J. Appl. Environ. Biol. Sci., 6(6)69-77, 2016

ISSN: 2090-4274
Journal of Applied Environmental and Biological Sciences
www.textroad.com

Audio Steganographic Technique Based On Fletcher Munson Curve

[1]Rehan Ullah, [2]Zakir Khan, [3]Noor Ul Amin, [4]Mohsin Shah, [5]Arif Iqbal Umar, [6]Abdul Hakeem

[123456]Department of Information technology Hazara University
Mansehra, KPK, Pakistan.

Received: February 20, 2016
Accepted: April 25, 2016

ABSTRACT

Exchange of secure information through insecure channels is a challenging problem now a day. Data hiding technique is one of the kinds of secret communication mechanism in which the very existence of secret data is made hidden. Steganography is the art of science in which secret data is hiding in different files. The major motive of this paper is to present a novel hiding technique. Audio steganography is such a mechanism in which secret messages is embedded in audio signal. In this paper audio steganographic technique based on Fletcher Munson curve is presented. The proposed technique hides secret message bits according to consecutive amplitude samples of the audio signal. Data embedding occur according to minimum of two consecutive amplitude of audio sample. If the amplitude sample bits is less than 8 bits than we have to embed 8 bits sample while if the amplitude sample bits is more than that of 8 bits than we have to embed data according to Fletcher Munson curve. The proposed and design technique have more SNR, highly robust and more data hiding capability than existing techniques.
KEYWORDS: Steganography, Fletcher Munson curve, Nyquist Theorem and SNR.

1. INTRODUCTION

Steganography is the branch of science in which we study about the concealed or covered writing. Steganography is derived from two Greek words *Stegano*; means "*Covered*" and *grafia* means "*Writing*". So, Steganography is the study of cover writing [1]. Various files types are used for information hiding including images, text, audio, video, and executable files. The hidden message is only apparent to sender and receiver while the observer sees only a cover object. In past people use information hidden techniques such as tattoos or invisible inks to convey steganographic contents. Simmons in 1983 for the first time introduced the idea of data hiding with the example of prisoners' covert message [2]. The major aim of steganography is that the third party is unaware from communicating of two parties [3]. Three basic properties of an efficient audio steganographic technique are Inaudibility of distortion (Transparency), pay load and Robustness. These properties are known as the magic triangle for information hiding [4]. Embedding data into audio signal is more difficult task as compare to embedding in images as the humans ear is very sensitive to disruption in sound and can easily detect the very low disturbance as one part in 10 million [5].

Fletcher-Munson Curves

The propose technique is based on Fletcher Munson curve. The propose technique embeds data according to Fletcher Munson curves. If the audio amplitude sample is more than 8 bits data embedding will be occur according to Fletcher Munson curves. The Fletcher Munson curves put data according to amplitude of audio sample in such a manner that embedding occurs according to minimum of consecutive amplitude sample. If the amplitude of audio sample is less than 8 bits than 8 bits data well be embed. Fletcher Munson curve is also known as equal-loudness curves, or loudness curves. A series of curves plots the sound loudness of some original tones, in intensity vs. frequency in Hz for all audible frequencies in order to identify all frequencies at the same potency. The sensitivity also changes and frequency of hearing sensitivity also varies which depends on sound pressure level. According to Fletcher Munson curve, the audio sample in the range of -255 up to +255 is not auditable.

Figure 1 explains that the sample that lies in between high amplitude samples will not be auditable due to surrounding high amplitude samples [24].

***Corresponding Author:** Rehan Ullah, Department of Information technology Hazara University, Mansehra, KPK, Pakistan. rehanullah551@yahoo.com,

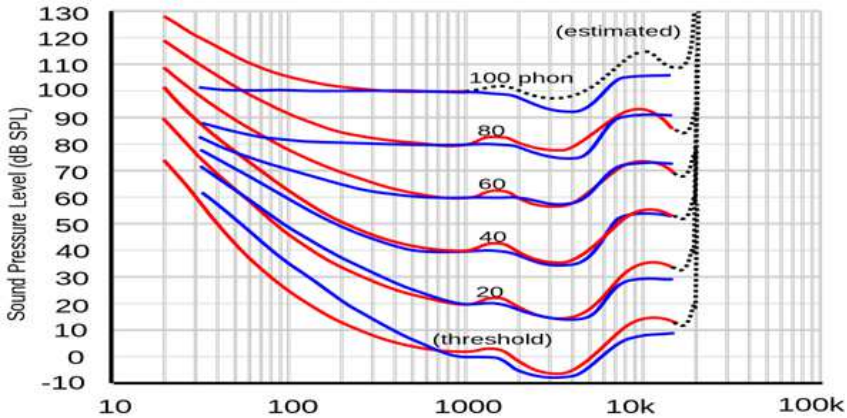

Figure 1 Fletcher Munson Curve

Let us take 13 audio samples of variable amplitudes25, 456, 34, 945, 450, 1034, 950, 345, 300, 220, 210, 150, 120**.** According to Fletcher Munson curve, samples less than 255 will not be auditable, for example, 25, 34, 220, 210, 150, and 120. Next, sample surrounded by bigger samples will not auditable. For example 450 will not be heard although 450 are greater than 255 but it is surrounded by 945 and 1034. So the human ear only hears 945 and 1034.

1. LITERATURE REVIEW

Various techniques in audio steganography are available in literature. Some of the most common techniques are discussed as follows:

LSB Coding

The simple technique for concealing the covert data in audio file is LSB coding. It is also called "Low-bit encoding". The Least Significant Bit coding technique is one of the earlier techniques used for hiding of secret information [6]. In LSB coding technique least significant bit of binary sequence of every sample of digitized audio file is altered with binary equivalent of covert information. The technique has high embedding capability and very simple and easy for hiding data. While the limitation of this technique as: it is not robust in nature and the secret message can be easily extracted.

Parity Coding

In [7] S.K Bandyopadhyay et al proposed a parity coding techniques in which breaking of signal occur into different section of sample instead of individual sample. Each bit is encoded from the secret information in sample regions parity bit. The procedure flicks the L-S-B of one of the sample in the region if, the parity bit of a chosen section does not hold the covert bit to be embedded. To encode the secret bit the dispatcher has more option and the signal can be altered in a more inconspicuous way. The application of this technique as the dispatcher has additional of an option for embedding the covert message bit, and the signal can be altered in more inconspicuous way [21]. While the limitation of this technique as it is not robust in nature.

Discrete Wave Transform

In this technique secret message are embedded in the LSB of the wavelet coefficients of audio files [8]. For the imperceptibility of the audio file, secret message bits are hidden in the integer wavelet coefficient and not in the silent sections of the audio signal. The limitation of this technique is that the covert message can be lost during the recovering process.

Substitution

In [8] the insignificant bits of carrier signal substitutes with secret bits data. Insignificant bits can modify the carrier signal without harming the quality of audio. For example, sound units are made of series of bits. If the LSB of this series is altered, the impact of perceptible sound is much minimized so that normal human ear can't distinguish between the original and altered one. The data hiding capacity of one LSB audio sample for this technique is 44.1 kbps. The technique has application of the bounded capacity of the HAS which could not identify two sounds which are little different. The advantage of this technique is high data hiding capacity while, it has medium robustness.

Phase Coding

In [7] S.K Bandyopadhyay et al, discus that phase coding confide on the evidence that the phase constituent of sound could not audible to human ear as noise. This technique acts as by replacing the phase of an initial audio

sector with a reference section that shows the information. So, to protect the relative phase between segments, the phase of following sectors is then adjusted. The limitation of this technique is low data transmission rate and has also complex method.

Spread Spectrum

In spread spectrum techniques the embedded data is disperse across the obtainable frequencies as much as possible [9]. Using a code that is independent of the original signal, the spread spectrum techniques disperse the covert message over the sound file's frequency spectrum. As a result, the final signals inhabit a bandwidth in surplus of what's required for broadcasting in reality.

Advantage of this technique as it offers conservative data communication and has highly robustness. While the limitation of this technique as it can initiate noise into audio file.

Echo data hiding

In this technique data is embedded in audio signal by initiating an echo to the carrier audio signal [9]. Three main factor of the echo like initial amplitude, decay rate, and offset from original signal are varied for hiding of information successfully. One bit information could be embedded as by introducing one echo from original audio signal. Before the embedding process begins the original audio signal breaks down into blocks. After completion of encoding, the blocks are regaining concatenated which form the final signal.

Tone insertion

Tone insertion technique guarantees that lower power tone is not audible in the presences of higher power tone. Inaudible tones are inserted into cover audio signals for embedding data is presented in [10, 11]. This technique can withstand against attacks like low-pass filtering and bit truncation. Embedded data could be maliciously extracted due to low embedding capacity since tone insertion is easy to detect. Its application is imperceptibility of embedded data while the limitations of tone insertion are lack of transparency and security.

Sample Selection

In this technique a few samples are used for embedding data instead of all samples. In this technique 1st three MSB's decide the data embedding and also randomness is created in sample numbers. The last column shows the next audio sample that contained the covert message bit. If the current sample is between two consecutive secret data bits the number of samples leave out which is equal to one more than the decimal value of 1st three bits [12]. This technique has low data hiding capability.

Bit Selection

In bit selection technique different bits of audio sample are selected for embedding of secret message. To hide the secret information in different bits of audio sample, randomness method is used for the confusion of eavesdropper. The decision is brought by the first two MSBs of audio sample. Table1 shows a possible Bit Selection mapping. From below table 1 it is clear that, If 1st and 2nd MSB's of the audio sample are 00, then the secret data is hidden in 3rd LSB. If the first and 2nd MSBs are equal to 01, than 2nd LSB is used and while if the 1st and 2nd MSB's are either 11 or 10 than 1st LSB is used for hiding secret information.

Table 1
Bit selection mapping

Secret message bit	1st MSB	2nd MSB
3rd LSB	0	0
1st LSB	1	1
2nd LSB	0	1
2nd LSB	1	0

Bit selection technique is more secure than Sample selection but it has Low payload capacity.

Variable Low Bit Coding

This technique has more data hiding capability than that of LSB Coding. Suppose audio data of range is 0 to 255 and sound is silent in middle range which is 128 [13]. Hence the secret information can't hide in the middle range, so using the above calculating the standard level and two thresholds 1and 2. The secret data is not hiding when the amplitude range is less than 1. One bit is used for information hiding if the amplitude range is between threshold 1 and 2, while two bits are used for information hiding if the amplitude range is above threshold 2. It has more data hiding capability than that of lowest bit coding but easy to extract & destroy.

XOR-ing Method

In XOR-ing technique the XOR operation is performs on the LSB's of audio sample and depends on XOR operation result and the message bit to be hiding. The LSB of the sample is remaining unchanged depending on the

XOR operational result and covert message bit to be encoded. This technique increases the hiding capability 8 times of the cove audio signal and highly robust encryption property [14]. It has high data embedding capability but has comparatively low robustness.

Average Amplitude

In this technique the average amplitude information of around audio data is used as threshold. Two digits of binary are used for encoding if the range of amplitude is greater than threshold, then embedding of two digits of binary are used else no embedding occur. This technique increases the capacity and security of embedding [20]. Limitation of this technique is that it is more complex and it is computational and also this method is limited to two binary digits.

Mazdak et al, used substitution method in which message bit are embedded in deeper layer of audio samples and change to reduce the error [15]. It has high embedding capacity and Robustness.

Padmashree & Venugopala in [17] proposed encoding technique which used 4-th bit LSB method that embedded message into audio file. In his proposed scheme public key cryptographic algorithm and RSA is used to ensure greater security.

Hakeem et al, proposed a new threshold base LSB audio steganographic technique in which low bit data hide in high amplitude sample and vice versa [18].

The threshold based LSB audio steganography has comparative low SNR and has low data hiding capability.

2. Proposed Solution

The proposed scheme has two phases; embedding phase and extracting phase. The encoding phase hide the secret message data through steganographic techniques while extracting phase unhide the secret message to its original form.

Embedding Phase

In embedding phase we have to hide the secret message bits through some techniques form eavesdropper. The embedding phase consists of following flow chart which is discus in Figure 2. In embedding phase algorithm first we have to read the audio signal. We have to embed secret message bits after each sample. For every even sample first we have to know the minimum amplitude sample according to which we have to hide at least half of data. By knowing the amplitude of consecutive samples we have to put secret message bits. We have to find out the capacity by the help of formula Capacity = $Log_2(A)$. Than we have to take the floor of A. After this we have to hide the secret information according to capacity. If the amplitude of message bits is less than 8 bits than the proposed technique embed 8 bits data. By finishing the sample the proposed technique double the audio frequency and give us stego audio file. The stego audio and original cover audio remain same. The figure 2 explains the embedding phase flow chart.

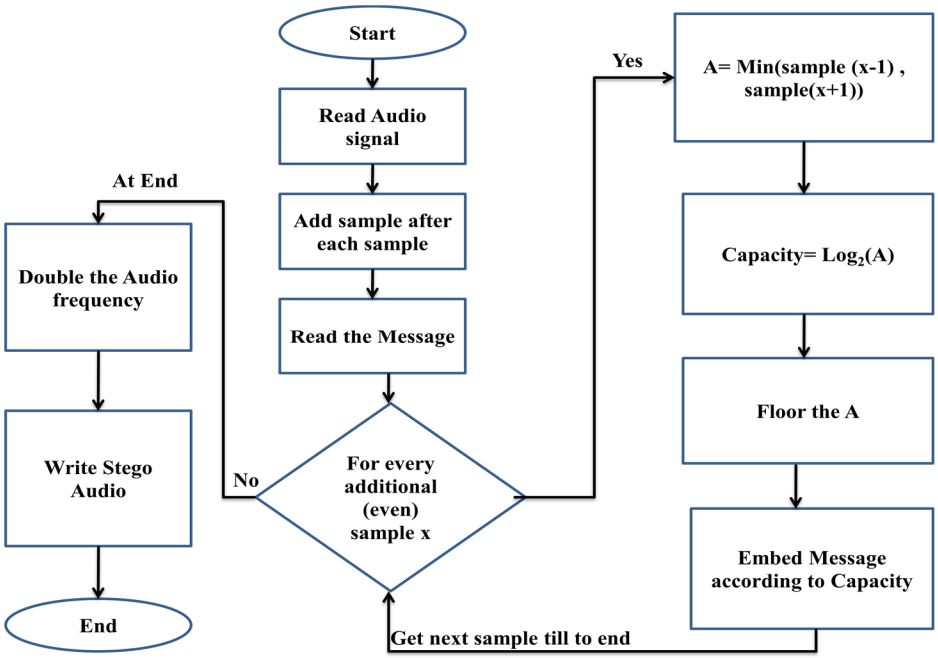

Figure 2 Embedding Flow Chart

Extracting Phase

Figure 3 shows the flowchart for extraction phase. The proposed Extracting phase extract stego audio file for secret message and original cover file. The Extracting algorithm consist of following steps. First the proposed extracting algorithm read the stego audio and then get the amplitude of every even sample. By getting the amplitude bits our proposed technique concatenate the message bits string till to last sample. At last secret message is extracted from that of cover audio file.

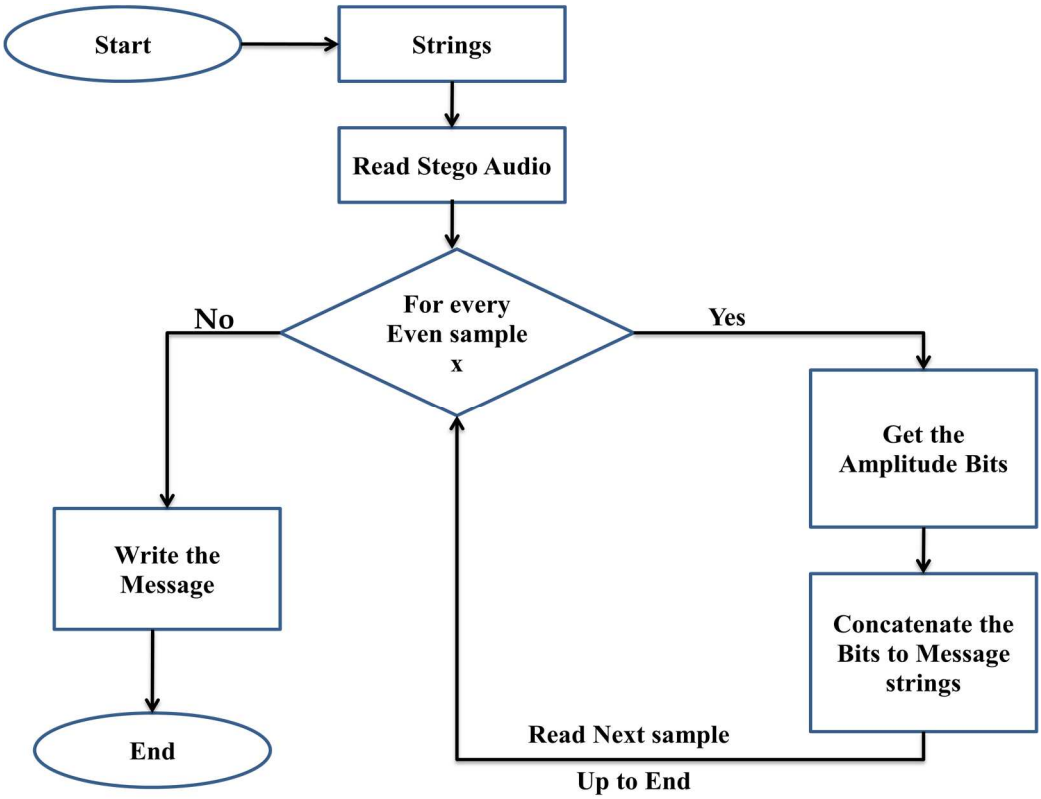

Figure 3 Extracting Flow Chart

3. Experimental Results

Different results are obtained by implementing the proposed technique for different types of audio files to check the effectiveness of the technique. These file include the sound of chirp, gong, handle, laughter, splat and train. Signal-to-Noise Ratio (SNR) and embedding of data are the main parameters to analyze the proposed method's performance. It is observe from listening the resultant stego audio file and cover chirp file that there is no significant distinction between the stego chirp audio and original chirp audio. The result of stego chirp audio and original chirp audio is given below in Figure 4(a) and Figure (b).From Figures 4(a) and 4(b) it is clear that the original chirp audio and stego chirp audio have remain the same because the HAS cannot detected it. As the (HAS) of human is more sensitive than (HVS). Frequencies and durations of some original MATLAB audio files are given in Table 1.

Table 1 Input Audios

MATLAB audio files						
Audio	**Chirp**	**Gong**	**Handel**	**Laughter**	**Splat**	**Train**
Frequency	8192	8192	8192	8192	8192	8192
Time (Duration)	1.6027	5.1304	8.9249	6.425	1.2208	1.5723

Figure 4(a) and 4(b) shows the result that has been obtained during the implementation in MATLB. Figure 4(a) shows us the host audio signal while the figure 4(b) show us the stego chirp audio. As Human Auditory System is more sensitive than that of Human Visual System consequently, the Human Auditory System cannot differentiate among the cover audio and that of stego audio. In this way the sender send his message to receiver in safe manner.

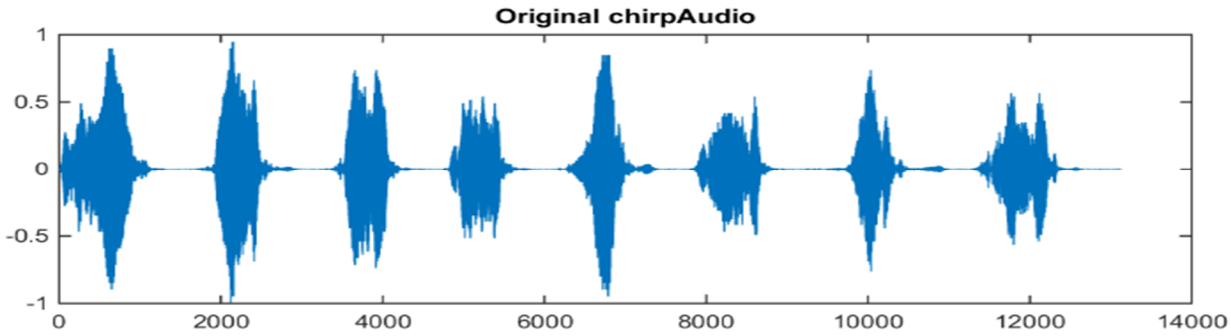

Figure 4 (a) Cover Audio Signal

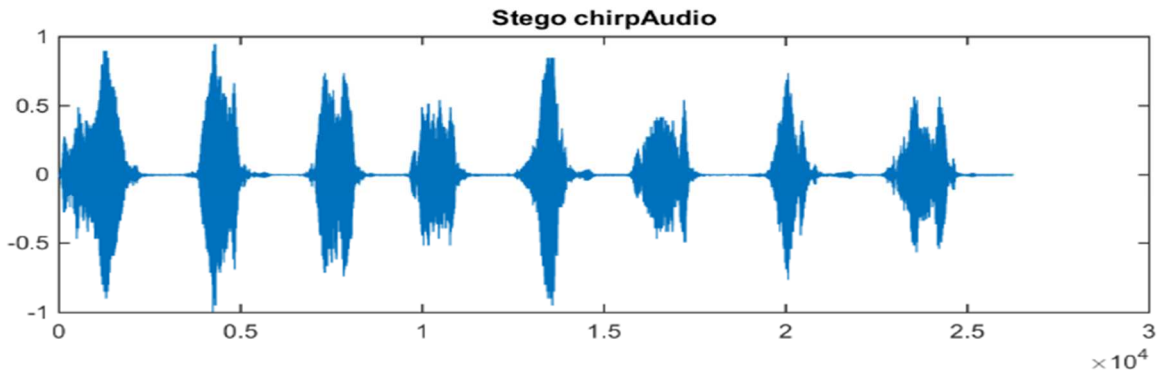

Figure 5 (b) Stego Audio Signal

Table 2 shows comparison of payload in (bytes) of the proposed technique and base techniques for different audio signals.

Table 2 Payload in Bytes

Payload in Bytes		
Sounds	**Base Paper**	**Proposed Technique**
Chirp	13129	15377
Gong	42028	50571
Handel	73113	96532
Laughter	52634	66588
Splat	10001	10854
Train	12880	17970

The below figure 5 shows the payload compression of proposed technique and that of existing techniques. The red bar shows the payload of proposed technique while the other bars show the payload of earlier mechanisms. Therefore, the proposed mechanism has more data embedding capability than existing techniques.

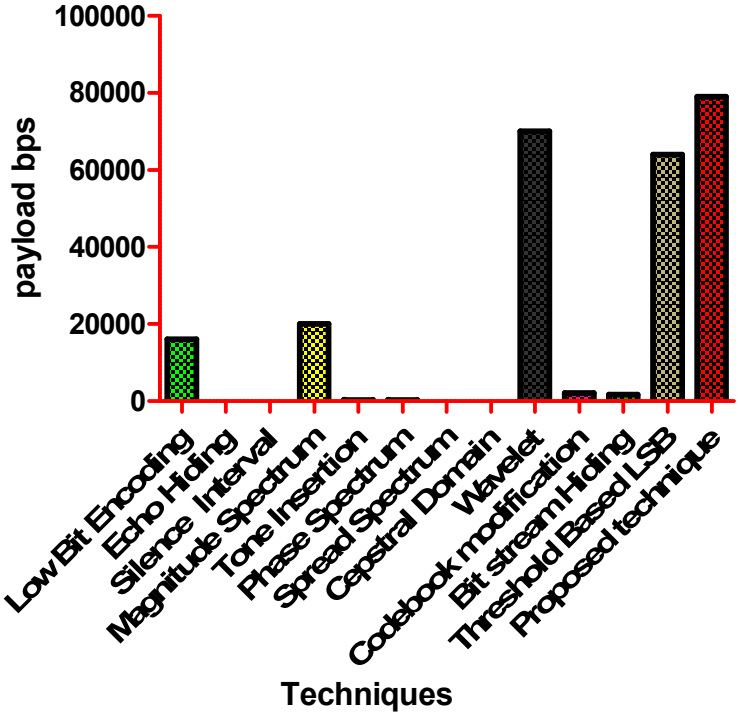

Figure 5 Payload Comparison Graph

Table 3 shows the payload in bytes per second of the proposed technique. From the table 3 it is clear that the proposed technique has 79 kbps per second embedding rate.

Table 3 Payload in Bytes Per second

Payload in Bytes			
Sounds	**Proposed Technique**	**Duration in Second**	**Proposed Payload Per Second**
Chirp	15377	1.6027	9594
Gong	50571	5.1304	9857
Handel	96532	8.9249	10816
Laughter	66588	6.425	10364
Splat	10854	1.2208	8891
Train	17970	1.5723	11429
Average payload Per Second rate in Bytes		10159	
Average Per Sec Rate in Bits		81269	
Average Per Sec Rate in Kilo Bits		79	

Table 4 shows us the comparison of proposed technique with existing techniques. This table also explains the advantages, limitations and also embedding rate of techniques. The table shows that the proposed technique is efficient in term of improved payload (79kbps). It has also more SNR and highly robust than that of existing techniques.

Table 4 Comparison of different Techniques

"Hiding Domain"	"Method"	Embedding Technique	Hiding Rate	Applications	Limitations
Transform Domain	Tone Insertion"	"Insertion of inaudible tones at selected frequencies	250 bps	Imperceptibility and concealment of embedded data	Lack of security and transparency
	Magnitude Spectrum	Use frequency band to hide information	20kbps	Longer message to hide and less" likely to be affected by error during transmission	Low robustness to simple audio manipulation
	Phase Spectrum	Modulate the phase of the cover signal	333 bps	Robust against the signal processing and modulate data retrieved" needs original signal	Low data hiding capability
	Cepstral Domain	Altering the Cepstral coefficient for embedding information	54 bps	Robust against signal processing operation	Perceptible signal distortion and low robustness
	Spread Spectrum	Spread the data over all signal frequencies	20 bps	Provide better robustness	Vulnerable to time scale modification
	Wavelet	Altering wavelet coefficient for embedding data	70 kbps	"Provide high "embedding" capacity	Lossy data retrieval
Temporal Domain	Echo Hiding	Embeds data by introducing echo in the cover signal	50bps	Resilient to lossy data compression algorithms	Low security and capacity
	Silence Interval	Use the number of sample in silence interval to represent the hidden data	64bps	Resilient to lossy data compression algorithms	Low hiding capability
	Low Bit Encoding	LSB of each sample in the audio is replaced by one bit information	16kbps	Simple and easy method of hiding data with high bit rate	Easily extract and destroy
Codecs Domain	Bit stream Hiding	LSB is apply on the bit stream resulting from the encoder process	1.6 kbps	Robust	Low embedding capability
	Codebook modification	Altering Codebook parameter	2 kb	Robust	Low embedding capability
Base Paper	Threshold Based LSB	Change LSB Randomly	64 kbps	Robust high embedding data rate Imperceptible	Low Embedding Rate from Proposed
Proposed	Fletcher Munson curve based Steganography	Add non-audible Samples	79kbps	Robust high embedding data rate non-Audible	Hiding rate Depends upon the amplitude of consecutive samples of original audio

4. Conclusion

Data hiding technique is one of the kinds of secret communication mechanism. Sending secret information through insecure path is prone to attacks. Audio steganography is one of the challenging techniques as compared to that of image steganography because the visual system of human is slightly less sensitive than that of to human auditory system. This manuscript explains a mechanism of hiding secret information in audio based on Fletcher Munson curve. The proposed technique has more payload and highly robust and have more SNR than the existing techniques. Proposed technique has 79kbps data embedding capability which has more data embedding capability than that of existing techniques.

REFERENCES

[1] Pfitzmann, B., Information hiding terminology - results of an informal plenary meeting and additional proposals. In: Proceedings of the First International Workshop on Information Hiding. Springer-Verlag, London, UK, pp. 347–350. (1996).

[2] G. J. Simmons, "The prisoners' problem and the subliminal channel" in Proc. Advances in Cryptology (CRYPTO '83), pp. 51-67.Berglund, J.F. and K.H. Hofmann, 1967. Compact semi topological semi groups and weakly almost periodic functions. Lecture Notes in Mathematics, No. 42, Springer-Verlag, Berlin-New York.

[3] Pooja P. Balgurgi, PG Student Elec. & Telecommunication department SKN College of Engineering Vadgaon Bk. Pune, India "Intelligent Processing: An Approach of Audio Steganography".

[4] H.B.Kekre, Archana Athawale, Swarnalata Rao, Uttara Athawale, "Information Hiding in Audio Signals" International Journal of Computer Applications (0975 – 8887) Volume 7– No.9, October 2010.

[5] S. Kalzeabelsser and E Petitcoals," *Information Hiding techniques for Steganography and watermarking"*, Artechhouse, Computer security series

[6] W Bender, D Gruhl, N Morimoto, A Lu, Techniques for Data Hiding. IBM Syst. J. 35(3 and 4), 313–336 (1996)

[7] Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjee and Poulami Das, "A Tutorial Review on Steganography".

[8] Bassil, Youssef. "A Two Intermediates Audio Steganography Technique." arXiv preprint arXiv: 1212.2207 (2012).

[9] "audio steg: methods", Internet publication on www.snotmonkey.com http://www.snotmonkey.com/work/school/405/methods.html.

[10] K Gopalan, et al, Covert Speech Communication Via Cover Speech By Tone Insertion, Proceeding of IEEE Aerospace Conference, (Big Sky, Montana, March 2003)

[11] K Gopalan, S Wenndt, Audio Steganography for Covert Data Transmission by Imperceptible Tone Insertion, WOC 2004, (Banff, Canada, July 8–10, 2004)

[12] M.Asad, J.Gilani, A.Khalid, 2011," An Enhanced Least Significant Bit Modification Technique for Audio Steganography", IEEE978-1-61284- 941-6/111$26.00.

[13] P.Dutta1, D. Bhattacharyya, and T.Kim, June 2009" Data Hiding in Audio Signal: A Review", International Journal of Database Theory and Application, Vol. 2, No. 2.

[14] H.B.Kekre, Archana Athawale, Swarnalata Rao, Uttara Athawale, October 2010, Information Hiding in Audio Signals, International Journal of Computer Applications (0975 – 8887) Volume 7– No.9.

[15] Zamani, Mazdak, et al. "Robust audio steganography via genetic algorithm. "Information and Communication Technologies, 2009. ICICT'09. International Conference on. IEEE, 2009.

[16] Djebbar, Fatiha, et al. "A view on latest audio steganography techniques." Innovations in Information Technology (IIT), 2011 International Conference on. IEEE, 2011.

[17] Padmashree, G., and P. S. Venugopala. "Audio Stegnography and Cryptography: Using LSB algorithm at 4th and 5th LSB layers." International Journal of Engineering and Innovative Technology (IJEIT) Volume 2 (2012).

[18] Hakeem, Abdul, Noor Ul Amin, Mohsin Shah, Zakir Khan, and Abdul Qadi. "Threshold Based LSB Audio Steganography."

[19] N. Johnson and S. Jajodia, Exploring steganography: seeing the unseen, IEEE Computer, pp. 26-34, February (1998).

[20] Dutta, P., D. Bhattacharyya, and T.-h. Kim, *Data hiding in audio signal: A review.* International journal of database theory and application, 2009. 2(2): p. 1-8.

[21] Nosrati, Masoud, Ronak Karimi, and Mehdi Hariri. "Audio Steganography: A Survey on Recent Approaches." World Applied Programming 2.3 (2012): 202-205.

[24] https://en.wikipedia.org/wiki/Fletcher%E2%80%93Munson_curves.