A Perusal Study of Audio Steganography with LSB Techniques

Mr. Satish Bhalshankar
M.E. Student
Department of Computer Science and Engg.
Government College of Engineering Aurangabad
Aurangabad, India

Mr. Avinash K. Gulve
Associate Professor and Guide
Department of Computer Science and Engg.
Government College of Engineering Aurangabad
Aurangabad, India

Abstract— **The art of information hiding has done much progress in the recent years as security of information has become a big issue in this online communication era. The demand of security and privacy is increasing for confidential matter day by day, necessity of covering valuable and secret information have much importance during online communication. To fulfil this necessity, Steganography technique is very much useful which embed information in a digital media in such transparent way so no one should able to understand it. Audio Steganography is one of the most prominent and recognized technique. As it is known, imperceptibility, robustness and payload or hiding capacity are pillars of the steganography. The previous LSB techniques when increases payload capacity would hamper robustness as well as imperceptibility of the cover media. As well as when it matters of robustness to maintain then hiding capacity gets limited.**

This paper includes study of some audio steganography techniques with their merits and demerits. This paper proposes an audio steganography technique to improve the performance. The proposed method will provide optimum increment in the payload capacity by dividing the bytes of cover media into ranges to hide the bits of secret message appropriately. Use of range to hide secret data will maintain the robustness of cover media along with preserving the imperceptibility.

Key words— Audio data hiding, LSB, HAS, HVS, Parity, Range of Bytes.

I. INTRODUCTION

Steganography is the adroit skill to cloak data in a cover media such as text, audio, image, video, etc. The term steganography derived from Greek which means, “Covered Writing”. Steganography is the one of major technique of developing area of information hiding. Steganography provides techniques for masking the existence of a secondary message in the presence of a primitive message. The primitive message is accredited to as the carrier signal or carrier message, the carrier signal can be text, audio, image, video, etc., the secondary message is assigned to as the payload signal or payload message. The message is being hidden in such a way that the presence of secondary message is unrecognized to the onlooker and the carrier signal is modified in an imperceptible manner as shown in fig 1.

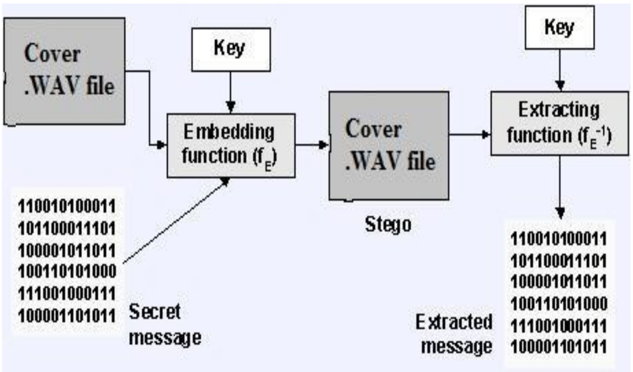


Fig. 1 Audio Steganography System (Stego-System)

Majorly, Cryptography involves the encryption of message. It makes no attempt to hide the encrypted message. In steganography the original message is not altered but the very existence is hidden from the observer by embedding the message in the selected medium.

Audio steganography:

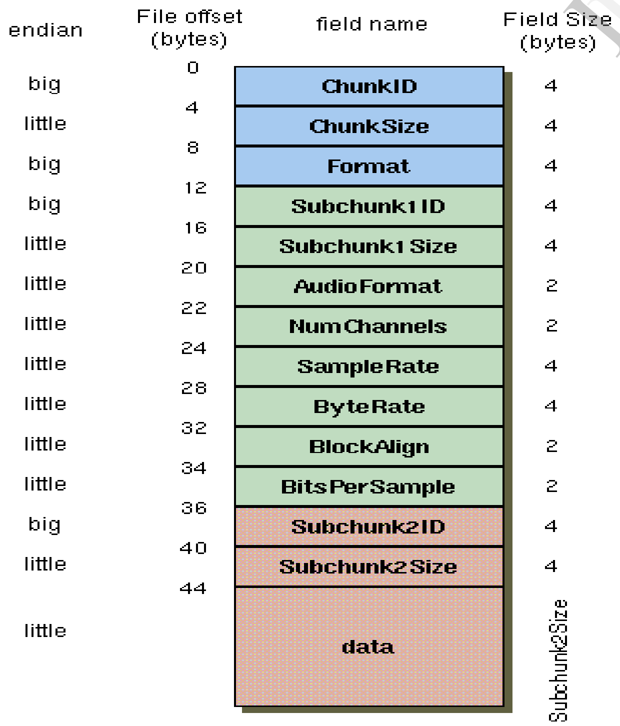
Cover signal + Target data = Stego signal (Transmitted)

There are distinct steganographic methods for masking the furtive message. The principal requirement for a steganographic method is imperceptibility which means that the furtive messages should not be discernible to the human by vision or audio. There are two more requirements, one is to maximize the hiding capacity, and the other is protection. Among different Steganography types, one technique is using audio files as stego-object. In a computer-based audio steganography system, digital sound is used for masking furtive message. By slightly varying the binary sequence of a sound file the secret message is embedded into the audio data file. In the last few years, various algorithms have been developed for the embedding and extraction of message in audio signals. All of the developed algorithms take advantage of the perceptual properties of the human auditory system (HAS) in order to add a message into a host signal in a perceptually transparent manner. Hiding extra information into audio signals is a little bit interesting but suspicious, as Human Auditory System (HAS) is more sensitive than Human Visual System (HVS) [1].

The masking of the confidential data into the covert medium should not make any loathsome changes to the covert medium so that the genuineness of the file should not disturbed. The audio steganography view is to ingrain valuable confidential data into an audio file in such a way that human auditory system (HAS) not supposed to detect the change that has been occurred due to ingraining of the data into the audio file. The audio steganography most followed such as (Least Significant Bit) LSB, Spread spectrum, and Echo hiding approaches along with other current applications that has been developed in recent years. The properties of audio steganography [2] that is exploited in different steganography applications are

a. Confidentiality
b. Imperceptibility
c. High capacity
d. Difficult detectability
e. Accurateness
f. Survivability
g. Visibility

Audio steganography is found to be a durable and strong avenue auditory system is much wise than human visual system. The idea is to ingrain the secret data into an audio file such that there is imperceptible difference between the original audio file and embedded file. While embedding the furtive data the format has to be keep in mind so that that header part of the wave file (first 44 byte) [3] should be untouched because in case the header gets corrupted, the audio file will also corrupt as shown in fig 2. The second consideration that should be made is not to embed data into the silent zone as that might cause undesirable change to the audio file.



endian	File offset (bytes)	field name	Field Size (bytes)
big	0	ChunkID	4
little	4	ChunkSize	4
big	8	Format	4
big	12	Subchunk1 ID	4
little	16	Subchunk1 Size	4
little	20	AudioFormat	2
little	22	NumChannels	2
little	24	SampleRate	4
little	28	ByteRate	4
little	32	BlockAlign	2
little	34	BitsPerSample	2
big	36	Subchunk2ID	4
little	40	Subchunk2Size	4
little	44	data	Subchunk2Size

Fig. 2 Wav File Format

II. Previous Approaches

A very interesting audio steganography method is the LSB (Least Significant Bit) algorithm. The least significant bit of the cover media is playing as a mask to the secret message. The modification made in such a way to the LSB bit should not be understood in the final stego object. Being an easy technique, a high level of security is not achieved. Changes are done to the existing LSB method to improve security. Also security, certain other parameters like time complexity, the computational load, SNR (Signal to Noise Ratio), BER (Bit Error Rate), efficiency, etc. are major points for considerations in Audio Steganography.

LSB have advantages like low computational load and easiness but still lacks in guarantee to protect the secret information. Hence, Enhanced Audio Steganography (EAS) with additional layers of encryption and decryption techniques can be implemented. So encoding the data, it is encrypted in advance. The main features of EAS are the size of the file is not changed after encoding and there is no software available to determine the sound variation caused by bit level manipulations. By Sridevi and Damodaram [4], a solution is suggested to both of these issues thus supporting different audio formats and reducing the time for encoding and decoding are discussed. Secret Data is embedded in such a way that each character requires eight 254/255 bytes. The efficiency of the algorithm in terms of security is the advantage of this method and the constraint is that sound quality depends upon the size of the audio selected and the length of a message embedded.
Merit: Enhanced Security due to Encryption
Demerit: Limited Payload Capacity

Kekre [5] proposed two methods that were used with LSB. First method is parity coding which is also described by B. Sandhi et. al. [10] and the other is XORing of LSB. Initially the lid or mask audio signal is read and one should ensure that the size of the message to be embedded is less than the mask audio signal. In parity method, the parity bit is considered before directly replacing the LSB. Depending upon the message bit to be embedded, the LSB is either flipped or retained. If the message bit is 0, LSB has to be modified in such a way that parity of the sample is even. Else if the message bit is 1, LSB is modified in such a way that parity of the sample is odd. In second method, XORed operation between the LSB and the next bit has to be equivalent to the message bit to be embedded. If equal the LSB is retained, else flipped. Also they reduce the computational load.

From experimental results it is found that the encryption with steganography provides better security. Embedding data in the higher LSB layers is prone to less attack than those embedded in the lower layers. But embedding in higher LSB will result in distortion. Therefore further steps have to be included to reduce these distortions.
Merit: Easy to modify bits of Cover media.
Demerits: No Security as well as if white space injected in current data it will create distortion.

Nedeljko and Tapio [6] proposed a method that enabled to embed data extending it from the fourth to sixth LSB layers with minimum distortions in two steps. Watermarked bit is embedded in any higher LSB layer using novel LSB method in the first step and second step changes white noise properties by shaping the impulse noise which is caused by the embedding bit. The proposed algorithm is encouraged for maintaining the imperceptible. Depending upon the message bit to embedded, the particular case is chosen.

Experimental results shows that SNR value is around 8QS (Quantization Step) in the standard algorithm which uses the 4th LSB and in the proposed algorithm from 1-4QS. Average power of the introduced noise is 9.31 dB lesser than the conventional method. When the data to be embedded is watermarked, the error rate is much reduced. The BER is also very less compared to the standard method. The adversary cannot exactly detect the bit layer where data is embedded. But this in turn makes the algorithm much more complex.

Merit: Enhancement shown in Imperceptibility.

Demerits: Detection of Exact Bit is complex as well as payload capacity is limited.

Even though algorithm perform embedding in different deep layers, to confine result to fix deep layers if it go for 4th and 1st layer. The results by Samir and Biswajita [7] experimentally proved to yield a stego signal that does not differ much from cover audio signal. To ensure no information loss it is necessary to check with a string length embedded in a first 8 samples. Message is embedded in the samples selected by the small logic as follows: consider the prime number next to the string length and determine all the prime numbers following it up-to the number of characters to be hidden. Each character requires three samples.

To embed the message, it converted to 7 bits binary equivalent and removes the MSB making it 6 bits thus paring 2 bits per sample. In each pair MSB is selected and embedded in the 4th LSB of the cover signal and certain changes are made to the other bits to reduce distortion, which follows the same logic specified by Nedeljko and Tapio [6]. The other bit of the pair is embedded in the LSB after this. At the receiver end, MSB (7th LSB layer) is chosen as 1 for upper case letters and 0 for numbers and special characters. Distortion is experimentally proved to be very less. Capacity and robustness is found to increase when 4th and 1st LSB layers are used.

Merit: The extraction algorithm is also very simple.

Demerit: supports mainly upper case characters.

LSB is combined with other techniques in different domains like temporal, cepstral and transform domain. Ahmad and Mohammad [8] selected temporal domain. This domain reduces computational load and supports fast implementation. Algorithm calculates the hearing threshold in the temporal domain which is exploited as the embedding threshold, yielding more capacity compared to uniform embedding pattern. Proposed method uses compression of information using lossless compressor, thus increasing total bit rate.

With the key to pseudo random number generator, the compressed data is encrypted. Embedding threshold is calculated based on the cover signal. Thresholds are assigned according to the samples magnitude. Lower magnitudes have less embedding capacity than the higher ones. SNR comparison of audio and stego through experimental and theoretical approaches are equal. BER calculated for pop, classic, country and speech resulted zero, thus efficient.

Merit: Enhanced hiding due to compression

Demerit: In presence of slight distortions, this method cannot achieve full recovery.

Gurvinder et al. [9], proposed algorithm for both image and audio steganography. Regarding audio steganography, it states the technique of producing an echo signal from the original signal. Data is embedded in the echo signal varying its parameters like decay rate, offset and amplitude. These parameters should be set below human audible range for imperceptibility. The original signal is segmented into blocks and each block is given the value 0 or 1 depending upon the secret message. The original signal is echoed and the message is embedded into it. This is then given to the mixer, the output of which is fed to the encoder. At the receiver end, auto correlation and decoding is done to separate the secret signal and the original signal. Further development of this echo hiding is Time Spread Echo Hiding. Here several echoes are produced and are stretched in time from which only certain echoes are selected for embedding data based on the PN generator.

The main theme proposed by Samir et al. [7], is based on psycho-acoustic theory of persistence and phase shifting. Persistence of hearing is based on the fact that two sounds successively with a difference of less than one-tenth of a second hit human ears, and then the difference between the sounds is imperceptible. 'i' is called the phase shift, the change of which is same as the shift in time. Samir et al. [7] used uncompressed audio format (WAV format). Consider Y1, Z1 and Y2, Z2 as the sampling rate and total duration of the primitive and target file. The target file is split after every 'i' seconds, 'i' varying between 0 and 1/10. Hence the total samples is equal to Y2 * i in target audio file. Phase shift and cover audio will be (i * Y2)/Y1. In cover audio file, data is embedded at the interval of (Z1*i)/Z2 seconds.

Merits: Insertion is quite undetectable and capacity is large.

Demerits: works with WAV file.

Few limitations that are generally observed in this survey are: Certain algorithms are very time consuming and have complex implementation, they don't support all audio formats. Even though full recovery and security are very essential and possible, there are some algorithms that cannot achieve it. As each and every algorithm has its own advantages and limitations, they are chosen depending upon the parameters required. This survey focuses the limitations in imperceptibility as well as enhancement in payload capacity with capacity with respect to high level of robustness and proposes the algorithm in the following section.

III. PROPOSED ALGORITHM

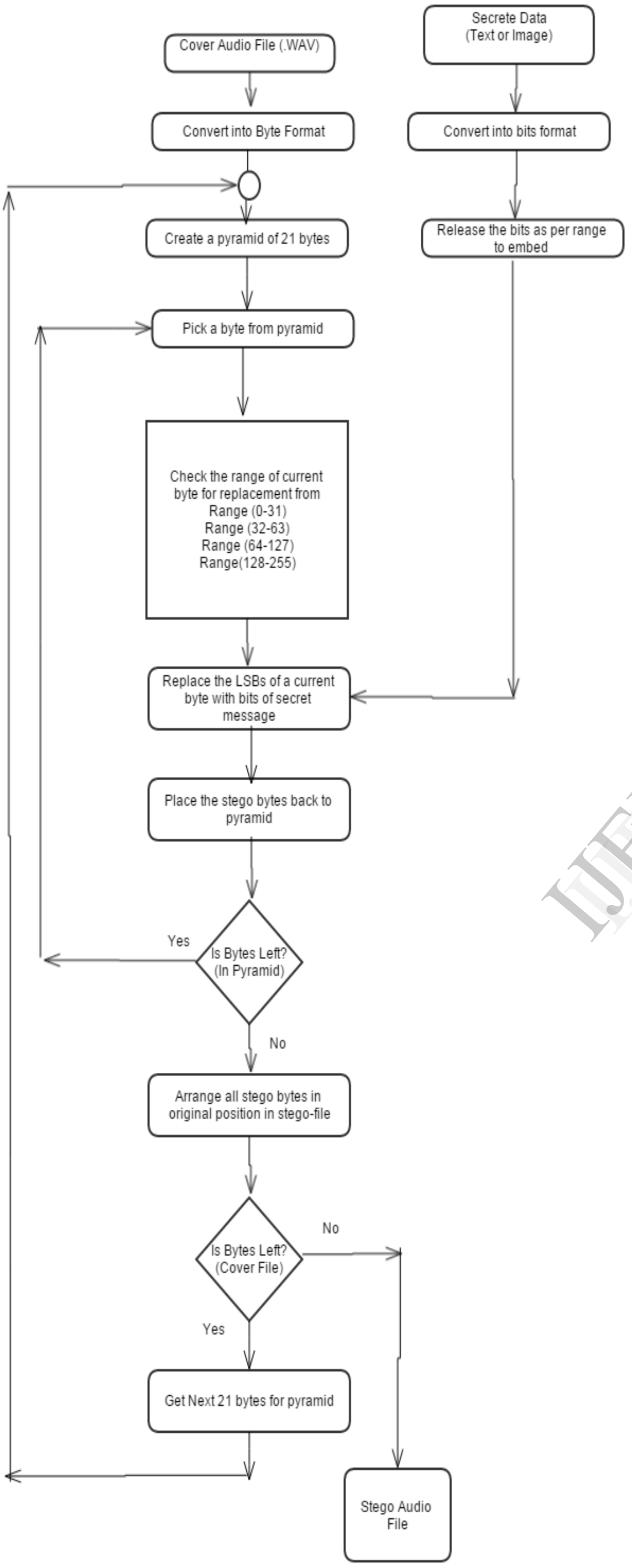

Cover Audio File (.WAV)
Secrete Data (Text or Image)
Convert into Byte Format
Convert into bits format
Create a pyramid of 21 bytes
Release the bits as per range to embed
Pick a byte from pyramid
Check the range of current byte for replacement from Range (0-31) Range (32-63) Range (64-127) Range(128-255)
Replace the LSBs of a current byte with bits of secret message
Place the stego bytes back to pyramid
Yes
Is Bytes Left? (In Pyramid)
No
Arrange all stego bytes in original position in stego-file
No
Is Bytes Left? (Cover File)
Yes
Get Next 21 bytes for pyramid
Stego Audio File

Fig 3. Work Flow Diagram For Proposed Algorithm

To overcome the limitations as per perusal, the new method for audio steganography is invented. To improve the payload capacity with very less distortion in original sound file where slightly modify the LSBs using this method. As well as maintain the imperceptibility. Fig 3 depicts the workflow of this proposed algorithm.

Proposed Algorithm uses ranges of bytes of cover audio file to hide the bits of secret information. But before replacing the LSBs of the selected bytes to ensure the randomness the pyramid of bytes is supposed to design and then data bits are embedded in LSB or higher layers based on the Ranges of bytes. Fig. 4 shows how to pick the byte for storing purpose.

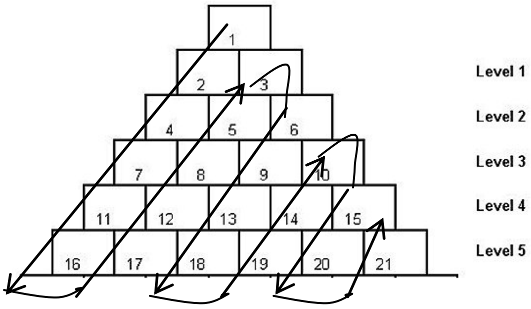


Fig. 4 Pyramid structure of bytes

The task of picking the bytes from ranges for embedding playing important role in this algorithm. For e.g., Range is (32-63) with byte value is 63 of cover file. Whereas form secret file the bit pattern is 110.
Then

0011 1111 = 63 (Before embedding)
011 = 03 (No. of Bits for Replacement)

0011 1011 = 61 (After embedding)

As here it seems the current byte is not having much variation in there after replacing the three LSBs. The main use of ranges of byte is to maintain the robustness again the attacks. Now as Range (i.e. in between 0 to 255) is increasing then replacement of maximum bits (From 2nd to 5th layer) also possible. So automatically the payload capacity will enhance.
This method may expect a better level of security in LSB modifications with Pyramid Structure. In future, the practical implementation of this algorithm will be done and performance analysis may be discussed in detail.

IV. CONCLUSION

End user thirsts for protection by using audio steganography to his important files as per discussed techniques to fulfil his requirements during online communication. This important that each method has its merits and demerits and can be useful for different platforms. The level of security and protection the end user wish, toughness of implementation, the payload capacity, and all these factors concludes the selection of the technique to be benefited.

REFERENCES

1. Lee, Y. K., & Chen, L. H. "High capacity image steganographic model", In IEEE proceedings vision, image and signal processing (pp. 288–294) 2000.
2. Harish Kumar & Anuradha, "Enhanced LSB technique for Audio Steganography", IEEE July 26 2012.
3. https://ccrma.stanford.edu/courses/422/projects/WaveFormat
4. Sridevi, R., A. Damodaram and S.V.L. Narasimham, "Efficient method of audio steganography by modified LSB algorithm and strong encryption key with enhanced security", J. Theor. Appl. Inf. Technol., 769-771, 2005.
5. Kekre, H.B., A. Archana R. Swarnalata and A. Uttara, "Information hiding in audio signals", International Journal on Computer. Appl., 2010
6. Nedeljko, C. and S.A. Tapio, "Increasing robustness of lsb audio steganography by reduced distortion lsb coding", J. Universal Comput. Sci. 11(1): 56-65.
7. Samir, K.B. and D. Biswajita, "Higher LSB layer based audio steganography technique", IJECT, 2(4) 2011.
8. Ahmad, D. and P. Mohammad, "Adaptive and Efficient Audio Data Hiding Method in Temporal Domain," International Conference on Information and Communication Systems. 2009
9. Gurvinder, S., S.K. Dey, S. Dubey and S. Katiyal, " Increasing the efficiency of Echo Hiding Digital Audio Steganography", 4th National Conference, INDIACom-2010 Computing for National Development, Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi.
10. B. Santhi, G. Radhika and S. Ruthra Reka, "Information Security using Audio Steganography -A Survey", Research Journal of Applied Sciences, Engineering and Technology 4(14): 2255-2258, 2012.