A Modified Approch Audio Stagnography Based On Technique LSB Coding

Surekha Shrivastava, Mr. Gajendra Singh chandel, Mr. Kaislash Patidar

Abstract :- Information security is becoming very important part of our life now-a-days. Information hiding is the fundamental of information security. Information hiding can be achieved by steganography as well. This paper presents a modified method of audio stegnography. Audio steganography is the technique of hiding secret information in the audio files. We have presented a high capacity and high stego-signal quality audio steganography scheme based on samples comparison in DWT domain where selected coefficient of a segment are compared with pre determined threshold value T and based on comparison bits are embedded. The strength of our algorithm is depend on the segment size and their strength are enabled the algorithm to achieve very high embedding capacity for different data type that can reach up to 25% from the input audio file size with lest of 35 dB SNR for the output stego signal. Further we have tabulated the result and the conclusion is made on the basis of the obtained results.

***Index Terms*- Steganography, DWT, SNR, audio, embedding.**

I. INTRODUCTION

Steganography word is originated from Greek words Steganós (Covered), and Graptos (Writing) which literally means "cover writing"[1]. Generally steganography is known as "invisible" communication. Steganography means to conceal messages existence in another medium (audio, video, image, communication). Today's steganography systems use multimedia objects like image, audio, video etc as cover media because people often transmit digital images over email or share them through other internet communication application[2].

Different type of object can be used as carrier and message object. It can be Image, Text, audio and video[6-8].

Steganography terminologies are as follows:-

• Cover Data-: Original data which is used as a carrier for hidden information.
• Message : Actual information which is used to hide into images. Message could be a plain text or some other image.
• Stego-data: After embedding message into cover image is known as stego-image. • Stego-Key: A key is used for embedding or extracting the messages from cover-data and stego-data.

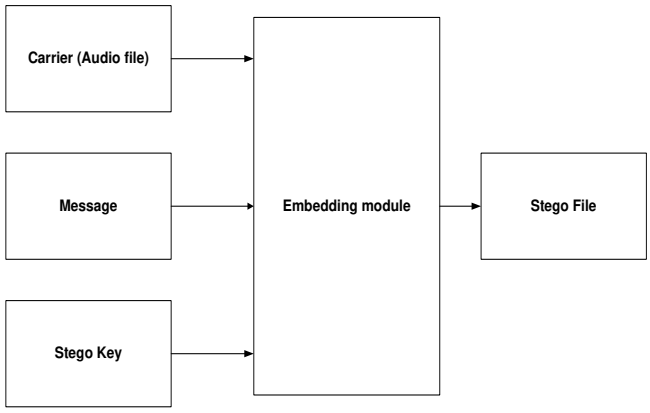

Figure 1.1 Classification of Information Hiding.

A. Types of Steganography

There are basically three types[2] of steganographic protocols used[9-10]. They are:

- Pure Steganography
- Secret Key Steganography
- Public Key Steganography

Pure Steganography is defined as a steganographic system which does not require the exchange of a cipher such as a stego-key. This method of is not much secure because the sender and receiver can rely only upon the assumption that no other parties are aware of the secret message.

Secret Key Steganography is defined as a steganographic system that requires the exchange of a secret key (stego-key) previous to communication. Secret key Steganography takes a cover message and embeds the secret message inside of it by using a secret key (stego-key). Only the parties who know the secret key can reverse the process and read the secret message. Unlike Pure Steganography where a perceived invisible communication channel is present, Secret Key Steganography exchanges a stego-key, which makes it more vulnerable to interception. The benefit to Secret Key Steganography is even if it is intercepted; only parties who know the secret key can extract the secret message.

Public Key Steganography is defined as a steganographic system that uses a public key and a private key to secure the communication between the parties wanting to communicate secretly. Sender will use the public key during the encoding process and only the private key, which has a direct mathematical relationship with the public key, can decipher the secret message. Public Key Steganography provides a more strong way of implementing a steganographic system because it can utilize a much more robust and researched technology in Public Key Cryptography. It also has multiple levels of security in that unwanted parties must first suspect the use of Steganography and then they would have to find a way to crack the algorithm used by the public key system before they could intercept the secret message.

B. Steganography in Digital Mediums

Information hiding can be achieved either exploiting loopholes of Human Visual System (HVS) or Human Auditory System (HAS). Steganography of audio signals is more challenging than Steganography of images due to wider dynamic range of the HAS in comparison with human visual system (HVS). The HAS perceives sounds over a range of power greater than 109 to 1 and a range of frequencies greater than 103 to 1. Two properties of the HAS used in steganographic algorithms are frequency masking and temporal masking. Frequency (simultaneous) masking is a frequency domain trend where a low level signal can be made inaudible (masked) by a simultaneously appearing stronger signal (the masker) [12].

Depending on the type of the cover object there are many suitable steganographic techniques which are followed in order to obtain security.

Audio Steganography: When taking audio as a carrier for information hiding it is called audio steganography. It has become very significant medium due to voice over IP (VOIP) popularity. Audio steganography uses digital audio formats such as WAVE, MIDI, AVI MPEG or etc for steganography.

Image Steganography: Taking the cover object as image in steganography is known as image steganography. Generally, in this technique pixel intensities are used to hide the information. **Network Steganography:** When taking cover object as network protocol, such as TCP, UDP, ICMP, IP etc, where protocol is used as carrier, is known as network protocol steganography.. **Video Steganography:** Video Steganography is a technique to hide any kind of files or information into digital video format. Video (combination of pictures) is used as carrier for hidden information. Generally discrete cosine transform (DCT) alter values (e.g., 8.667 to 9) which is used to hide the information in each of the images in the video. **Text Steganography:** General technique in text steganography, such as number of tabs, white spaces, capital letters, just like Morse code and etc is used to achieve information hiding.

C. Data Embedding Techniques

Some commonly used methods of audio steganography are Phase coding Phase coding relies on the fact that the phase components of sound are not as perceptible to the human ear as noise is[13-15].. It "works by substituting the phase of an initial audio segment with a reference phase that represents the data. The phase of subsequent segments is then adjusted in order to preserve the relative phase between segments".

Spread Spectrum (SS) coding attempts to spread out the encoded data across the available frequencies as much as possible. This is analogous to a system using an implementation of the LSB coding that randomly spreads the message bits over the entire sound file. In Echo data hiding, Text can be embedded in audio data by introducing an echo to the original signal. The data is then hidden by varying three parameters of the echo: initial amplitude, decay rate, and offset.

Least Significant Bit (LSB) Coding : One of the earliest techniques studied in the information hiding of digital audio (as well as other media types) is LSB coding. In this technique LSB of binary sequence of each sample of digitized audio file is replaced with binary equivalent of secret message. Parity Coding: Instead of breaking a signal down into individual samples, the parity coding method breaks a signal down into separate regions of samples and encodes each bit from the secret message in a sample region's parity bit.

II. AUDIO STAGNOGRAPHY AND ITS ADVANTAGES

Audio steganography is focused in hiding secret information in an innocent cover audio file or signal securely and strongly. By embedding secret information using an audio signal as a cover medium, the very existence of secret information is hidden away during communication. This is a serious and vital issue in some applications such as battlefield communications and banking transactions [1-4]. 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.
The basic model of Audio steganography consists of Carrier (Audio file), Message and Password. Carrier is also known as a cover-file, which conceals the secret information.. Message is the data that the sender wishes to remain it confidential. Message can be plain text, image, audio or any type of file. Password is known as a stego-key, which ensures that only the recipient who knows the corresponding decoding key will be

able to extract the message from a cover-file. The cover-file with the secret information is known as a stego-file.

The information hiding process consists of following two steps [23].

i. Identification of redundant bits in a cover-file. Redundant bits are those bit that can he modified without corrupting the quality or destroying the integrity of the cover-file.

ii. To embed the secret information in the cover file, the redundant bits in the cover file is replaced by the bits of the secret information.

Audio based Steganography has the potential to conceal more information. Audio files are generally larger than images. Our hearing can be easily fooled. Slight changes in amplitude can store vast amounts of information. The flexibility of audio Steganography is makes it very potentially powerful. The methods discussed provide users with a large amount of choice and makes the technology more accessible to everyone. A party that wishes to communicate can rank the importance of factors such as data transmission rate, bandwidth, robustness, and noise audibility and then select the method that best fits their specifications.

Another aspect of audio Steganography that makes it so attractive is its ability to combine with existing cryptography technologies. Users no longer have to rely on one method alone. Not only can information be encrypted, it can be hidden altogether. Many sources and types makes statistical analysis more difficult and Greater amounts of information can be embedded without audible degradation

Many attacks that are malicious against image Steganography algorithms (e.g. geometrical distortions, spatial scaling, etc.) cannot be implemented against audio Steganography schemes. Audio Steganography in particular addresses key issues brought about by the MP3 format, P2P software, and the need for a secure broadcasting scheme that can maintain the secrecy of the transmitted information, even when passing through insecure channels.

III. PROPOSED METHODOLOGY

In the proposed method the carrier file is taken as audio format and the secret message may be a text or audio format files. Our system provides a very friendly User Interface where the user had to specify just the required inputs (audio, text). After embedding or extracting the user can save /open or just discord the output of that particular operation according to their wish. In view of providing security by preventing unauthorized person to access the software password facility is provided to the user in order to work with the software. To provide more security by avoiding an intruder to extract the embedded data a security key is used while embedding and extracting message.

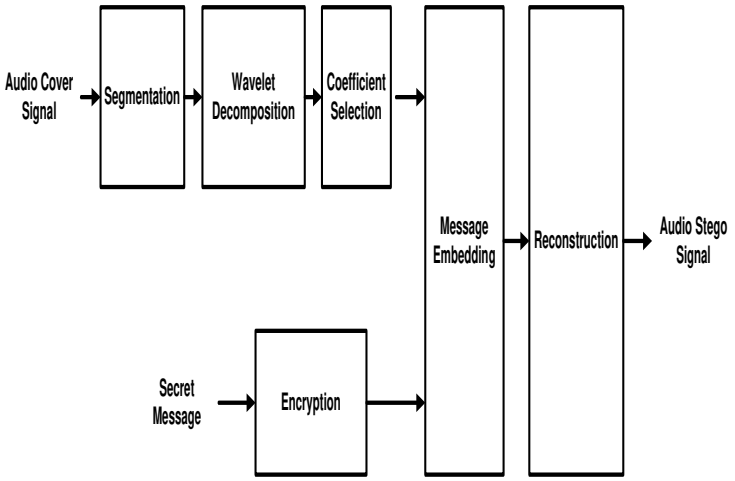

Figure 4.1 the General Structure of the Proposed Hiding Scheme

A. Algorithm for embedding text files content into audio file at the sender side:

step1: select the audio file for embedding the secret message.

step2: play the audio file so that it sounds clear to the end user.

step3: select the text file containing the secret message.

step4: encrypt the text file contents.

step5: compare text file and audio file size. If text file size > audio file contents error message displayed indicating cannot embed secret message. else embed secret message in the audio file in the 4^{th} and 5th lsb bit of every sample.

step6: Display message to user of the new audio file created after embedding secret message.

B. Algorithm For Extracting The Embedded Text From Audio File At The Receiver Side. [4]

Step 1: Select the new audio file for extracting the secret message.

Step 2: Extract the secret message from the audio file from the 4th and 5th LSB bit of every sample.

Step3: If secret message present in audio file Then Display message to end user after extracting message. Else Display that no hidden data is present in the text.

Step4: Decrypt the secret message.

Step5: Display message to end user after decrypting the message.

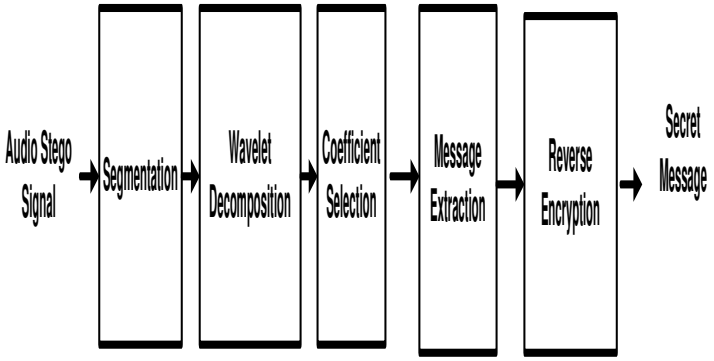

Figure 4.2 Block diagram of the Message Recovery Algorithm

A. Least Significant Bit (LSB) Coding

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. Figure 3 illustrates how the message 'HEY' is encoded in a 16-bit CD quality sample using the LSB method. In LSB coding, the ideal data transmission rate is 1 kbps per 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. Yet now the embedding process ends up changing far more samples than the transmission of the secret required. This increases the probability that a would-be attacker will suspect secret communication.

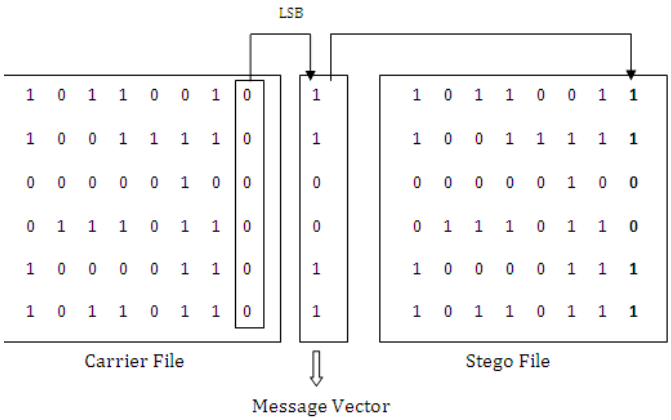

Figure 3.1 Example of LSB coding

IV. PERFORMANCE PARAMETERS

Bit Error Rate: Bit error rate can be defined as the percentage of bits corrupted in the transmission of digital information due to the effects of noise, interference and distortion.

$$\mathbf{BER = N_W/N_S*100}$$

Where, Nw is the number of error bits and NS refers to the No of Secret bits. Signal-to-Noise ratio: SNRseg is defined as the average of the SNR values over short segments:

$$SNRseg = \frac{10}{M}\sum_{m=0}^{M-1}\log_{10}\sum_{i=Nm}^{Nm+N-1}\left(\frac{x^2(i)}{\left(x(i)-y(i)\right)^2}\right)$$

where *x(i)* is the original audio signal, *y(i)* is the distorted audio signal. The length of segments is typically 15 to 20 ms for speech. The SNRseg is applied for frames which have energy above a specified threshold in order to avoid silence regions. Signal-to-Noise Ratio (SNR), is a special case of SNRseg, when M=1 and one segment encompasses the whole record [18]. The SNR is very sensitive to the time alignment of the original and distorted audio signal. The SNR is measured as

$$SNR = 10\log_{10}\frac{\sum_{i=1}^{N}x^2(i)}{\sum_{i=1}^{N}\left(x(i)-y(i)\right)^2}$$

Here N represents the number of samples in both signals.

V. RESULTS

All algorithms, including proposed technique, are implemented on Windows PC having Intel 2.4 GHz processor and 4GB RAM, and run using MATLAB R2010a. We have considered three different audio files in this experiment to embed digital data. One of the audio file is adios sound and is a 8 bit mono

audio signal sampled at 11.25 kHz. The embedded data is a text file namely Input.txt (see Figure 5.1).

We applied Haar wavelets on cover signal and choose the coefficient where the data is to be hide using a pre determined threshold value T. The performance of the embedded information is studied by applying attacks such as re-quantization, re-sampling, low-pass filtering, high-pass filtering, AWGN, MP3 compression, jittering and cropping. For the complete analysis of the proposed technique different audio signals are considered such as the adios, aaaaagh, and shutdwn track.

Cover Signal	Threshold T	Output SNR (dB)	Processing Time (sec)
adios.wav	0.01	33.45	2.11
	0.02	27.65	2.24
	0.03	25.56	2.86
aaaaagh.wav	0.01	33.43	2.45
	0.02	28.56	2.54
	0.03	25.92	2.72
shutdwn.wav	0.01	34.65	2.15
	0.02	28.32	2.28
	0.03	25.16	2.37

Table 5.1 SNR and Processing Time for adios.wav with different Threshold value T

Cover Signal	AWGN (dB)	BER
adios.wav	35	54.34
	30	48.65
	25	44.56
aaaaagh.wav	35	52.43
	30	50.56
	25	48.42
shutdwn.wav	35	53.65
	30	48.32
	25	46.55

Table 5-2 Performance evaluation of the embedded data with respect to AWGN and BER

VI. CONCLUSION

In this paper, we have seen the significance and the requirements of the stagno-graphy. We have also seen the Types of Steganography that is Pure Steganography, Secret Key Steganography, Public Key Steganography. Further we have seen the classification of stagno graphy on the basis of HAS or HVS and on the basis of cover object ie. Text, vedio, audio, image, Network Protocal. Then we have described the Date embedding techniques. Then we have proposed the method of stegno-graphy in which the LSB coding is used and the encrypting the secret massage and embedding it with the audio cover signal. Result is compared the performance on the basis of the SNR and processing time by varying the threshold for different audio signal and we found that with the increment of the threshold the processing time increases and output SNR decreases. Further Analysis is done on the basis of the BER by varying the noise power level of the AWGN channel. With the decrement in the noise power the BER also decreases.

Disadvantages associated with this proposed system are a low data transmission rate due to the fact that the each bit of secret message is embedded into one segment and size of segment is approx 4 to 16 samples. It means that utilization of samples is very poor. As a result, this method can be used when only a small amount of data needs to be concealed. Otherwise this can be proved as a good method for audio Steganography. In future we will modify and improve this technique so that more data can be embedded into cover signal.

REFERENCES

[1] Pal S.K., Saxena P. K. and Mutto S.K. "The Future of Audio Steganography". Pacific Rim Workshop on Digital Steganography, Japan, 2002.

[2] Lee, Y. K. and Chen L. H. "High Capacity Image Steganographic Model". IEEE Proceedings Vision, Image and Signal Processing, pp. 288-294, 2000.

[3] Zaidoon Kh. AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan. O. Alanazi, Overview: Main Fundamentals for Steganography, journal of computing, volume 2, issue 3, march 2010, issn 2151-9617.

[4] Sos S. Agaian, David Akopian and Sunil A. D'Souza" two algorithms in digital audio steganography using quantized frequency domain embedding and reversible integer transforms" 1Non-linear Signal Processing Lab, University of Texas at San Antonio, Texas 78249, USA.

[5] Ashwini Mane, Gajanan Galshetwar, Amutha Jeyakumar, "Data Hiding Technique: Audio Steganographyusing LSB Technique" International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 3, May-Jun 2012, pp.1123-1125.

[6] Neil Jenkins, Jean Everson Martina ," Steganography in Audio" Anais do IX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais page: 269-278,2007

[7] Westfeld, A. (2003). Detecting low embedding rates. In Petitcolas, F. A., editor, Information Hiding: 5th International Workshop. Springer.

[8] I. J. Cox, J. Kilian, F. T. Leighton and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," IEEE Trans. Signal Processing, vol. 6, no. 12, pp. 1673- 1687, December 1997.

[9] Petitcolas, F.A.P., Anderson, R., Kuhn, M.G.,"Information Hiding - A Survey", July1999.

[10] Miss Deepal Sushil Dhariwal," A Seminar Report On Audio Steganography "Department of Computer Engineering & Information Technology, College of Engineering, Pune, 2009-2010.

[11] Prof. Samir Kumar Bandyopadhyay, Tuhin Utsab Paul, Avishek Raychoudhury," A Robust Audio Steganographic Technique based on Phase Shifting and Psycho – acoustic Persistence of Human Hearing Ability", International Journal of Computing and Corporate Research.

[12] Rajkiran Ravula," Audio Watermarking Using Transformation Techniques", M.sc.thesis, The Department of Electrical and Computer Engineering, Louisiana State University, December, 2010.

[13] A. B. Watson, "Image Compression Using the Discrete Cosine Transform,"Mathematical Journal , vol. 4(1), pp. 81-88, 1994.

[14] B. Chen and G. W. Wornell, "Digital Watermarking and Information Embedding using Dither Modulation," Multimedia Signal Processing, 1998 IEEE Second Workshop, pp: 273-278, December 1998.

[15] Nedeljko Cvejic, "Algorithms For Audio Watermarking And Steganography", Department of Electrical and Information Engineering, Information Processing Laboratory, University of Oulu 2004.

Surekha Shrivastava, Student M.Tech, SSSIST, Sehore, M.P., India., surekhashrivastava@gmail.com.

Mr. Gajendra Singh Chandel, *Hod, CSE Department, SSSIST, Sehore,M.P., India,* gajendrasingh86@rediffmail.com

Mr.Kailash Patidar, Assit. Professor, CSE Deparment, SSSIST, Sehore, M.P., India, kailashpatidar123@gmail.com