information hiding using audio steganography ", The International Journal of Multimedia & Its Applications (IJMA) Vol.3, pp. 86-96, Aug. 2011.

[4] Ajay.B.Gadicha, "audio wave steganography ", International Journal of Soft Computing and Engineering (IJSCE), Vol. 1, pp. 174-177, Nov. 2011.

[5] S.S. Divya, M. Ram Mohan Reddy,"Hiding Text In Audio Using Multiple LSB Steganography And Provide Security Using Cryptography", International Journal of Scientific & Technology Research, Vol. 1, pp. 68-70, July 2012.

[6] Gunjan Nehru and Puja Dhar, "A Detailed Look Of Audio Steganography Techniques Using LSB And Genetic Algorithm Approach", International Journal of Computer Science (IJCSI), Vol. 9, pp. 402-406, Jan. 2012.

[7] Swati Malviya, Manish Saxena, "audio steganography by different methods ", International Journal of Emerging Technology and Advanced Engineering, Vol. 2, pp. 371-376 July 2012.