Performance Improving LSB Audio Steganography Technique

Burate D. J.[1]
Student ME (E & TC)
Kolhapur Institute of Technology Gokulshirgaon
Kolhapur - India

M. R. Dixit[2]
Associate Professor, Department of Electronics Engineering
Kolhapur Institute of Technology Gokulshirgaon
Kolhapur - India

Abstract: Boosted by recent advances in the information technology field, methods applied to ensure privacy of digital data became very important in many real life applications. Efficient secrecy can be achieved at least in part, by implementing Steganography techniques. In this paper, we propose a new technique to hide text in speech in noise free environment. We opted to work in the digital domain and hide the text information within speech signal using audio steganography technique. More precisely, our method increases the hiding data rate. We better preserve the originality of the speech carrier by employing an embedding rather than a replacement operation on the secret text. To increase security steganography combined with cryptography, but our method doesn't use any of the cryptography technique, it uses coding technique. Our simulation results show that this approach maintains the robustness of the cover signal and achieves a higher hiding capacity for different audio and speech signal sampled at different frequencies as well as read at different bit rates. Our proposed method shows high hiding capacity as compared with other technique.

Keywords: Audio Steganography, LSB, High Hiding Capacity, M.O.S., TII.

I. INTRODUCTION

The fast improvement of the Internet and the digital information revolution caused major changes in the overall culture. Flexible and simple-to-use software and decreasing prices of digital devices (e.g. portable CD and MP3players, DVD players, CD and DVD recorders, laptops, PDAs) have made it feasible for consumers from all over the world to create, edit and exchange multimedia data. Broadband Internet connections almost an errorless transmission of data helps people to distribute large multimedia files and makes identical digital copies of them [5]. In modern communication system Data Hiding is most essential for Network Security issue. Sending sensitive messages and files over the Internet are transmitted in an unsecured form but everyone has got something to keep in secret. Three main methods are being used: encryption, watermarking, and 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. The word steganography is of Greek origin and means "covered writing" from the Greek words steganos means "covered or protected", and graphy means "writing". Covers can be of different types including image files, audio and video, text and IP data gram. Several methods of audio and video data hiding have been proposed and demonstrated whether in time domain as well as in frequency domain. Due to lack in hiding capacity of existing text-based steganography, a new technique will be proposed to hide larger quantity of data using speech as a medium cover [5].

General principles of data hiding technology, as well as terminology adopted at the First International Workshop on Information Hiding, Cambridge, U.K. [6] are illustrated in Figure.
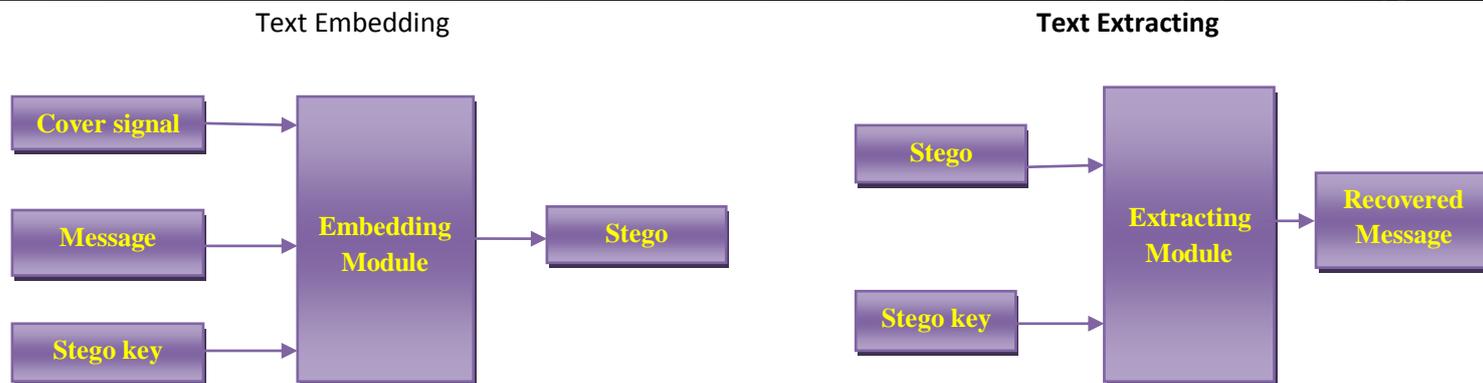
Burate D. J. [1]
M. R. Dixit [2]

International Journal of Advance Research in Computer Science and Management Studies
Volume 1, Issue 4, September 2013 pg. 67-75

Text Embedding

Text Extracting

Fig 1. Block diagram of Steganography.

A. *Terms used in Steganography [6]:*

- Cover/ Carrier file:Also known as envelope which carries hidden text, these are of different type as male voice speech, female voice speech, music signal with different duration are collected.

- Stego key: a key is used to do embedding.

- Embeddor: is a block which will hide text in cover signal according with which technique or method used.

- Stego signal: Cover signal after embedding text in it is called stego signal .embedding should be like, it is impossible to distinguish between cover and stego signal.

- Extractor/ Detector: is a block which takes stego signal as input and extract hidden text from it.

B. *An effective steganographic scheme should posses the following desired characteristics [4]:*

- **Secrecy:** A person should not be able to extract the covert data from the host medium without the knowledge of the proper secret key used in the extracting procedure.

- **Imperceptibility:** The medium after being embedded with the covert data should be indiscernible from the original medium. One should not become suspicious of the existence of the covert data within the medium.

- **High capacity:** The maximum length of the covert message that can be embedded should be as long as possible.

- **Resistance:** The covert data should be able to survive when the host medium has been manipulated, for example by some lossy compression scheme.

- **Accurate extraction:** The extraction of the covert data from the medium should be accurate and reliable. Basically, the purpose of steganography is to provide secret communicate like cryptography.

II. PRESENT TECHNIQUES

Techniques used for Audio Steganography:

A. Least Significant Bit (LSB) Coding[2]: 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. That's usually an effective technique in cases where the LSB substitution doesn't Cause significant quality degradation. For example The LSB represents a value of 1.

For example, to hide the letter "D" (ASCII code 68, which is 01000100) inside eight bytes of a cover, set the LSB of each byte by selecting one bit of the text data at a time and correcting the LSB of the envelope data bytes accordingly as fallows.

Burate D. J. [1]
M. R. Dixit [2]

International Journal of Advance Research in Computer Science and Management Studies
Volume 1, Issue 4, September 2013 pg. 67-75

Original Audio Bytes	Text data to hide	Text data Embedded Audio Bytes
1001001**0**	0	1001001**0**
0101001**1**	1	0101001**1**
1001101**1**	0	1001101**0**
1101001**1**	0	1101001**0**
1000101**0**	0	1000101**0**
0000001**0**	1	0000001**1**
0111001**0**	0	0111001**0**
0010101**1**	0	0010101**0**

B. Parity coding: One of the prior works in audio data hiding technique is parity coding technique. Instead of breaking a signal down into individual samples, the parity coding method breaks a signal down into separate frame of samples and encodes each bit from the secret message in a sample region's parity bit. If the parity bit of a selected region does not match with the secret bit to be encoded, the process flips the LSB of one of the samples in the frame. Thus, the sender has more of a choice in encoding the secret bit, and the signal can be changed in a more unobtrusive fashion [2]. Fig 2 shows the parity coding procedure.
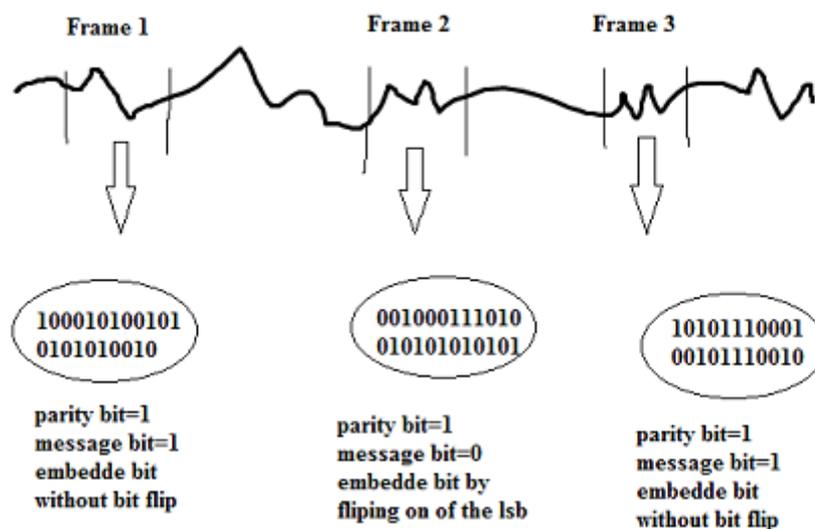
Fig 2. Parity coding procedure

C. Phase Coding: The phase coding method works by substituting the phase of an initial audio segment with a reference phase that represents the data. The phase of subsequent segments is adjusted in order to preserve the relative phase between segments. New phase allocated to the signals are given below

$$\text{New phase} = \pi/2 \quad \text{if symbol o is embedded}$$
$$= -\pi/2 \quad \text{if symbol 1 is embedded}$$

D. Spread Spectrum Technique: In a normal communication channel, it is often desirable to concentrate the information in as narrow a region of the frequency spectrum as possible in order to conserve available bandwidth and to reduce power. The basic spread spectrum technique, on the other hand, is designed to encode a stream of information by spreading the encoded data across as much of the frequency spectrum as possible.

Burate D. J. [1]
M. R. Dixit [2]

International Journal of Advance Research in Computer Science and Management Studies
Volume 1, Issue 4, September 2013 pg. 67-75

E. Echo hiding [2]: In echo hiding, information is embedded in a sound file by introducing an echo into the discrete signal. Like the spread spectrum method, it too provides advantages in that it allows for a high data transmission rate and provides superior robustness when compared to the noise inducing methods.

III. PROPOSED TECHNIQUE

With reference to literature survey LSB technique gives best results hence considered for implementation. The present steganography techniques take help of well known cryptography algorithm to increase security level. But our proposed method uses other coding technique. The message to be embedded is first converted to decimal then converted to binary. After words it is converted to matrix whose rows are equal to total no of character to be embedded. Then that matrix is converted to column matrix. And then each bit is embedded into LSB of each audio sample.

When embedding the textual information in any audio file, first the audio signal is converted into bits. Then the message to be embedded is converted from above strategy. By applying LSB algorithm, the message is embedded into audio sample read at 16 bit format.

Encoding Algorithm and Decoding Algorithm:

Encoding Algorithm:

- Input the text to be embedded.
- Convert the text into binary bit and forms coded text by coding it as described above
- Read WAV audio file as cover file find header and total count size.
- Find size of message, if size of message is more than count size, display message 'message is too big' select small message.
- Select audio sample and first hide key and then converted code of the text in WAV file using LSB algorithm.
- Repeat the above step still the whole message will be embedded in audio.

Decoding Algorithm:

- Read the stego file i.e. covers audio after embedding.
- Extract the message by reading LSB.
- Extract key from audio samples if key matches then extract hidden message otherwise display message as 'no message is hidden'.
- Select all samples and store all LSB position bits in array.
- Divide the array into number of rows and columns, convert binary hex and then into ascii character.
- Display the secret message.

Burate D. J. [1]
M. R. Dixit [2]

International Journal of Advance Research in Computer Science and Management Studies
Volume 1, Issue 4, September 2013 pg. 67-75

IV. FLOW CHARTS

Encoding Algorithm:

```
              ┌─────────────────────────────┐
              │  Input the text to be embedded │
              └─────────────────────────────┘
                           │
              ┌─────────────────────────────┐
              │  Convert it into coded text using coding
              │            technique          │
              └─────────────────────────────┘
                           │
              ┌─────────────────────────────┐
              │  Read WAV audio file as cover file
              │   find header and total count size │
              └─────────────────────────────┘
                           │
              ┌─────────────────────────────┐
              │      Find size of message     │
              └─────────────────────────────┘
                           │
                  ╱─────────────────────╲       Yes   ┌────────────────────────┐
                 ╱  Message size > count size ╲──────────│  Message too big select │
                  ╲─────────────────────╱              │     small message       │
                           │ No                          └────────────────────────┘
              ┌─────────────────────────────┐
              │  Select audio sample and first hide key │
              └─────────────────────────────┘
                           │
              ┌─────────────────────────────┐
              │  Hide converted code of the text in WAV file
              │         using LSB algorithm   │
              └─────────────────────────────┘
                           │
              ┌─────────────────────────────┐
              │  Repeat the above step still the whole
              │  message will be embedded in audio │
              └─────────────────────────────┘
                           │
              ┌─────────────────────────────┐
              │       Stego signal is formed  │
              └─────────────────────────────┘
```
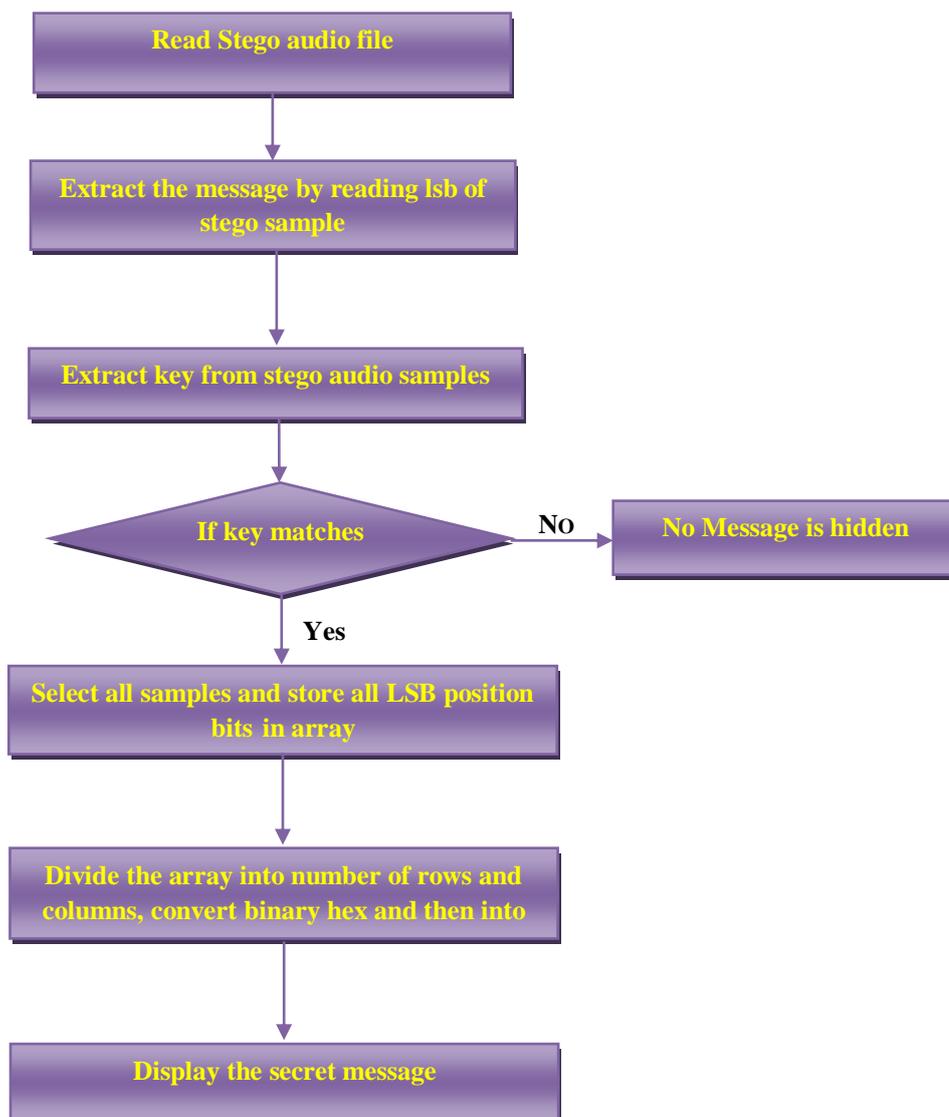
Decoding Algorithm:

```
                    ┌─────────────────────────────┐
                    │    Read Stego audio file    │
                    └─────────────────────────────┘
                                  │
                                  ▼
                    ┌─────────────────────────────┐
                    │ Extract the message by      │
                    │ reading lsb of stego sample │
                    └─────────────────────────────┘
                                  │
                                  ▼
                    ┌─────────────────────────────┐
                    │ Extract key from stego      │
                    │ audio samples               │
                    └─────────────────────────────┘
                                  │
                                  ▼
                       ◇ If key matches ◇ ──NO──► ┌──────────────────────┐
                                  │                │ No Message is hidden │
                                 Yes               └──────────────────────┘
                                  ▼
                    ┌─────────────────────────────┐
                    │ Select all samples and      │
                    │ store all LSB position      │
                    │ bits in array               │
                    └─────────────────────────────┘
                                  │
                                  ▼
                    ┌─────────────────────────────┐
                    │ Divide the array into       │
                    │ number of rows and columns, │
                    │ convert binary hex and then │
                    │ into                        │
                    └─────────────────────────────┘
                                  │
                                  ▼
                    ┌─────────────────────────────┐
                    │   Display the secret message│
                    └─────────────────────────────┘
```

V. RESULTS

This Steganography is implemented in Matlab 7.10. To measure the performance of proposed method, MOS (Mean Opinion Score strategy is used. Mean value is calculated by asking people about the difference in the original wav file and embedded wav file. This rating is done on 5 point scale. The LSB algorithm is tested for data rates at different frequencies. In order to evaluate the sound quality after embedding the secret message into audio files, test carried out known as MOS, original & stego signals are plotted in time domain to find difference between them.

A. *Mean Opinion Score (MOS):*

Subjective quality evaluation for the text hiding in audio has been done by listening tests involving twenty persons. The audio files are categorized as per number of bits per sample, number of channels. The entire tests have been carried out at each category of sound files. Initially in the first part repeatedly presented the audio clips with hidden text and audio clips without hidden text into it, in random order to the listeners. Listeners were asked to determine which one is the audio with text hidden in it and without it. To calculate the mean opinion score, five point scales is used by the individual after listening the music file and final mean of all scores is M.O.S. Mean Opinion Score for all four categories of sound are as shown in Table1. This five-point scale is defined in the following manner as given under, using a 5-point impairment scale [1]:

5: Imperceptible

Burate D. J. [1]
M. R. Dixit [2]

International Journal of Advance Research in Computer Science and Management Studies
Volume 1, Issue 4, September 2013 pg. 67-75

4: Slightly Perceptible but not noisy

3: Slightly noisy

2: Noisy

1: Very Noisy

Table 1: showing MOS score for different types of audio signal

Sr.No.	Audio signal at different frequencies	MOS
1	Stego-8k-s1(a cover is a song ,sampled at f_s=8khz)	4.6
2	Stego-16k-m1 (a cover is a male speech, sampled at f_s=16khz)	4.8
3	Stego-44.1k-s1 (a cover is a song, sampled at f_s=44.1khz)	4.8
4	Stego-48k-f1 (a cover is a female speech, sampled at f_s=48khz)	5

B. *High Hiding Data Rate:*

As compared with other lsb technique proposed technique have high capacity of hiding / embedding text in a audio signal. The following table shows the hiding capacity for audio signal sampled at different frequencies for different types of cover. One more point considered is Text Intelligibility Index (TII) which gives how much text extracted correctly. It is calculated by analyzing original text and recovered text .Table shows the maximum length of messages that can be embedded in a cover. Hiding capacity is same for different types of cover samples such as song, male speech, and female speech.

Table 2: show maximum hiding capacity of different cover signals sampled at different frequencies with TII

| Sr.No.	Cover sampled at frequency f_s		Length of sample	The rate at which wave data read	Total char hidden	Total bit hidden	Text intelligibility index(TII)
1	8 kHz	Song sample	1 Sec	16 bit	2067	16536bits/ 16.5kbps	100%
		Male speech sample					
		Female speech sample					
2	16 kHz	Song sample	1 Sec	16 bit	4163	33304Bits/ 33.3kbps	100%
		Male speech sample					
		Female speech sample					
3	44.1kHz	Song sample	1 Sec	16 bit	11504	92032bits/ 92kbps	100%
		Male speech sample					
		Female speech sample					
4	48 kHz	Song sample	1 Sec	16 bit	12207	97656 bits/ 97.6kbps	100%
		Male speech sample					
		Female speech sample					

C. *Time Domain Representation:*
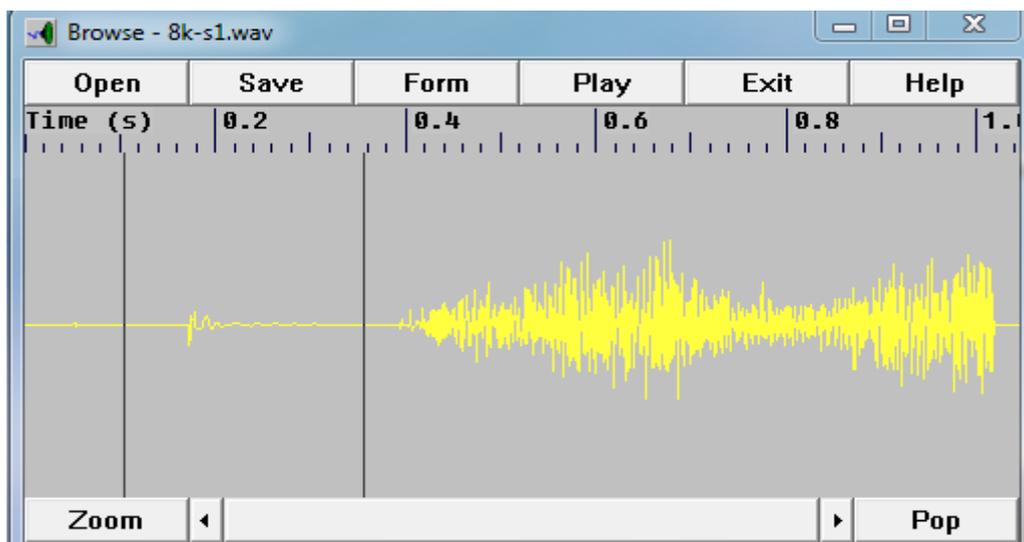
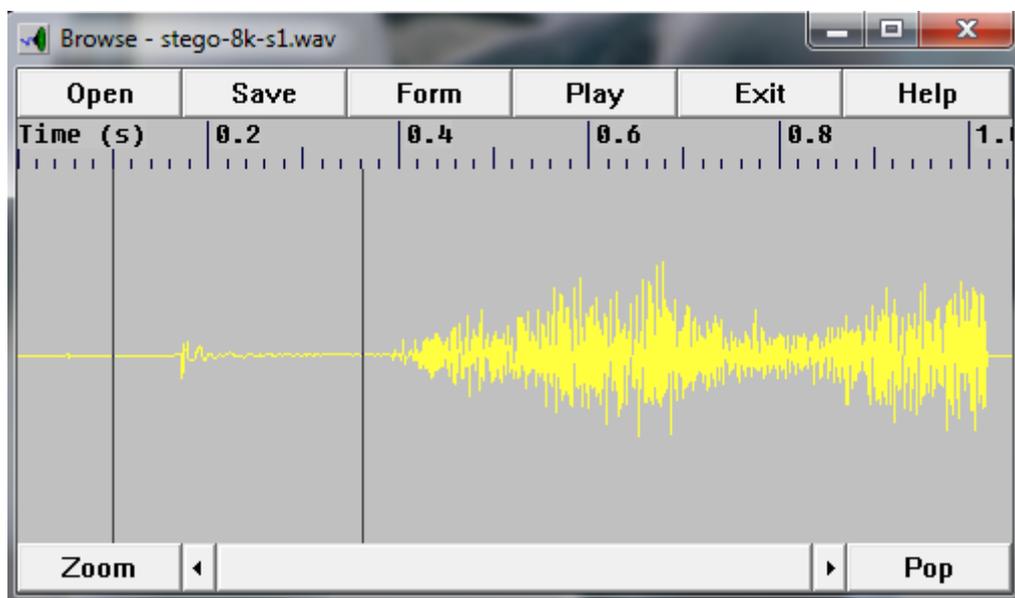*Fig 3. Original cover signal of type song sampled at f_s=8 kHz*

Fig 4. Stego signal of type song sampled at f_s=8 kHz

Similarly the graph of original and stego signal obtained at different sampling frequencies can be shown. From the above two figures it indicates that there is change in time domain REPRESENTATION OF both SIGNALS, but it is inaudible when heard.

VI. CONCLUSION

The proposed method is improved version of the LSB technique used as audio steganography, combined with coding technique gives high embedding capacity. Listening test is carried out to find Minimum Opinion Score (MOS) which satisfies imperceptibility quality. Text Intelligibility Index (TII) shows 100% correct extraction of the embedded text, for different message length, which varies from 16.5 kbps minimum to 97.6 kbps maximum length of messages. Time domain representation of original and stego signals show variations, but the effect of these variations is inaudible when the two audio signals heard separately. Proposed technique is applied to various audio, speech and music envelope signals and it gives best results satisfying steganography concept.

Burate D. J. [1]
M. R. Dixit [2]

International Journal of Advance Research in Computer Science and Management Studies
Volume 1, Issue 4, September 2013 pg. 67-75

References

1. K.P.Adhiya Swati A. Patil CSE Dept. SSBT's COET Bambhori,Jalgaon,Bambhori,India "Hiding Text in Audio Using LSB Based Steganography" Information and Knowledge Management Vol 2, No.3, 2011.

2. Jayram p, Ranganatha H R,Anupama H S"Inforamation Hiding Using Audio Steganography- A Survey". The international journal of Multimedia & Its application (IJMA) Vol.3, No.3 , August 2011

3. H.B.kekre , Archana Athawale , "Information Hiding In Audio Signal".Intertional Journal of Computer Application volume 7-No.9 October 2010

4. Pramatha Nath Basu, On "Embedding of Text in Audio – A case of Steganography"International Conference on Recent Trends in Information, Telecommunication and Computing, 2010

5. J. Johnston and K. Brandenburg, "Wideband Coding Perceptual Consideration for Speech and Music". Advances in Speech Signal Processing, S. Furoi and M. Sondhi, Eds. New York: Marcel Dekker, 1992.

6. Pfitzmann, "Information Hiding Terminology", First International Workshop on Information Hiding, Ma 30 – June 1, 1996, Cambridge, UK, pp.347-350

AUTHOR(S) PROFILE

Ms.D.J.Burate, received the B.E. degree in Electronic and Telecommunication Engineering from Bharati Vidyapeeths College Of Engineering Kolhapur in 2009. Was working as Assistant Professor in electronics department at Bharati Vidyapeeths College Of Engineering Kolhapur for last 4 years.

Mrs.M.R.Dixit, received the B.E. and M.E. Degree in Electronic Engineering from Walchand College of Engineering Sangali in 1985 and 1992 respectively. She has got 28 years of teaching experience at under graduate level and 8 years of experience at post graduate level. Currently she is working as associate professor electronics department at college of engineering Kolhapur, her fed of interests are microwave engineering, digital signal processing, image and speech processing .She has worked as Board Of Studies (BOS) member for E&TC in Shivaji University. She has also worked as cenate member at Shivaji University. She has guided 28 PG Student and published 18 papers in international journals.