Webology (ISSN: 1735-188X)
Volume 18, Number 6, 2021

# A Digital Information Security Using Proposed Audio Steganography Approach

**Santosh Gaikwad [1], Bharti Gawali [2], Sandeep Thorat [3]**

[1]Department of Computer Science, Dr. Babasaheb Ambedkar Marathwada University Constituent Model College Ghansawangi, Jalna, India.

[2,3]Department of Computer Science and IT, Dr. Babasaheb Ambedkar Marathwada University, Aurangabad.

## Abstract

In the current era of digital technology, information security is a challenging task. For the secrete communication information hiding is an essential element. The current information steganography system uses objects like audio, image, and video. The audio steganography is the technique that convey hidden message by modifying an audio signal in an unnoticeable manner. It is technique for the hiding secrete message in the host audio signal. The original audio message before steganography and after encoding message has uniform characteristics. The embedding secrete audio message in the original audio file is a more challenging and difficult task.

This paper presents a comprehensive survey of audio steganography techniques for information security. The experiment was tested using proposed LSB technique for audio steganography. This paper extended towards quality measure of steganography message. The quality of audio steganography measures using energy score, Mean square error, Peak signal to noise ratio. From this experiment the quality of audio steganography is observed as 92.759 % for M.S.E and 94.971 % for PSNR technique. Audio information hiding is one of the robust and dynamic ways of protecting privacy and secreting communication.

**Keyword** Information, Steganography, quality, LSB, PSNR, MSE, quality, Energy, HAS.

## 1. Introduction

In this era of rising technologies, digital communication has become an integral and significant part of everyone's life. In the rapid development of digital communication, information security becomes an important concern. The methods and algorithm available for digital data security use a cryptographic primitive for secure data transmission and secrete communication.

With the advent of technology, people started to private communication for sharing and transmission using the technological approach. As a result, securing these secrete message became a critical issue for everyone. Cryptography and Steganography are two security methods for secure

data communication and data confidentiality [1]. In the cryptography method it ciphers the secrete message, so that it cannot be readable by everyone without part of that communication, while steganography hides the secret message into an original file so that it cannot be seen by eavesdroppers [2]. For the third-party user an encrypted message would right away imply a secret communication. The hidden message is not able to draw any attention and therefore would not raise suspicions that it is a secret communication. Due to this reason steganography is often regarded as a surreptitious method for transmitting receptive information into total secrecy across public channels [3]. Audio steganography is a type of digital steganography, which hides digital information into the digital audio media [4]. Human Auditory System (HAS) cannot observe slight variation of high frequency based audible message so; audio steganography has a great choice for secrete communication [5]. The hiding speech in the audio file algorithms could be embedded message with the bit rate that is a considerable portion of the host audio bit rate, up to 150 kbps [6]. The robustness of the audio steganography method is referred to as the capability of the data detector to extract the embedded message after common signal processing manipulations [7].

This paper presents a comprehensive survey of audio steganography techniques for information hiding. The LSB technique was used for the implementation of audio steganography. The experiment tested in time domain and frequency domain.

The rest of the paper is structured in seven sections. Audio steganography is described in section 2. Related work is explained in section 3. The techniques of audio steganography are illustrated in section 4. Section 5 deals with proposed techniques for audio steganography. Experimental analysis is described in section 6. Section 7 deals with conclusion followed by references.

## 2. Audio Steganography

Audio steganography is the ability and science of thrashing digital information such as text messages, documents, and binary files into audio files. The primary message is known as the carrier signal or message and the secondary message is known as the payload signal or message. Characteristically normal audio file and carrier file are same and not recognized in tapping communication technology [8]. The general steganography technique is shown in figure 1.

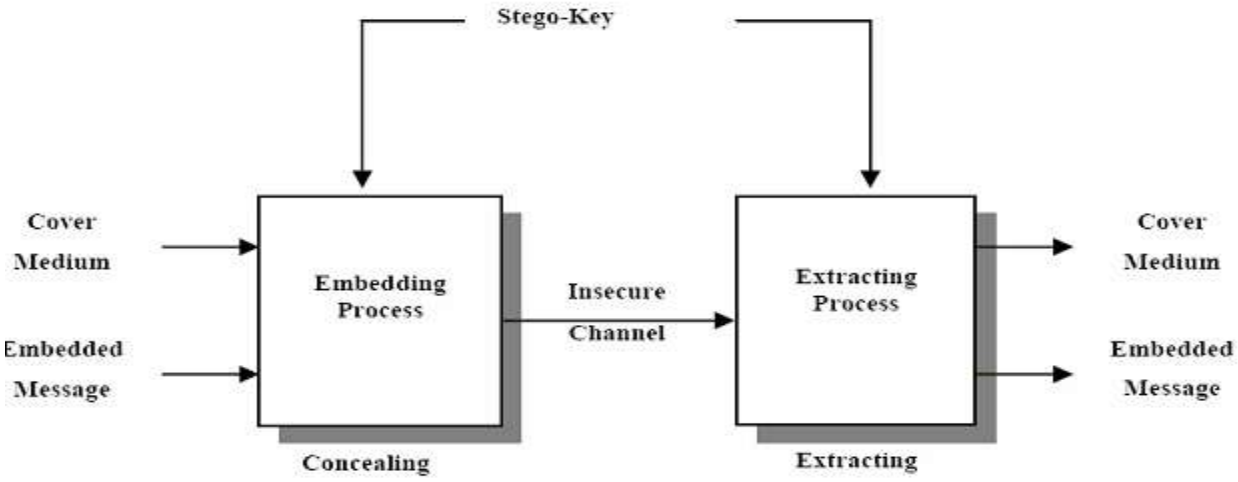


Figure 1: general steganography system

Steganography can be achieved by means of three types of techniques: injection, substitution, and generation. The insertion technique is embedded the data to cover in the insignificant part of the carrier file, which is normally unseen by operating systems and application software. The substitution technique substitutes the insignificant bits in the original carrier message with the bits of the data to secrete. Insignificant bits are those bits that can be modified without destroying the eminence or destroying the reliability of the carrier message. This technique takes advantage of the limited abilities of the human auditory system (HAS), which cannot identify two sounds that are slightly not alike. The generation technique examines the data to cover and produces out of them a new set of data. It is a dynamic method of creating a carrier message based on the information enclosed in the data to cover [9].

## 3. Related Work

Researchers proposed a three-layered architectural model for audio steganography which defines the replacement of Least Significant Bit. Before storing the cover message into the last layer, the private message to be transmitted and it is passed through the two layers. The stego message is transmitted over the network towards the receiver side and secrete message is obtained by performing the operations in reverse order. The main objective of the paper is to keep the security and robustness of the carrier message. They define the different parameters such as capacity, transparency, and robustness for the implementation of three-layered architecture. This experimental analysis proposed by Muhammad Asad et. al. gave the signal to noise ratio of 54.78 dB compared with conventional LSB method having 51.12 dB SNR [10].

Audio steganography system implemented by Lovey Rane et. al. gives improved security. For this, they used dual layer randomization approach. In this system, the first layer is obtained by choosing randomly the byte number or samples. Here, an additional layer of security is provided by selecting the bit position randomly at which embedding is done in selected samples. By using this system,

transparency and robustness of the technique is improved [11]. Researchers observe a new method which is like the well-known LSB method. Due to less robustness and more susceptibility, LSB method is not desired. In this method, two bits are used for protecting the message by increasing data hiding capacity. A filter is added to restrict the changes in the stego file. Obtained stego file is used to generate unique key. The filtered file and the generated key were sent to the receiver. The key is used to extract the correct message at receiver side [12]. R. Sridevi et.al. proposed a useful method of audio steganography by customizing LSB algorithm and strong encryption key with enhanced security is suggested. Enhanced Audio Steganography (EAS) is a combination of audio steganography and cryptography. EAS works in two steps: it used the most effective encryption algorithm in the first level and in the second level it uses a modified LSB (Least Significant Bit) algorithm to enclose the message into audio [13]. Submission technique is also a god choice for audio steganography. Message bits are placed into multiple and higher LSB layer values using genetic algorithm ensuing in enhancement of robustness. The robustness of the system should be increased against intruders which try to exhibit the secrete message and some involuntary attacks like noise etc [14]. Ashwini Mane et.al. suggested a method known as Least Significant Bit (LSB) method. In this method, consecutive least significant bits are replaced with private message bit from each sample of cover audio. The LSB method is very simple but less powerful. This paper differentiates the spectrum of original audio before embedding and audio signal after embedding [15]. A new 4th bit rate LSB audio steganography method is new proposed approach in current era. This method minimizes the embedding distortion of the host audio. In this method, message bits are fixed into 4th LSB layer. It leads to high robustness against noise addition. As compared to standard LSB method, the perceptual quality of audio is more in proposed method [16].

The substitution method has some limitation for audio steganography. The main problem of this technique is that it is less significant against attack. There are two types of attack: One, it tries to extract the private message and other tries to destroy it. As in standard LSB method, the secrete message is stored into the least significant bit, so this method is more susceptible to attack. Therefore, for security purposes, the message is stored in a bit other than LSB. If the message is stored into deeper bits, the system will become more powerful. But the main disadvantage is that when the message is stored into MSB, the host audio signal gets altered. So, by using an intelligent algorithm this problem is solved where the message bits are embedded into MSB and other bits are altered to decrease errors. The message is stored into multiple MSB to make a system more robust and high capacity [17]. S.S.Divya et.al. proposed a method where multiple LSB bits are used for hiding a text in audio signal using steganography and cryptography is used for security purpose. For LSB audio steganography, maximum number of bits is altered from 16-bit audio sample. They use two novel approaches for substitution technique of audio steganography improving capacity of cover audio for storing additional data. In this technique, the message bits are stored between 35% to 70% compared to standard LSB technique which uses 4 LSBs for data storing [18]. The researcher proposed a Genetic algorithm is also good choice for audio steganography. They studied various audio steganography techniques using genetic algorithm and

LSB approach. They tried some approaches which help in audio steganography. In these techniques, hidden messages are written in such a way that only sender and corresponding receiver are able to see the message [19].

## 4. Techniques of Audio Steganography

Researchers are currently turning towards hiding the high quality secrete message in audio file. The abundance of audio message makes them eligible to convey secret information. Many researchers started to explore how the audio signals and audio properties can be exploited in the era of information security [20]. Several approaches were considered, the most robust and significant ones are Least Significant Bit [21], Echo hiding [22], Hiding in Silence Interval [23], Phase Coding [24], Amplitude Coding [25], Spread Spectrum [26], and Discrete Wave Transform [27].

### 4.1 LSB Technique

Fundamentally, the LSB technique depends on implanting every bit from the data to hide into the rightmost bits of every audio sample of the carrier audio message. The LSB technique proved as advancement towards a HAS unable to understand the slight variation of audio sampling frequency towards the high frequency region of the audible spectrum. The LSB technique allows high embedding rate without impairing the quality of the audio file. This technique is robust and dynamic for audio steganography.

The technique uses the fact that most of the information in a sample in any audio file is contained in the MSBs rather than LSBs. In the LSB coding approach the slandered data broadcasting rate is 1 kbps per 1 kHz. In some implementations of LSB coding, the two smallest significant bits of a sample are substituted with two message bits. This implementation increases the amount of data that will be determined but also enlarges the amount of resultant noise in the audio file as well. The representation of LSB coding technique is shown in figure 2.

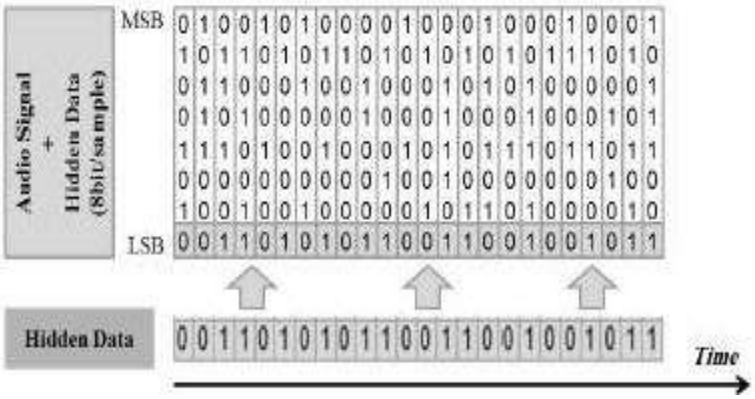


Figure 2: Graphical representation of LSB coding technique

### 4.2 Echo Hiding Technique

In this echo hiding technique, the secret data are embedded into the audio signals as a short acoustic echo. In fact, an echo is a reproduction of sound, however, received by the listener some time after the original sound. The echo is perceptible; its amplitude must be reduced and undetectable. In order to hide data, bits whose values are 0, it is characterized by an echo overdue 1ms; bits whose values are 0 are represented by an echo delayed 2ms.
In this technique, the original signal is divided into chunks before the encoding process. Once the encoding process is finished, the blocks are concatenated back together to create the final signal [28]. The complete block diagram of echo hiding technique is shown in figure 3.

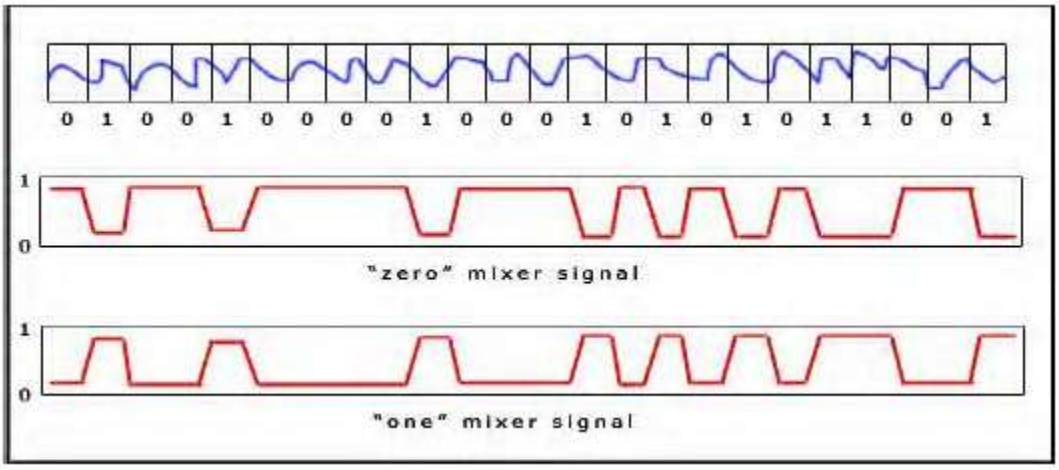


Figure 3: Graphical representation of Echo hiding Technique

### 4.3 Amplitude coding

Amplitude coding technique conceals secret data in the magnitude speech spectrum while not distorting the carrier audio signal. It is based on finding a safe spectral area in the signal whose magnitude speech spectrum is below a certain value. In addition, the carrier locations are preferred based on how much they can badly affect the audio signal [25].

### 4.4 Spread Spectrum

The Spread Spectrum technique scatters secret data over the frequency spectrum of the audio file using a precise code independent of the original signal. Fundamentally, secret data are multiplied by a code known to the corresponding level only, and then implanted in the carrier audio message. In this technique the data is generated by m-sequences code known as sender and receiver for the secrete communication [29]. To control stego speech distortion, [30] and [31] have proposed an embedding method where splitted data is secreted under a frequency cover. In the spread spectrum is combined to phase changing to increase the strength of the transmitted data against additive noise and allows easy detection of the fixed data. In this method, a reliable hiding capacity of 3 bps was attained. The graphical representation of spread spectrum information encoded in the original message is described in figure 4.

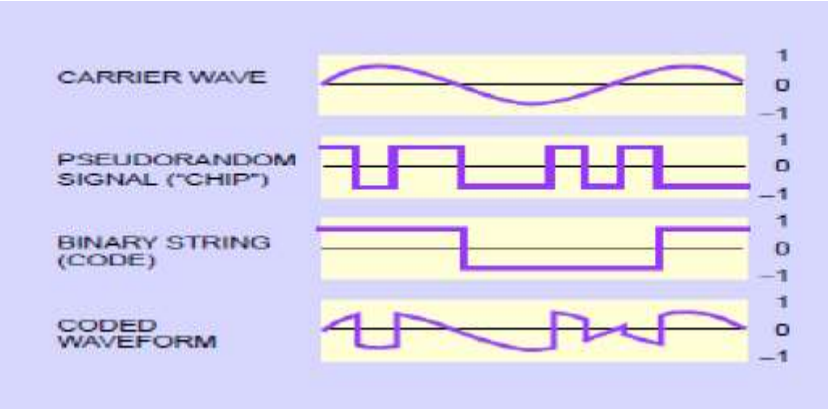


Figure 4: Synthesized spread spectrum information encoded in original message.

### 4.5 Discrete Wave Transform

Discrete Wave Transform technique private messages are encoded in the smallest significant bits of the wavelet coefficients of the audio signals. Often, private data is chosen to be secreted in the wavelet coefficients and not in silent sections of the audio signal to promote the imperceptibility of the audio file [27].

## 5. Proposed approach

From the enriched literature observed the limitation of available techniques and their procedure. The human ear is highly sensitive and can regularly notice even the slightest bit of noise introduced into a sound file .The main limitation associated with parity coding is not much closure, making introduced noise inaudible. The limitation of phase coding towards data transmission rate because in this technique message is encoded in the first segment of signal only. Phase coding technique recommended only when the small amount of data is considered for steganography approach. Least significant bit (LSB) coding is the robust way to encode message in a digital audio file. Substituting the least significant bit to each frequency point with a binary message allows for a large amount of data to be encoded [21]. In the available data hiding methods in enriched literature the proposed method for embedding secrete message within audio file, LSB is the simple and robust method for inserting message in audio signal towards noise free environment. It embeds secret message-bits in a subset of the LSB levels of the audio message. The following steps are:

a. Receive Audio file.

b. Convert the file into bit Pattern

c. Each character of secrete message convert into the bit pattern.

d. Replaces the LSB bit from audio with LSB bit from character in the message.

The proposed system is to provide a good, robust, and dynamic method for information hiding in audio from hackers and sent to the destination for secrete communication. The advantages of the

proposed system are that it does not change the size of the original audio file even after encoding and also suitable for all audio formats.

## 6. Experimental Analysis

For these experiments a real example was tested to illustrate how the proposed steganography technique works. It involved using the various steps of the algorithm to envelop a secret text message into a 16-bit WAV carrier audio file. For this experiment we selected the different 10 secrete message. The secret data to hide is a text message is shown in the experiment is "**we will kill You**". The private message is preprocessed and converted into a binary form. Ten audio samples were randomly selected for this experiment. The chunks obtained in implementation step one is stored into the three LSBs of the audio samples selected in step two. The final output is the carrier WAV audio file now carrying the secret data. The graphical representation of the original audio message "you are very nice" is shown in figure 5. Figure 6 represents the audio file with encoded secrete message. The spectrogram of audio file with encoded message is shown in figure 7. Figure 8 represents the spectrogram of original audio message after secrete message extracted.

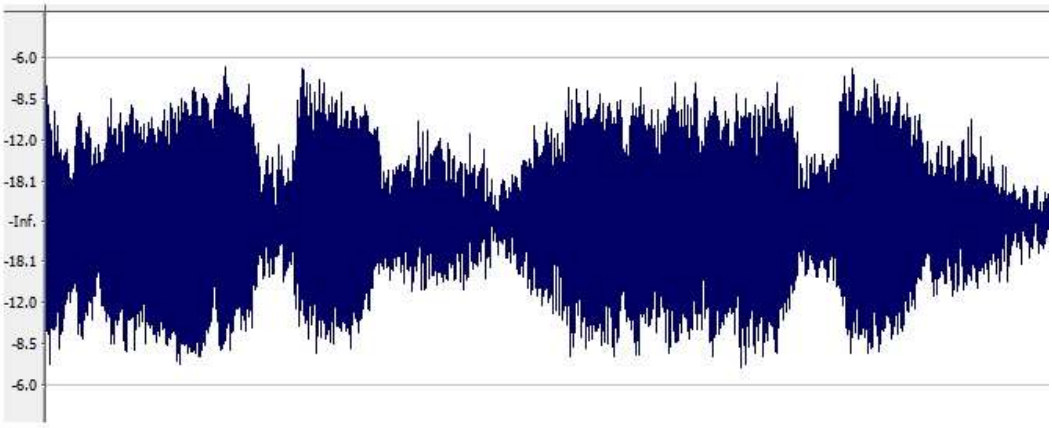


Figure 5: original audio signal message for the "you are very nice".

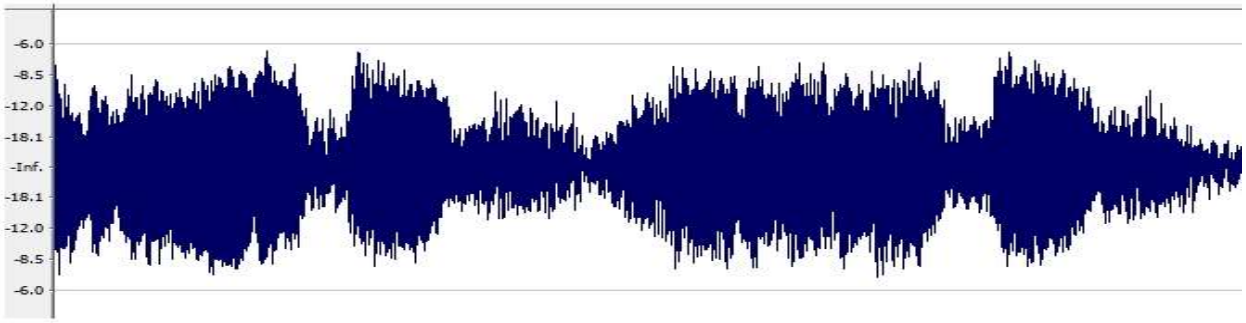


Figure 6: the audio file with encoded message "we will kill you"

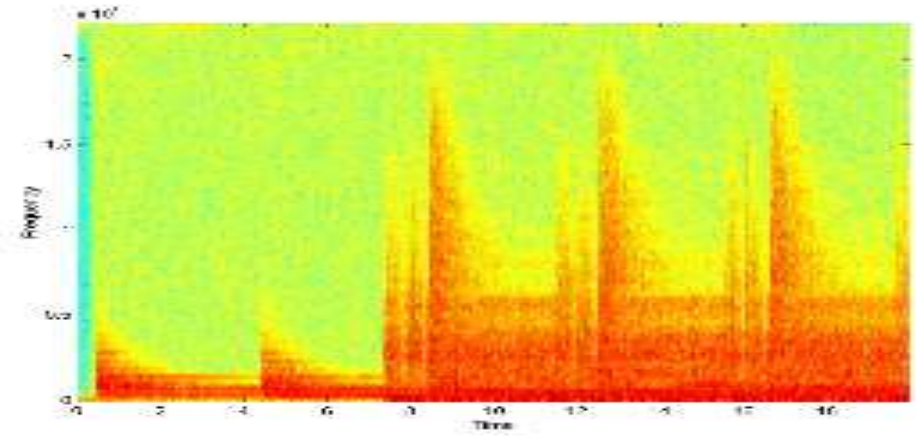

Figure 7: The spectrogram of combine orignal signal and secrete message

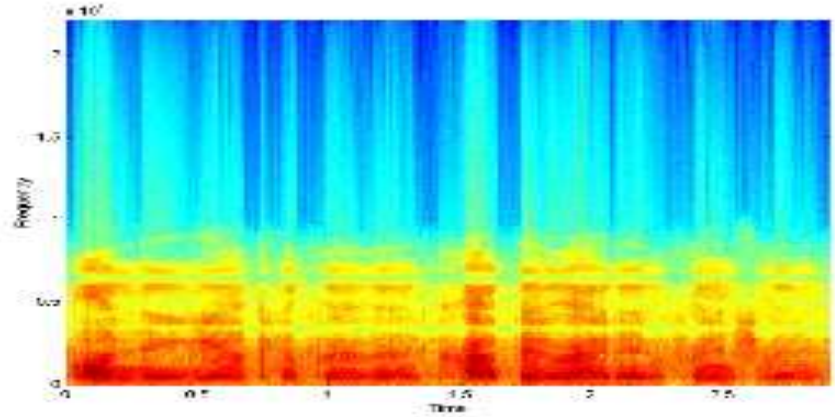

Figure 8 : original signal after extracted secrete message

### 6.1 Stegno Audio Quality Measurement

Steganography audio quality measurement replaces the listener panel with a computational algorithm, thus facilitating automated real-time quality measurement. Indeed, for the purpose of real-time quality examining and organizing on a network-wide scale, objective speech quality measurement is the only viable option. Objective measurement methods aim to convey quality examination that is highly correlated with those obtained from subjective listening experiments. In the objective quality measure mean square error (MSE) and peak signal-to-noise ratio (PSNR) technique was used.

#### 6.1.1 Mean Square Error (MSE)

The mean squared error (MSE) of an estimator calculates the average of the squares of the errors, that is, the variation between the estimator and what is estimated. MSE is a risk function, equivalent to the predictable value of the squared error loss or quadratic loss. The difference occurs because of uncertainty or because the estimator doesn't account for information that could produce a more accurate estimation of speech synthesis [32].

### 6.1.2 Peak Signal to Noise Ratio(PSNR)

Peak signal-to-noise ratio, often abbreviated PSNR, is the ratio between the most probable influence of a signal and the power of corrupting noise that affects the quality of its illustration. PSNR is usually articulated in terms of the logarithmic decibel scale. PSNR is most used to measure the quality of reconstruction of signal and image. The signal in this case is the original data, and the noise is the error introduced by synthesis [33]. The PSNR and MSE method was used for quality measure of steganography audio based on proposed LSB technique. Table 1 represents the MSE and PSNR values for LSB technique.

**Table 1: MSE and PSNR results for audio steganography using proposed LSB technique**.

| Sr.No | Original Audio signal | Stegno Audio signal | M.S.E | P.S.N.R |
|---|---|---|---|---|
| 1 | S001 | N001 | 5.23 | 1.26 |
| 2 | S002 | N002 | 8.9 | 7.56 |
| 3 | S003 | N003 | 7.61 | 1.29 |
| 4 | S004 | N004 | 5.32 | 3.24 |
| 5 | S005 | N005 | 7.61 | 7.32 |
| 6 | S006 | N006 | 9.1 | 9.78 |
| 7 | S007 | N007 | 8.06 | 11.23 |
| 8 | S008 | N008 | 5.32 | 1.29 |
| 9 | S009 | N009 | 8.06 | 3.24 |
| 10 | S0010 | N0010 | 7.2 | 4.08 |
| **Average** | | | **7.241** | **5.029** |
| **Quality (100-Average)** | | | **92.759** | **94.971** |

## 7. Conclusion

In this experiment, we have proposed a LSB robust technique for imperceptible audio steganography. This system is useful to provide a good, efficient method for data secrecy from hackers and send it to the destination safely. This proposed technique will not change the size of the file even after encoding and is suitable for any type of audio file format. Thus, we conclude that audio steganography techniques can be used for several purposes other than covert communication and information tracking. The superiority of steganography message plays an important role in secretes communication. The experiment extended towards quality measure of audio steganography. The quality measure experiment was tested using MSE and PSNR techniques. The observed quality is extracted as 92.759 % from MSE and 94.971 % from PSNR. The authors recommended the PSNR technique to be robust and dynamic for steganography audio quality measure.

**References**

1. Peter Wayner, "Disappearing cryptography: information hiding: steganography & watermarking", 3rd Edition, Morgan Kaufmann Publishers, 2009.
2. Fabien A. P. Petitcolas, Ross J. Anderson and Markus G.Kuhn, "Information Hiding - A Survey", Proceedings of the IEEE, special issue on protection of multimedia content, vol. 87, no.7, pp.1062-1078, 1999.
3. W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding", IBM Systems Journal, vol. 35, no. 3-4, pp. 313-336, 1996.
4. X. Dong, M. Bocko, Z. Ignjatovic, "Data hiding via phase manipulation of audio signals", IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), vol. 5, pp. 377-380, 2004.
5. Kandel ER, Schwartz JH, Jessell TM, "Principles of Neural Science", 4th edition, McGraw-Hill, 2000.
6. Lee, Y. K. and Chen L. H. "High Capacity Image Steganographic Model". IEEE Proceedings Vision, Image and Signal Processing, pp. 288-294, 2000
7. Martín Alvaro, Sapiro Guillermo and Seroussi Gadiel, "Is Image Steganography Natural?" IEEE Transactions On Image Processing, Vol. 14, No. 12, December, 2005
8. Nedeljko Cvejic, Tapio Seppben, "Increasing the capacity of LSB-based audio steganography", FIN-90014, Finland, 2002.
9. Johnson, N. F. and Jajodia, S., "Exploring steganography: Seeing the unseen", Computer Journal, vol. 31, no. 2, pp. 26-34, 1998.
10. Muhammad Asad, Junaid Gilani, Adnan Khalid, "Three Layered Model for Audio Steganography", 2012 International Conference on Emerging Technologies (ICET)
11. Lovey Rana, Saikat Banerjee, "Dual Layer Randomization in Audio Steganography Using Random Byte Position Encoding", International Journal of Engineering and Innovative Technology, Volume 2, Issue 8, February 2013
12. Kirti Gandhi, Gaurav Garg, " Modified LSB Audio Steganography Approach" International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 6, June 2012, pp 158-161
13. 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.
14. Bankar Priyanka R., Katariya Vrushabh R, Patil Komal K, "Audio Steganography using LSB'', International Journal of Electronics, Communication and Soft Computing Science and Engineering, March 2012, pp 90-92

15. Ashwini Mane, Gajanan Galshetwar, Amutha Jeyakumar, "Data Hiding Technique: Audio Steganography using LSB Technique", International Journal of Engineering Research and Applications, Vol.2, No.4, May- June 2012, pp 1123-1125.
16. Ajay.B.Gadicha, "Audio wave Steganography", International Journal of Soft Computing and Engineering (IJSCE), Vol. 1, pp. 174-177, Nov. 2011.
17. Mazdak Zamani et.al. "A Secure Audio Steganography Approach", International Conference for Internet Technology and Secured Transactions 2009.
18. 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.
19. Gunjan Nehru, 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.
20. F.Djebbar, B. Ayad, K. Abed-Meraim and H. Hamam, "A view on latest audio steganography", 7th IEEE International Conference on Innovations in Information Technology, 2011.
21. K. Gopalan, "Audio steganography using bit modification", Proceedings of International Conference on Multimedia, vol. 1, pp.629-632, 2003.
22. D. Gruhl and W. Bender, "Echo hiding", Proceeding of Information Hiding Workshop, pp. 295-315, 1996.
23. S. Shirali-Shahreza, M. Shirali-Shahreza, "Steganography in Silence Intervals of Speech", proceedings of the Fourth IEEE International Conference on Intelligent Information Hiding and Multimedia Signal, pp. 605-607, 2008,
24. Yin-Cheng Qi, Liang Ye, Chong Liu, "Wavelet Domain Audio Steganalysis for Multiplicative Embedding Model", Proceedings of the 2009 International Conference on Wavelet Analysis and Pattern Recognition, 2009.
25. F. Djebbar, B. Ayad, K. Abed-Meraim, H. Habib, "Unified phase and magnitude speech spectra data hiding algorithm", Journal of Security and Communication Networks, John Wiley and Sons, 2012.
26. Khan, K., "Cryptology and the origins of spread spectrum", IEEE Spectrum, vol. 21, pp. 70-80, 1984.
27. N. Cvejic, T. Seppanen, "A wavelet domain LSB insertion algorithm for high capacity audio steganography", Proc. 10th IEEE Digital Signal Processing Workshop and 2nd Signal Processing Education Workshop, pp. 5355, 2002.
28. K. Gopalan and S. Wenndt, "Audio Steganography for Covert DataTransmission by Imperceptible Tone Insertion", WOC 2004, Banff,Canada July 8 10, 2004

29. Steve Czerwinski, Richard Fromm, Todd Hodes, “Digital Music Distribution and Audio Watermarking”.http://reference.kfupm.edu.sa/content/d/i/digital_music_distribution_and_audio_wat_1045219.pdf
30. Francesco Queirolo, “Steganography in Images”, Final Communications Report http://eric.purpletree.org/file/ Steganography%20In%20Images.pdf
31. Ingemar J. Cox, Ton Kalker, Georg Pakura and Mathias Scheel. “Information Transmission and Steganography”, Springer, Vol. 3710/2005, pp. 15-29
32. Lehmann, E. L.; Casella, George (1998). Theory of Point Estimation (2nd ed.). New York: Springer. ISBN 0-387-98502-6. MR 1639875
33. Huynh-Thu, Q.; Ghanbari, M. (2008). "Scope of validity of PSNR in image/video quality assessment". Electronics Letters 44 (13): 800. doi:10.1049/el:20080522