IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 4, April 2016

Information Hiding Techniques: Watermarking, Steganography: A Review

Shruhad Kumar J. Patel[1], Nikunj V. Tahilramani [2]

Research Scholar, Electronics and communication Dept., CGPIT, Bardoli, India [1]

Assistant Professor, Electronics and Communication Dept., CGPIT, Bardoli, India [2]

Abstract: Information hiding techniques have recently become important in a number of application areas. Now a day's digital communication has become an essential part of data transmission. Due to the increasing demand of various internet applications such as voice over IP (VOIP), audio conferencing etc, it is required that the data is transmitted in a much secure and robust manner. Direct transmission of data over the communication channel is not secure as it can be easily manipulated by intruders. This leads to lots of development of various techniques for data hiding. Steganography, Cryptography and Water marking are the popular techniques available to hide data securely.

Keywords: Information Hiding, Classification, Watermarking, Steganography.

I. INTRODUCTION

Data or information is very crucial to any individual person. None of us likes our conversation being overheard as it contains the potential of being misused. Same is the case with the data of any organization or of any person. The exchange of data among two potential parties must be in done in a secured method so as to avoid any tampering. Two types of threats exist during any information exchange. The unintended user who may try to overhear this conversation can either tamper with this information to change its original meaning or it can try to listen to the message with intention to decode it and use it to his/her advantage. Both these attacks violated the confidentiality and integrity of the message passed. Providing intended access and avoiding unintended access is a very challenging task. Information hiding has been since long time. In past, people used hidden pictures or invisible ink to convey secret information [1].

II. IMPORTANCE

The importance of data hiding techniques comes from the fact the there is no reliability over the medium through which the information is send, in other words the medium is not secured[2]. So, some methods are needed so that it becomes difficult for unintended user to extract the information from the message. Few reasons behind data hiding are:

1 Personal and private data
2 Sensitive data
3 Confidential data and trade secrets
4 To avoid misuse of data
5 Unintentional damage to data, human error and accidental deletion of data
6 Blackmailing purposes
7 Cyber crime

III. DATA HIDING TECHNIQUES

There are two major information hiding techniques focused in this paper:

1. Watermarking 2.Steganography

IV. WATERMARKING

Watermarking is the technique and art of hiding additional data (such as watermarked bits, logo and text message) in the host signal which includes image, video, audio, speech, text, without any perceptibility of the existence of additional information. The additional information which is embedded in the host signal should be extractable and must resist various intentional and unintentional attacks [3].

A. Types of digital speech watermarking

There are two main types of digital speech watermarking in terms of robustness [3]:

1. Robust digital speech watermarking in which embedded and additional information must resist channel attacks.
2. Fragile digital speech watermarking in which additional information must be destroyed if any attack or transformation takes place like for paper watermarks in bank notes. These watermarks do not survive any kind of copying and therefore can be used to indicate the bill's authenticity. Reaching for fragility is more difficult than robustness.

B. Different Techniques of watermarking:

1 Auditory Masking:

Auditory masking in general is defined by the American standards agency as 'the process by which the threshold of audibility for one sound is raised by the presence of another sound' and 'the amount by which the threshold of audibility of sound is raised by the presence of another sound'.

- Frequency Masking

In frequency (spectral) masking, if two signals have close frequencies and occur simultaneously, then the stronger signal makes the weaker signal inaudible. Each frequency has a minimum sound pressure level (SPL) for hearing called threshold which is not always linear for all frequencies. For example, high frequencies are masked more easily than mid frequencies. Frequency masking can be detected by using frequency domain [3].

IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 4, April 2016

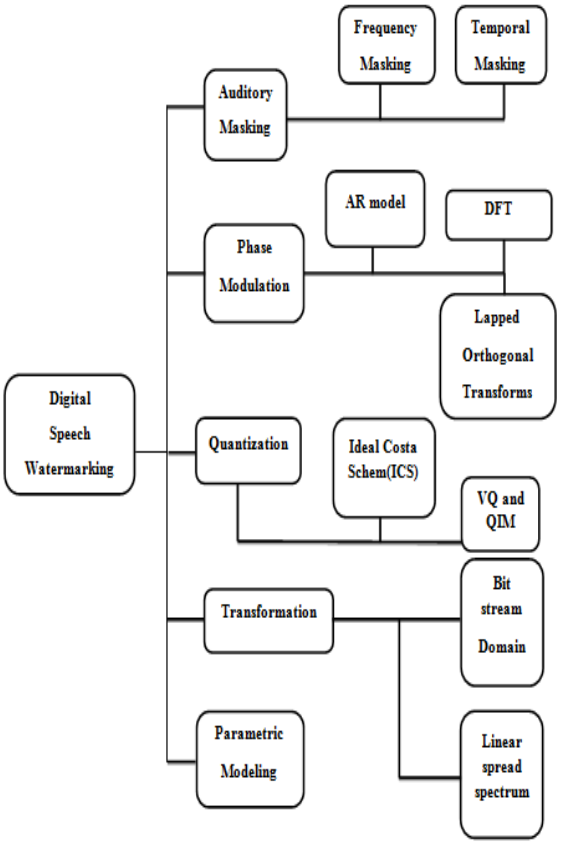

Fig 1: Classification of watermarking techniques

• Temporal Masking:
Temporal masking is of two types:1.Pre-masking 2.Post-masking.In pre-masking weaker signal becomes inaudible due to the presence of stronger masker about 5 to 20 ms. In post masking the weaker signal becomes inaudible for 50 to 200 ms after the masker[3].

2 Phase Modulation:

In the phase modulation technique watermark bits are embedded by manipulating the phase of speech signal. One main advantage of phase modulation is that the watermarked and original speech has the same power spectrum.

• Discrete Fourier Transform:
DFT phase model By applying the discrete Fourier transform (DFT), the speech signal is modeled as complex coefficient and phase angle. Short-term Fourier transform (STFT) is used for mapping between AR and DFT phase model by defining the well-defined transform size, window length and overlap. While applying DFT on unvoiced speech frames of length L, constant magnitude which remains unchanged is given, and the phase is modified. DFT uses $\frac{1}{\sqrt{L}}$Weighting for forward and inverse DFT making a unitary transform. Although every frame has L complex coefficient, only $\frac{L}{2}$ of this coefficient is independent. If L is even, DC and Nyquist frequency are real, then the total independent coefficient is $\frac{L}{2}+1$. If L is odd, DC coefficient is real but Nyquist frequency is not available, then the total independent coefficient is $\frac{L+1}{2}$. For the speech frame with L length, DFT has 2L real coefficients R, where the L odd-numbered dimensions represent the real part R_{rl} and the L even-numbered dimensions represent the imaginary part Rim of the complex DFT coefficients $X = R_{rl} + jR_{im}$. Equation shows how these phases can be calculated to become real and imaginary parts

$$X = re^{j\varphi} = a + jb$$

$$r = \sqrt{a^2 + b^2} \qquad \varphi = \text{Arctan}(\frac{a}{b})$$

where X is complex variable, r is magnitude, ϕ is phase, a is real coefficient, and b is imaginary coefficient. Some digital speech watermarking methods replace DFT phase of the original speech frames with the phase of the watermark angle while the original magnitude remains unchanged. This watermarking method is subject to AWGN n with DFT coefficient N, phase angle ψ and variance σ_N^2, resulting in the noisy watermarked signal $\hat{s}+n$, with DFT coefficient output phase angle Θ.

3 Quantization:
Depending on the application, different techniques have focus on different parameters like robustness, inaudibility etc. For some watermarking applications, quantization techniques embed the watermark in the perceptually irrelevant part of the speech. The quantization techniques for watermarking have improved the capacity of embedding the watermark in perceptually relevant and irrelevant parts of the speech (Cox et al. 2002.)

• Vector Quantization:
In this method, the original speech signals are segmented into non-overlapping frames and LPCs of each frame are calculated as input vectors for VQ. After getting input vectors, they are compared with the nearest code word in the codebook [3]. By doing this we found output vector based on pre-defined formula. At the receiver side same indices are used to get desired watermark.

• Quantization Index Modulation:
Quantization Index Modulation (QIM) applies the associated quantizer for quantizing the original speech which embeds the speech dependent watermarks [8]. For digital watermarking, the QIM technique can achieve good balance between watermark embedding capacity and robustness [3].

4 Transformation:
Transformation techniques focus on some special techniques of speech signal such as production, perception and bit rate.

• Linear Spread Spectrum:
The spread spectrum (SS) technique attempts to hide or spread secret information across the frequency spectrum of the speech signal which is independent of the actual signal. Due to which, the final signal occupies a bandwidth which is more than what is actually required for transmission. The spread spectrum technique offers better performance, moderate data rate, high level of robustness but its main limitation is that it introduces noise in the sound file.

IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 4, April 2016

V. STEGANOGRAPHY

The word steganography is of Greek origin and means "covered writing" or "concealed writing". In other words, it is the art and science of communicating in a way which hides the existence of the communication. Steganography focuses more on high security and capacity. Even small changes to stego medium can change its meaning. Steganography masks the sensitive data in any cover media like speech, images, audio, video over the internet.

Steganography involves four steps [5]:
1. Selection of the cover media in which the data will be hidden.
2. The secret message or information that is to be masked in the cover media.
3. A function that will be used to hide data in the cover media and its inverse to retrieve the hidden data.
4. An optional key or the password to authenticate or to hide and unhide the data.

B. Different techniques of Steganography:

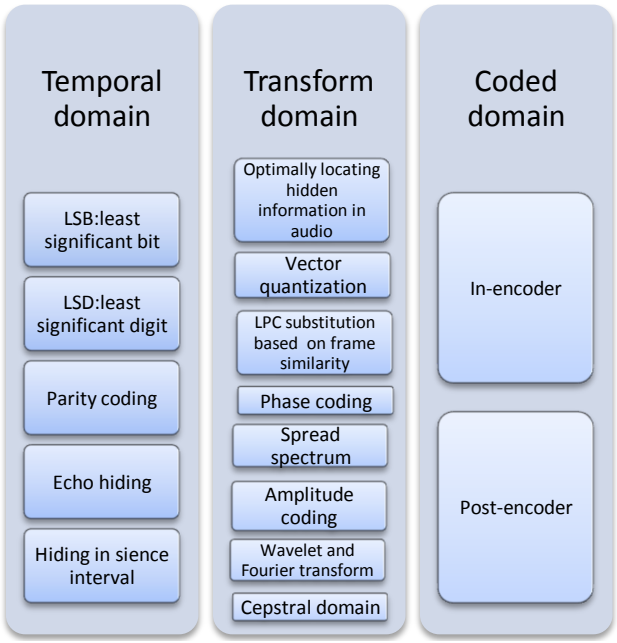

Fig: 2 Classification of steganography techniques

1. Temporal domain:
Different methods of temporal domain are discussed below.

• LSB: Least significant bit insertion:
This is one of the different methods of steganography which uses least significant bit modification.

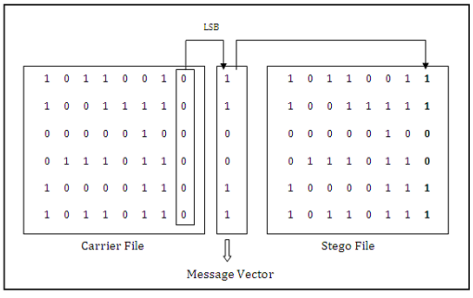

Fig: 3. LSB modification procedure [8]

This technique deals with the fact that information is contained by the MSBs rather than LSBs. In this method information hiding is done by manipulating consecutive LSBs with the message bits.

• LSD: Least significant digit insertion:
Due to the fact that LSB coding method has low hiding capacity, LSD coding technique supports higher data rate. In LSB substitution method only the operations of $0 \rightarrow 1$ and $1 \rightarrow 0$ of the LSB are applied i.e only 2 states are possible. More adjacent states of the parameter bits could be obtained in order to gain more hiding possibilities. The LSD method exploits the multiple adjacent states of the frame parameters, which are produced by multiple modification (+/-1,+/-2) and encoded as LSD using multiary numeration system[8]. In this technique of data hiding not only LSB are exploited but also least significant states are also took into consideration. Secret messages as well as the frame parameters are both encoded using the multi-ary numeration systems (e.g. ternary, 5-ary numeration), then the LSDs of the multi-ary numbers are obtained. This method takes full advantage of the various bit states of each frame parameters to gain more hiding bits ie more hiding capacity with lowest distortion, where ternary and 5-ary numerations are presented to embed $\lfloor \log^{(2n+1)}{}_2 \rfloor$ bits with n bits LSBs. For eg. In case of ternary numeration system we take into account, the three states $\{C, C + 1, C - 1\}$ which are mapped to ternary $\{0, 1, 2\}$ by a bijection. The three states represent a ternary digit denoted by $\{0, 1, 2\}$.

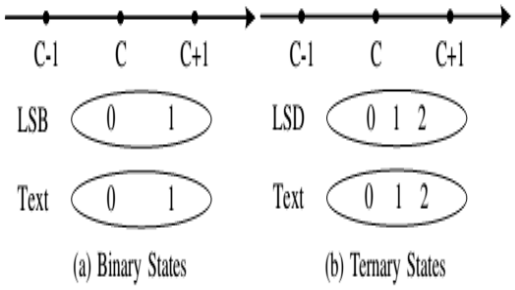

Fig: 4 State matching of LSB substitution [9]

• Parity coding:
In this method, original signal is divided into number of groups of samples which is known as sample region. one can encode the secret bits into this sample region parity bit. Hence the method is known as parity coding.

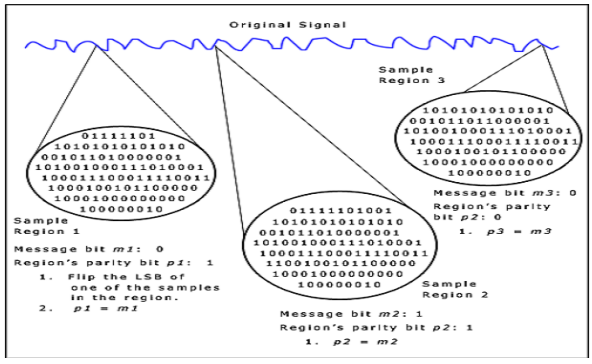

Fig: 5 Parity coding [10]

• Echo Hiding:
Echo hiding technique embeds data into a cover speech signal by introducing an echo. The secret data is hidden by varying three parameters of the echo which are initial amplitude, decay rate, and offset.

• Hiding in silence interval:
This is simple yet effective embedding method for steganography. This method exploits the silence interval in speech signal. Small intervals are not used since they occur during continuous speech and changing them would affect the speech quality. . This method has a good perceptual quality but actually it is sensitive to compression. Changes in silence intervals length would result into false data extraction.

2. Transform domain:
Steganographic systems that embed information in the frequency domain or any transform domain can be much more robust than embedding rules operating in the time domain. Most of the robust steganographic systems known today actually operate in some or other sort of transform domain. Each one of them will be discussed briefly:

• Optimally locating hidden information in audio:
Embedding a message in the selected frequency areas by making use of the human auditory system as follows[11]:

1. Find all frequency components using Fast Fourier Transform (FFT).
2. Find the magnitude range such that our human ear is not able to distinguish the difference after changing those harmonic components.
3. Within the range use any two amplitude value to distinguish message bit 0 and the message bit 1 as within that amplitude range any change to the magnitude value of the harmonics can't be distinguished by our ear. These amplitude values & position where embedding data starts, are chosen as a key and it is shared between the communication parties through secret channel.
4. Use the error correction technique so as to make it susceptible to channel errors.
5. Apply Inverse Fast Fourier Transform (IFFT) and this gives the stego data.

• Vector Quantization:
Vector Quantization (VQ) is one of the techniques based on the principle of block coding that have long been used to compress media in order to make efficient use of network bandwidth and data storage space. The codeword's of the codebook are used to substitute the closest coefficient block of the speech during the embedding.

• LPC substitution based on frame similarity:
In order to meet the requirements of high data hiding capacity, real-time and high robustness, a method based on frame similarity is suggested. This method is based on linear predictive coefficients (LPC) and analysis-by-synthesis (ABS) scheme. In this speech coding scheme, filter similarity coefficient is the better way of expressing the similarity between neighbouring frames. The reason for calculating this index is that the wave variation of neighbouring frames introduced by the slow changes of voiced signals track during voiced pronunciation is exhibited mainly on the exciting signal. If output of two filters has highly similar coefficients, their output waves are very similar. This feature is known as filter similarity.

• Phase coding:
The primary scheme is to split the original cover file into blocks and embed the whole message data sequence into the phase spectrum of the first block. One limitation of the phase coding method is that it has a considerably low data hiding rate because only the first block is used for embedding secret message and also that secret message is localized[8].

• Spread spectrum:
The spread spectrum (SS) technique attempts to hide or spread secret information across the frequency spectrum of the speech signal which is independent of the actual signal. Due to which, the final signal occupies a bandwidth which is more than what is actually required for transmission. The spread spectrum technique offers better performance, moderate data rate, high level of robustness but its main limitation is that it introduces noise in the sound file[10].

• Amplitude coding:
This technique finds secure spectral embedding-areas in a wideband magnitude spectrum of cover speech by using a frequency mask defined at 13 dB below the original signal spectrum. These embedding locations and hiding capacity in magnitude components are defined by using the human tolerated distortion level as defined in the magnitude spectrum. Since the frequency components within the range of 7 kHz to 8 kHz contribute minimally to wideband speech intelligibility, [7] so data can be hidden by completely replacing the frequencies 7-8 kHz by the message to be hidden. The method supports high hiding capacity without degrading the speech quality.

• Wavelet and Fourier transform:
This method of data embedding hides the secret speech signal into the coefficients in the wavelet domain-. DWT splits the cover speech into low and high frequency components where low frequency component is the most significant for speech perception whereas the high-frequency component impacts flavour or nuance (noise) to the signals. Hence, it is decided to hide information in the high-frequency portion of the wavelet domain. By using the wavelet analysis, the speech signal can be bifurcated in approximations and details ie. the high-scale and low-frequency components of the signal where the details are the low-scale and approximations are the high-frequency components. Both the secret and cover speech are subjected to pre-processing in order to facilitate the hiding process. Firstly the cover speech is partitioned into L-ms frames. Then for each of the time-frames DWT is calculated so as to decompose it into high and low frequency. Then the FFT is applied to the high-frequency wavelets part producing a spectrum. The obtained speech spectrum is then decomposed into magnitude and phase spectrum. The hiding process consists of representing the last L elements of the obtained spectra by the LPC parameters of the secret speech. Each of the L-ms of the

secret message is embedded in the low-amplitude high-frequency region of the magnitude spectrum of the cover signal.

• Cepstral domain:
Cepstral domain is also known as log spectral domain. Secret data in this method is embedded in the cepstrum coefficients which are more tolerant to most common signal processing attacks. Also, the cep-strum alteration at frequencies that are in the perceptually masked regions of the HAS which ensures the inaudibility of the resulting stego speech frames. The cover signal is first transformed into cepstral domain then secret data is embedded in selected cepstrum coefficient by applying statistical mean manipulations [16].

3. Coded domain:
The two codec domain technique can be distinguished as in-encoder and post-encoder.

• In-encoder:
This technique uses sub-band amplitude modulation in order to hide data in various speech and audio. Data embedding is done using a LPC vocoder. Pitch detection is done using a autocorrelation method which is used to segment speech into voiced/unvoiced. The linear prediction residual in the unvoiced segments is replaced by a secret data sequence. Once the residual's power is matched, this substitution of the cover data does not lead to perceptual distortion. The signal is conceived using the unmodified LPC filter coefficients. The technique offers a reliable hiding rate of 2kbps [7]. This technique hides secret data in the LSB of the Fourier transform of the host speech signal. An LPC filter is used to automatically shape the spectrum of LSB noise so as it remains below the audible distortion.

• Post-encoder:
This technique uses ACELP codec in order to embed data in the bitstream of cover data. Data in the bit stream of an ACELP codec which supports the analysis-by-synthesis codebook search. Data in this case is represented by folded binary code which codes each sample with a value between -127 and 127 including -0 and +0. One bit is embedded in 8-bits per sample so as to make the absolute amplitude to zero. Depending on the number of samples whose absolute amplitudes is 0, a potential data hiding rate ranging from 24 to 400 bps is achieved. The technique offers a reliable hiding rate of 2kbps [7] in a 12.2 kbps of cover speech.

VI. CONCLUSION

This paper has summarized the speech watermarking and stegnography techniques. Classification of different techniques for both watermarking and steganography is done in this paper. We believe that this paper might be useful for researchers who are interested in information hiding techniques like watermarking and steganography.

REFERENCES

1. Prof. S.N Wawale, Prof A Dasgupta, "Review of Data Hiding Techniques", International Journal for Advance Research in Engineering and Technology, Vol. 2, Issue II, Feb 2014
2. Richa Gupta , Sunny Gupta , Anuradha Singhal, "Importance and Techniques of Information Hiding : A Review", International Journal of Computer Trends and Technology (IJCTT) – volume 9 number 5– Mar 2014.
3. Mohammad Ali Nematollahi·S.A.R. Al-Haddad,"An overview of digital speech watermarking", International Journal of Speech Technology (2013) ,Springer.
4. Nikunj.V.Tahilramani and Ninad Bhatt, "Steganography in Speech Signal with Enhanced Multi-Pulse Excitation Codevector with Reduced Number of Bits", IEEE January, 2015.
5. H Kayarkar, Sugata Sanyal," A Survey of Data Hiding Techniques and their Comparative Analysis", arxiv.org
6. Mangesh Ghonge, Ankita Dhawale, Atul Tonge, "Review of Steganography Techniques", International Journal of Advent Research in Computer & Electronics, Vol. 1, No.1, March 2014.
7. Fatiha Djebbar, Beghdad Ayad Karim , Abed Meraim and Habib Hamam(2012), Comparative Study of Digital Audio Steganography Tech-niques," EURASIP journal on audio, speech and music processing, springer.
8. Shengbei Wang and Masashi Unoki, "Watermarking Method for Speech Signals based on Modifications to LSFs", © 2013 IEEE.
9. Prof. Samir Kumar(June 2012), BandyopadhyayBarnali, Gupta Banik , LSB Modification and Phase Encoding Technique of Audio Steganography Revisited, International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 4.
10. Jin Liu and Ke Zhou and Hui Tian (2011) Least-significant-digit Steganography in Low Bitrate Speech, National Basic Research Program (973 Program) of China under Grant No. 2011CB302305, Natural Science Foundation of Fujian Province of China under Grant No. 2011J05151, and Scientific Research Foundation of National Huaqiao University under Grant No. 11BS210.
11. Jayaram P, Ranganatha H R, Anupama H S(August 2011), information hiding using audio steganography – a survey, The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3
12. Premalatha P and Amritha P (2009) Optimally Locating for Hiding Information in Audio Signal, International Journal of Computer Applications (0975 – 8887) Volume 65– No.14, March 2013
13. Driss Guerchi and Fatiha Djebbar(2009), Narrowband Speech Hiding using Vector Quantization, International Journal of Information and Communication Engineering 5:8
14. WU Zhi-jun GAO Wei, YANG Wei(december,2009), LPC parameters substitution for speech information hiding ,The Journal of China Universities of Posts and Telecommunications, 16(6): 103–112
15. Siwar Rekik, Driss Guerchi, Sid-Ahmed Selouani and Habib Hamam, (2012) Speech steganography using wavelet and Fourier transforms, EURASIP Journal on Audio, Speech, and Music Processing,2012:20
16. K. Gopalan, Cepstral Domain Modification of Audio Signals for Data Embedding – Preliminary Results, "thesis Department of Engineering Purdue University Calumet Hammond, IN 46323
17. http://en.wikipedia.org/wiki/Digital_watermarking
18. Nikita Atul Malhotra and Nikunj Tahilramani, "Steganography Approach of Weighted Speech Analysis with and without Vector Quantization using Variation in Weight Factor", Vol.4, No.3 (June 2014), ©2014 INPRESSCO.
19. Qiang Cheng, Jeffrey Sorensen, "spread spectrum signaling for speech watermarking".
20. Xiaoxiao Dong, Mark F. Bocko, Zeljko Ignjatovic, "DATA HIDING VIA PHASE MANIPULATION OF AUDIO SIGNALS", ©2004 IEEE.
21. Li Xin ,Zhang Ru , Niu Xinxin, Liu Jianyi, "Analysis of the Security for Information Hiding Based on Behavior", (AISS) Volume4, Number5, March 2012.
22. Masahiro Yashita, Nozomu Hamada , "Time-Frequency Masking Method Using Wavelet Transform for BSS Problem", ©2006 IEEE.
23. Mohammadreza Narimannejad, Seyed Mohammad Ahadi, "Watermarking of Speech Signal through Phase Quantization of Sinusoidal Model".
24. Siwar Rekik, Driss Guerchi, Sid-Ahmed Selouani and Habib Hamam, "Speech steganography using wavelet and Fourier transforms", EURASIP Journal on Audio, Speech, and Music Processing 2012.
25. Brian Chen and Gregory W. Wornell, "Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding", IEEE Trans., September 2000.

BIOGRAPHIES

Shruhad Kumar J. Patel received his B.E., from A.I.T.S, Rajkot in 2014 and pursuing M.Tech. ICT in C.G. Patel Institute of Technology, Bardoli. He is working as a Research Scholar, Electronics and communication department, C.G. Patel Institute of Technology. His research interests are speech processing and wireless communication.

Mr. Nikunj Tahilramani has received B.E from Veer Narmad South Gujarat University, Surat in 2005 and received M.E from Mumbai University in 2012. He is pursuing his PhD degree in the area of Information Hiding in the Speech Signal from Uka Tarsadia. He has totally 4 years of teaching experience. Presently he is working as an Assistant Professor, Department of Electronics and Communication in Chhotubhai Gopalbhai Patel Institute of Technology (CGPIT), Bardoli. His research interest lies in Speech Processing Applications, Embedded Systems, Signal and Systems, Microprocessors & Microcontrollers and Industrial Automation. He is an active and Life member of IEEE, ISTE and IEI.

DOI 10.17148/IJIREEICE.2016.4440