Implementation of Embedding Text in Audio using Randomized LSB Method for Secured Audio Steganography

Ullas K
Department of Telecommunication Engineering
Siddaganga Institute of Technology,
Tumakuru-572103, Karnataka, India

Chandrashekar H M
Department of Telecommunication Engineering
Siddaganga Institute of Technology,
Tumakuru-572103, Karnataka, India

Abstract—**Steganography is a technique used for secure transmission of data. Secure data communication has a greater importance in the communication world. Audio Steganography is a technique of hiding an existence of secret information in an audio file. The conventional LSB modification technique is very simple and effective but vulnerable to steganalysis. This paper proposes two algorithms to improve the performance of conventional LSB modification technique andAdvanced Encryption Standard (AES)techniqueused to improve the information security. Secret message encryption and embedding using Randomized LSB modification are the two powerful techniques combined to get high level confidentiality.These improvised techniques works against steganalysis and decreases the chances of secret information being extracted by an intruder. Proposed method is compared with variable higher bit approach. Here, instead of simply embedding the relevant bit in LSB, the whole byte value is modified so that it holds the data byte value being nearest to the original byte value.**

Keywords- Steganography; Audio Steganography; Steganalysis;Randomized LSB Modification; Information Security; AES (Advanced Encryption Standard)

I. INTRODUCTION

Electronic communication is very important in everyone’s day to day life, because of the fact that it is very simple, faster and more secure. Since electronic communication is used in such a large scale, security is more important. Information security is needed for confidential data transfer. Steganography is a technique used for secure transmission of confidential information.

The message/object used to hide the secret information is called as host message/cover object. Modified cover object with secret information is called as stego object. Steganography is used to conceal the existence of secret information in the stego object[1]. Cryptography technique is used for more data security. Cryptography used to change the representation of the secret information whereas steganography used to hide the secret information. Cryptographic encryption technique can be used to express the communication by scrambling the data so that attacker cannot understand and it is very important for secured data communication [2]. Audio steganography is considered to be more difficult to implement because of the fact that Human Auditory System (HAS) is more sensitive than the Human Visual System (HVS). It requires text or audio data to be embedded inside the cover object (audio) [3]. Audio steganography technique needs to satisfy three conditions namely capability, transparency and robustness. Capability is the size of secret information that can be hidden inside the cover audio, while transparency means how well the secret information is embedded in the cover audio. Robustness of a technique indicates the ability of embedded secret message to withstand attacks [4].Steganalysis is the process of detecting secret information hidden using steganography technique. The two commonly used steganalysis techniques are auditory inspection and statistical analysis. Auditory inspection is that, one can detect the presence of secret message through HAS. Statistical analysis is that, the intruder compares the original host message and modified host message to extract the secret message [5].

The secret information bit can be inserted by slightly altering the binary sequence of an audio file. Available audio steganography software can embed messages in .WAV, .AU, and even .MP3 audio files. Inserting the secret information bits in audio file is usually a more difficult task than inserting information bits in other media, like digital images. Different types of methods are used to embed the secret information in digital audio. The methods that are commonly used for audio steganography include LSB coding, Parity coding, Phase coding, Spread spectrum, Echo hiding. Most commonly used technique for audio steganography involves bitwise manipulation of the cover object to embed the secret information bits. A very good approach for bitwise steganography is the Least Significant Bit (LSB) Steganography, where the secret information bit to be hidden into the LSBs of the cover object [6-10].

However, conventional LSB steganography has a problem in the ease of implementation and detection. Another approach for conventional LSB steganography can be using randomized LSB bits and randomized samples of LSB. The main objective of this paper is to come up with a technique of hiding the secret information in cover object and it should work against steganalysis as well. The audio steganography technique could be backed by an encryption scheme. However, encryption method will decrease the capability. Section II explains aboutproposed methodology that enhances the existing LSB modification technique to make it more secure against steganalysis. Experimental results of the proposed method and conclusion are presented in Section VI and Section VII respectively.

II .RANDOMIZED STEGANOGRAPHIC LSB ALGORITHM

The projected Steganography algorithm is named as randomized LSB method. The conventional LSB method and the proposed method are discussed in detail.

A. Conventional LSB Method

The Least Significant Bit (LSB) embedding method is a very simple method to implement the steganography technique. The data is hidden inside the cover object by replacing the least Significant Bit of each sample of the cover object. If the LSB is varied, it will not affect the characteristic of the sample and also the cover (audio) data. Because, the strength of the LSB compared with the other bits in the sample is negligible. Of course it will introduce some noise, but the obtained noise level should be kept below a threshold. In conventional method, itis easy for the intruder to extract the message from the stego signal.

B. Proposed Method

Proposed method can be used to overcome this problem. In randomized LSB algorithm, on the encoder side, the cover object/medium is passed through the ADC and it is sampled at the sampling rate of 8000samples/second also it contains 8 bits. Through this presented methodology, it is observed that by modifying the 1st, 2nd and 3rd LSB bit of a sample with secret message bit it doesn’t produce any detectable change. There are two methods in this methodology named Bit Selection and Sample Selection to improve the conventional LSB method. And also secret message is encrypted by using the AES-128; it will produce the relation between plain text and cipher text. Of course encryption method reduces the capacity of insertion but it’s sure that robustness will be increase.

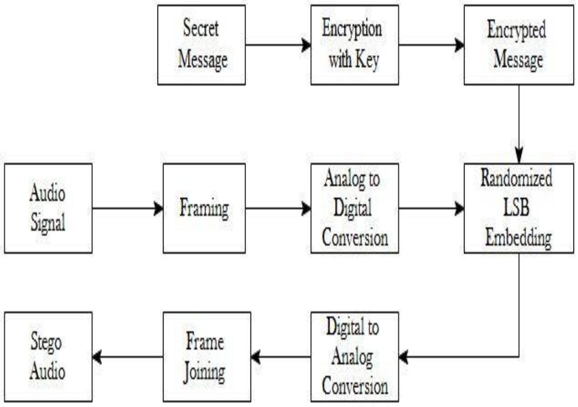

Fig 1: Randomized LSB Technique Encoder Module

Fig.1 shows the proposed method for sender part, where this methodology is carried out on the basis of Bit Selection and Sample Selection method. The cover audio file in the form of analog signal is dividing into number of frames and then it converted to digital form using ADC (analog-to-digital).Encryption Technique is also included in this method. For the worst case, when steganography algorithm fails; encryption algorithm will make the encrypted secret message to be displayed to intruder instead of original secret message. displayed to intruder instead of original secret message. Encrypted Secret message is embedding in cover audio file using this proposed methodology.

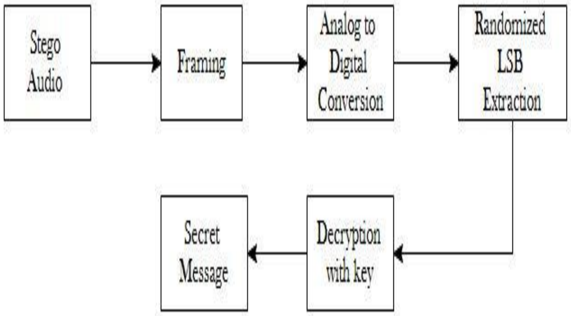

Fig 2: Randomized LSB Technique Decoder Module

Fig 2 shows the receiver part of thismethodology. The Stego audio file is converted intodifferent frames and then converted into digital form. On the basis of encoder, decoding part is performed. So the secret message bits are extracted from different samples. Decryption process is exactly reverse operation of encryption.

B (a). Bit Selection mapping

In order to confuse the third party, same bits of cover audio sample shouldn’t be used to embed the secret message bits. So, proposed method produces randomness in selecting different bits of a sample. First two MSB (Most Significant Bit) of each sample are going decide which bit of the same sample would contain the secret message bit. Following TABLE Ishow the proposed bit selection mapping. In this method only first three LSB bits are used to embed secret message bit.

If the first two MSB bits are equal to ‘00’, then third LSB will be replaced with secret message bit. If the first two MSB bits are equal to ‘01’, then second LSB will be replaced with secret message bit. If the first two MSB bits are equal to ‘10’or ‘11’ then first LSB will be replaced with secret message bit.

TABLE I
BIT SELECTION MAPPING

1st MSB	2nd MSB	Secret Message Bit
0	0	3rd LSB
0	1	2nd LSB
1	0	1st LSB
1	1	1st LSB

B (b). Sample Selection Mapping

It proposes another way to confuse third party, means it add some more randomness in embedding process by selecting random samples of a cover audio file. So, all the samples of audio file will not contain secret message bit but only few will contain. Here also the randomness is obtained by using first three MSB values of a sample. TABLEII shows this sample selection mapping. In this process some of the samples are skipped in between embedded samples.

TABLE II
SAMPLE SELECTION MAPPING

1^{st}MSB	2^{nd} MSB	3^{rd} MSB	Sample containing next secret Message bit
0	0	0	k+1
0	0	1	k+2
0	1	0	k+3
0	1	1	k+4
1	0	0	k+5
1	0	1	k+6
1	1	0	k+7
1	1	1	k+8

Consider k is the initial value of sample, the last column of TABLE II shows that next sample contain the secret message bit. In this process number of sampleare skipped in between two consecutive secret message bits. Initially (k=1), if the first three MSBBits of cover audio samples are equal to '010', then the last column indicates the next sample (k+3=4) contains second secret message bit. It means that, first secret message bit is embedded in first sample and next message bit is saved in fourth sample. In the same way, the fourth sample of audio file is equal to '011', and then the third message bit will be saved in eight sample of audio file.

III. METHODOLOGY

Randomized LSB algorithm -At the Sender side.
Input: Cover Audio file, Key and Secret Message
Output: Stego Audio File.
Step 1: Read the audio file
Step 2: Input the secret key for encryption
Step 3: Divide the Audio file into different framesand convert these number of audioframes in the form of bytes. The bytes arerepresented in the form of bit patterns by passing through ADC.
Step 4: Using theencryption key, the original message is encrypted using AES-128 algorithm.
Step 5: Split the Encrypted message bit patterns vertically into one column
Step 7: Insert the secret message bit into randomized LSB bits of the particular audio frame.
Step 8: Repeat the above Step for the remaining bits of encrypted text file.Combine the frames of audio files bit patterns.

Randomized LSB algorithm -At the Receiver side.
Input: Stego audio file, Key
Output: Original Secret Message, audio file.
Step 1: Read the Stego file
Step 2: Input the secret key for decryption (which is used for encryption)
Step 3: Extract the embedded data and audio files bit patterns from stego file.
// Reverse process of step 7 of randomized LSB algorithm at Sender side.
Step 4: Combine the frames of audio files bit patterns.

IV.A VARIABLE BIT APPROACH

As discussed earlier, LSB technique is most common method of audio steganography bitwise approach is considered. However, here higher order bit is used for embedding secret message bit. Instead of simply inserting the message bit in the cover audio sample value, the available sample byte value is replaced with nearest byte value, in which this nearest byte value has the relevant bit set or reset as per requirement. This method shows that, the entire byte value is changed so it is difficult to break this method and get the secret message.

C. The Concept

This method needs to be initialized with the bit position where message bit to be hidden. Consider that value as 'n'

Bitmask = $2^{(n-1)}$
Mask = $255 - (2^{(n-1)} - 1)$
Period = 2^{n}
Deviation = period/2
When these constants are initialized, need to define insert function for individual bytes to hide secret message bit at the n^{th} position.

Mathematically this insert function can be given as:

b'=b&mask
flag =b'mod period
b1=b'+ deviation
b2=b'−1

$$g\,(b) \;=\left\{\begin{matrix} b1 & \text{if } |b1-b| < |b2-b| \\ b2 & \text{otherwise} \end{matrix}\right\}$$

$$\text{Insert }(b,\text{bit}) \;=\begin{Bmatrix} g(b) & \text{if message bit} = 1 \text{ and flag} = 0 \\ g(b) & \text{if message bit} = 0 \text{ and flag} \neq 0 \\ b & \text{otherwise} \end{Bmatrix}$$

The resulting byte contains secret message bit at the specified n^{th} position.

Example 1: TheTABLE shows some of the values of insert function. In the TABLE III given, consider the first row. The first value present is 176 and the bit to be inserted is 1 at the byte position of 2 from the right side. From the mathematical calculation, the closest byte value in which it has the bit value of '1' at the bit position of 2 is 175. Therefore the byte value 176 is changed to 175.
Example 2: In the TABLE III given, consider the 8th row. The value present is 45 and the bit to be inserted is '0' at the byte

position of 4 from the right side. From the mathematical calculation, the closest byte value in which it has the bit value of '0' at the bit position of 4 is 48. Therefore the byte value 45 is changed to 48.

TABLE III
BYTE VALUES FROM THE INSERT FUNCTION

Byte Read		Bit to be inserted	Saved at Bit	Byte returned	
Binary	Decimal			Binary	Decimal
10110000	176	1	2	101011**1**1	175
10111101	189	1	2	101111**1**0	190
01110101	117	0	2	011101**0**1	117
00101101	45	0	3	00101**0**11	43
01011110	94	1	3	01011**1**10	94
01110101	117	0	3	01110**0**11	115
00010000	16	1	4	0000**1**111	15
00101101	45	0	4	0011**0**000	48
10110000	176	1	4	1010**1**111	175

V. IMPLEMENTATION

Increasing the number of altered LSBs will introduce more noise. If this noise is more than the threshold level then it becomes detectable by third party using any steganalysis method. Audio steganography is implemented on the basis of fixed LSBs.This proposed method produces some randomness in selection of bits and also selection of samples from cover audio data. The original audio file is shown in Fig. 3. The resulting Stego audio file (retrieved audio) after embedding secret message is shown in Fig. 4. It is clear that, there is not much difference in original audio data and retrieved audiodata by modifying the first three LSBs.

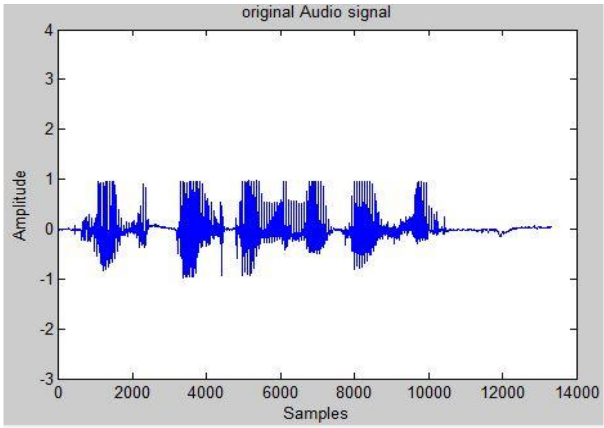

Fig. 3: Original (cover) Audio File (proposed LSB Method)

Initially, the secret information at the sender side is encrypted by using AES-128 cryptographic algorithm. It makes the relation between plain text and cipher text complex. Cover audio data and Encrypted information is converted into binary digits. A secret information **“SIRMVISVESVARAYA”** is encrypted into audio frame as ”**§K²šà IÕ™\®□ _**”.

By using proposed bit selection method secret information bits are embedded in first, second and third LSBs of cover audio. It embeds the secret information bits in selected LSB bits with selective samples. Fig. 5 shows the audio frame before embedding text and Fig. 6 shows the audio frame after embedding text respectively. Plot and audibility of cover (original) audio and stego (retrieved) audio are not differentiable.

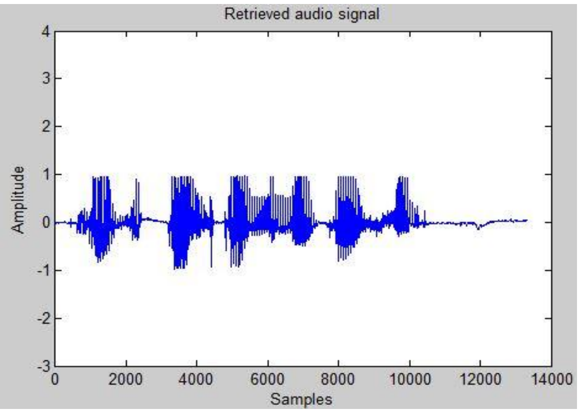

Fig. 4: Retrieved (stego) Audio File (proposed LSB Method)

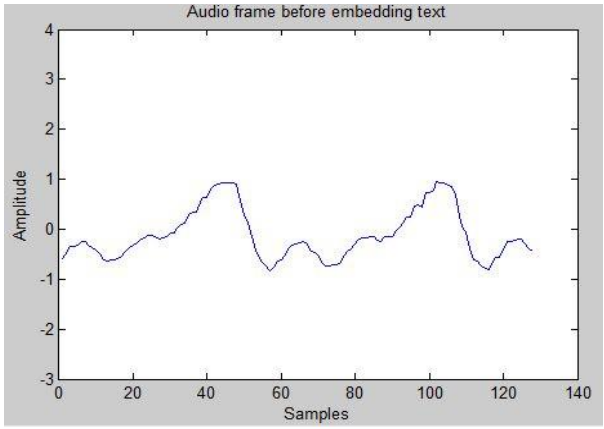

Fig. 5: Audio Frame before Embedding Text (LSB Method)

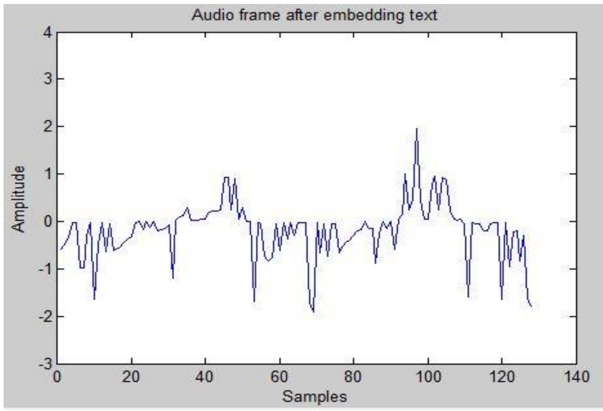

Fig. 6: Audio Frame after Embedding Text (LSB Method)

Another algorithm for audio steganography is variable bit approach. Instead of simply embedding the relevant bit in LSB,the whole byte value is modified so that it holds the data being nearest to the original byte value. It uses nth order of bits to hide this method and get the secret information. Fig. 8 shows thedata. The entire byte value is changed so it is difficult to break retrieved audio data when position of bit saved at' 2'. Fig. 9 Shows the retrieved audio data when position of bit saved at '3'. However, when the position of bit is saved at '1' will not make any difference in plot and audibility.

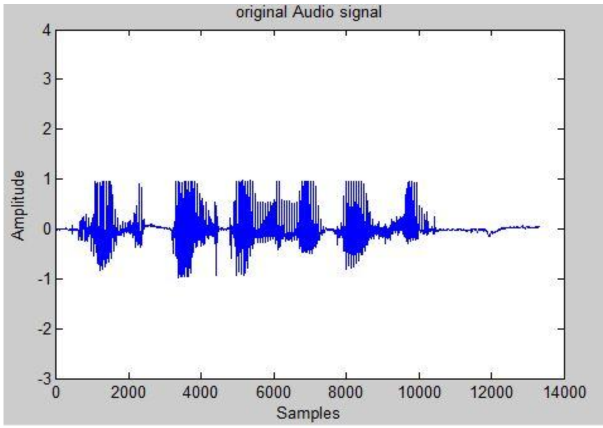

Fig. 7: Original (cover) Audio File (Variable Bit Method)

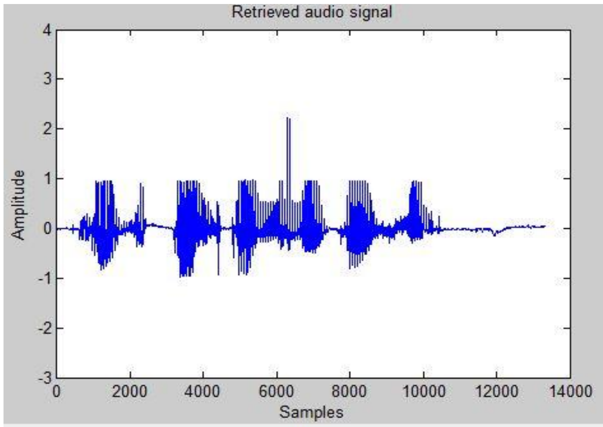

Fig. 8: Retrieved Audio File (Variable Bit Method When n=2)

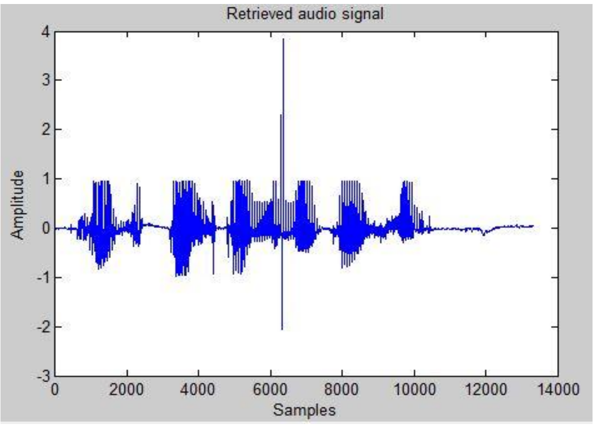

Fig. 9: Retrieved Audio File (Variable Bit Method When n=3)

VI. RESULTS AND COMPARISION

Transparency and robustness can be measured in terms of Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). MSE is given by equation (1) and PSNR is defined by equation (2).

$$\mathrm{MSE} = \frac{1}{N}\sum_{\mathrm{i}=1}^{\mathrm{N}}(\mathrm{xi}-\mathrm{yi})^{2} \ (1)$$

$$\mathrm{PSNR} = 20\log_{10}\left(\frac{2^{\mathrm{max}}-1}{\sqrt{\mathrm{MSE}}}\right)(2)$$

where N defines the total number of samples of the cover audio, max is the number of bits in one sample,xi is ith sample in cover audio signal(x), yi is the ith sample in stego audio signal(y) and value of i should be same for both original and stego audio signal.Secret message bits are inserted in binary form of cover audio, as shown in TABLE I and TABLEII. The example secret message with 128 bits and 128 AES key bits are used to embed in five different cover audio data.

TABLE IV
PERFORMANCE ANALYSIS OF MSE AND PSNR

Cover Audio	Randomized LSB Method		Variable Bit Approach			
			When n=2		When n=3	
	MSE	PSNR (dB)	MSE	PSNR (dB)	MSE	PSNR (dB)
digital.wav	2.98e-11	153.39	7.73e-5	89.24	2.87e-4	83.54
good morning.wav	3.75e-11	152.39	1.11e-4	87.68	1.83e-4	85.49
primeminister.wav	**4.72e-12**	**161.39**	4.09e-5	92.05	**4.66e-5**	**91.44**
telecommunication.wav	1.20e-11	157.33	6.46e-5	90.03	1.15e-4	87.51
sit_tumkur.wav	5.19e-12	160.98	**3.50e-5**	**92.69**	1.03e-4	88.05
Average	**1.78e-11**	**157.09**	**6.57e-5**	**90.32**	**1.47e-4**	**87.20**

A comparison of proposed randomized LSB method with variable bit method is made in TABLE IV.Proposed technique uses all three random LSBs, the PSNR of the randomized LSB method is larger and indicating more transparency and robustness.

VII. CONCLUSION

The conventional LSB modification techniques are easy for steganalysis. A randomized LSB model for audio Steganography is presented in this paper.TheCryptography (encryption) technique is applied to secret message bits, thus it changes the representation of the secret message. This change in representation of secret message bits increases robustness, but the use of secret key decreases the capacity.For Audio Steganography, the main challenge is the perceptual quality of the stego audio file which is satisfied in proposed method. The proposed method meets all the requirements in hiding the secret information and it is satisfied with working against steganalysis. There is not much difference between original and retrieved audio signal i.e hidden information recovered without any error. Variable bit method also difficult for steganalysis but transparency is very less. When compared with variable bit approach proposed system satisfied all the requirements such as capability, security and robustness for secure data transmission.

REFERENCES

[1] Muhammad Asad, Junaid Gilani, Adnan Khalid **“An Enhanced Least Significant Bit Modification Technique for Audio Steganography”,** 978-1-61284-941-6/11/ ©2011 IEEE

[2] Kaliappan Gopalan **“A Unified Audio and Image Steganography by Spectrum Modification”,** International Conference on Industrial Technology, 2009, Page(s): 1 - 5.

[3] Gopalan, K., **"Audio Steganography Using Bit Modification",** 2003 IEEE International Conference on Acoustics, Speech, and Signal Processing, Page(s): II - 421-4 vol.2.

[4] Gaurav Saini, Parulpreet Singh**“Audio Steganography by LSB Method and Enhanced Security with AES”,**International Journal of Advanced Research in Computer Science & Technology (IJARCST),Vol. 2, Issue 2, Ver. 2 (April - June 2014)

[5] Yali Lillo Ken Chiang, Cherita Corbett, Rennie Archibald, Biswanath Mukherjee, Dipak Ghosal, **"Novel Audio Steganalysis Based on High-Order Statistics of a Distortion Measure with Hausdorff Distance"**, ISC '08 Proceedings of the 11th international conference on Information Security.

[6] Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly,Swarnendu Mukherjee and Poulami Das **“Tutorial review on steganography”** University of Florida and Jaypee Institute of Information Technology University.

[7] Jayaram P, Ranganatha H R, Anupama H S, **“Information Hiding Using Audio Steganography – A Survey”** ,The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011.

[8] K.P. Adhiya and Swati A.Patel, **“Hiding Text in Audio using LSB Based Steganography”**, Information and Knowledge Management , ISSN 2224-5758 (Paper) ISSN 2224-896X (Online), Vol. 2, No.3, 2012.

[9] K. Geetha, P.Vanitha Muthu, **“Implementation of ETAS (Embedding Text in Audio Signal) Model to Ensure Secrecy”,** International Journal on Computer Science and EngineeringVol. 02, No. 04, 2010, 1308-1313.

[10] Soumya Banerjee, Saikat Roy, M.S.Chakraborty, Simpita Das,**“A Variable Higher Bit Approach to Audio Steganography”**,978-1-4799-1024-3/13/©2013 IEEE.