Tamper Detection in Speech based Access Control Systems using Watermarking

Bala Mallikarjunarao Garlapati, Srinivasa Rao Chalamala, Krishna Rao Kakkirala
TCS Innovation Labs, Hyderabad, India
balamallikarjuna.g@tcs.com, chalamala.srao@tcs.com, krishna.kakkirala@tcs.com

***Abstract*— General voice based access control systems are based on voice biometrics. This process enables an unauthorized access by recording the voice of the authorized person. So there is a requirement to prevent unauthorized access through recording speech. Other than voice biometrics, here we have two challenges. (i) To extract the authentication information. (ii) To find the unauthorized source. The speech goes through DA-AD-DA conversion, while it is recorded and used for access control. The watermarking method which will use for this purpose must be robust to DA-AD conversion attack, which is usually involved in recordings. In this work, we propose a method based on casting Log Co-ordinate Mapping (LCM), in which embedding two watermark segments in two different frequency regions, one for authentication information purpose and other for finding unauthorized source. The LCM method has approving performance against DA-AD conversion attacks [1]. The modifications made for this does not impact the perceptible auditory quality and the embedding capacity improved by selecting the appropriate frequency regions in the log scale. Our results show that our method robustly extracts the source identification information while detecting the malicious source if the audio is being recorded and played back by unauthorized source.**

Keywords*– *audio watermarking; DA-AD attack; tamper detection; access control;

I. INTRODUCTION

Audio/speech data can be easily recorded with the handheld devices available today, so it is important to ensure the integrity of the audio data used for authentication. An audio signal carries the watermark information and the embedding method is called watermarking scheme. There are different applications for audio watermarking. The initial purpose of watermarking is for copyright protection. The most important purposes are the proof of ownership and the enforcement of usage policy. In addition, watermarking can also be used for fingerprinting, broadcast TV ratings and for adding additional features to a media.

Access control systems that use the speech as biometric for authentication over the air, are increasingly being used. The user authentication of access control system is achieved by using watermarking schemes. These watermarking schemes robust to DA-AD conversion which will happen in audio recording process. The watermark should persist in the recording process and the system should grant the access. But if a traitor record the genuine audio and try to access the system, system should reject and can not provide the access. The watermarking method presented in this paper provides solution to this problem.

The watermark must be sustain for first time DA-AD process, this will happen in case of genuine user to provide the access and watermark will be removed for second time or more DA-AD conversion process, this will happen in case of malicious user to deny the access. The authenticity of the genuine user can be achieved by extracting user information as a watermark, from the audio/speech data. The genuineness of the user is achieved by finding the correctness of extracted watermark. Instead of two different techniques for the two purposes such as extraction of authentication information and finding of malicious source, we accomplished with one algorithm.

II. RELATED WORK

A scheme for tamper detection in audio based access control system is proposed. This can be achieved by using audio watermarking method which are robust against DA-AD conversion attacks. The geometric distortions that are caused against audio recordings are pitch invariant time-scale modification (TSM), tempo invariant pitch shifting and random cropping. Possible geometric distortions during recording are pitch invariant time-scale modification (TSM), tempo invariant pitch shifting and random cropping. There haven't been many works that are related to this application but some works that are relevant to the theme of watermarking schemes, which are robust for audio recordings over the air available.

There have been works that are robust against DA-AD conversion process explained [1]-[3]. An audio watermarking algorithm proposed by Xiangui Kang et al [1], based on LCM feature, which gives better results for an audio signal effected by geometric distortions. And also shows good performance against signal processing attacks like compression, low pass filtering. A relation based watermarking method proposed by Shijun Xiang [3] by adjusting the energies in adjacent sections of DWT coefficients.

An overview and basics about audio watermark methods can be found in[5] and refer [6-8] for spread spectrum based audio watermarking techniques. Other watermarking techniques have been studied in [10-11],[14], which gives overview of the today's audio watermarking technology.

978-1-4673-8675-3/15 $31.00 © 2015 IEEE
DOI 10.1109/AIMS.2015.59

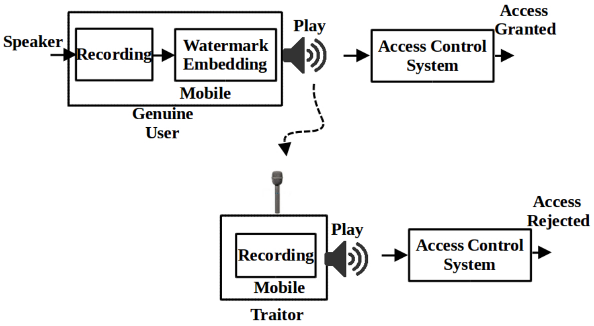

Figure 1. Tamper detection in Access Control System

A method proposed by Haitsma et al. [4] which modifies the Fourier coefficients according to watermark bits, shows good performance against pitch invariant TSM, MP3 (64 kbps), and echo addition, but suffers from pitch shifting attack. A chirp based blind watermarking method for tamper detection proposed by Omar Farooq [9]. A spread spectrum based scheme which has significant performance for DA-AD conversion with line-in jack proposed by Xing He and Michael S. Scordilis [12]. Lang, A et al. in [13] explained the performance evaluation of audio watermarking methods and DA-AD process.

III. Proposed scheme

We propose a mechanism for tamper detection in access control system, which uses a voice or speech used as a biometric. It is important to make the identification of genuine user while detecting the recorded signal by a unauthorized person. A LCM feature based watermarking algorithm, exhibits better performance for geometric variations in recorded signal. By choosing different frequency regions in the algorithm, we can achieve genuine user information extraction and unauthorized source detection. The selection of frequency region is based on which frequencies are more robust and vulnerable to DA-AD conversion. The region used for genuine user information extraction is low frequency region, because it is more robust to DA-AD conversion, as the low frequency regions are less affected by play & record process. The frequency region used for malicious user detection is high side (compared to the source identification frequency region), because if it is recorded by a traitor, the inserted watermark bits should effect in the extraction. The length of watermark bits used for malicious user detection are less compared to audio source information.

The pictorial view of speech based access control system shown in figure 1. This system provide access only when authentication data is extracted from playing audio. A genuine user who wants access, will record his voice. The system embeds authentication data into the live speech and this speech is used for gaining access. A traitor may record it over the air, for gaining unauthorized access. The access control system must be able to reject such kind of malicious access requests. Access control system extracts authentication information and validates it. On successful validation grants access. So we are presenting an algorithm which provide access to genuine user and reject the access for traitor. This is achieved if the authentication data was not available in traitor recordings.

The remaining sections are organized as follows. Introduction to Log coordinate mapping feature and the selection of different factors (frequency region and embedding strength factor) for tamper detection are explained in section IV. Detail description about watermark embedding and extraction methods implementation shown in section V. Section VI shows the results for proving the tamper detection and followed by conclusion in section VII.

IV. Background

Log coordinate mapping (LCM) feature based watermarking method [1] proven to be robust due to its inherent resistance to time scaling, pitch shifting and translation. In this section we briefly introduce the LCM feature calculation and how it is resilient to the scaling, pitch shifting etc.

A. Log coordinate mapping (LCM) feature

The log coordinate mapping process improves the robustness of watermark against geometric attacks. It is well known that scaling in time domain is equivalent to inverse scaling in the frequency domain. Also log scale converts scaling into shifting, translation in the direction axis. In general, the length of the audio clip varies when played and recorded over the air (DA-AD). The spacing between the sampling instances may not be uniform due to the hardware and clock jitter. We briefly discuss how the LCM transforms scaling into shifting.

The general Fourier transform is represented as

$$x_j = \sum_{k=0}^{N-1} z_k \exp(-2\pi ijk/N) \tag{1}$$

and its inverse transformation is

$$z_j = \frac{1}{N} \sum_{k=0}^{N-1} x_k \exp(2\pi ijk/N) \tag{2}$$

When the signal is scaled in time domain, its Fourier transform can be written as

$$f(pt) <-- > 1/pF(f/p) \tag{3}$$

If we represent

$$f' = \beta * f \tag{4}$$

in logarithmic domain, it becomes,

$$log(f') = log(\beta) + log(f) \tag{5}$$

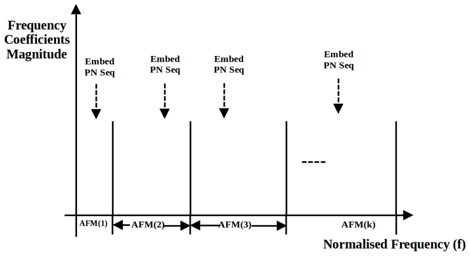

Figure 2. Average Frequency Magnitude (AFM) frequency bands

Hence the scaling in time domain becomes addition in logarithmic frequencies.

1) Calculation of Average Frequency Magnitude (AFM): AFM is the average of frequency component magnitudes over certain frequency bands. To compute the AFMs first convert discrete signal into frequency domain. The frequency index must be normalized after Fourier transform. Select a range of normalized frequency indexes and apply log coordinate mapping (LCM) on the selected frequency region. The bands are selected according to the requirements of the application, in our case for watermarking we need to select frequency range that is robust to the attacks. The number of AFM bands depends on the number of watermark bits required to be added i.e. embedding capacity. If the embedding capacity is more, we need more AFM bands and vice versa. Fig. 2 shows some more details of AFM bands. Repeatedly add a bit of PN sequence to all the frequency coefficients, in all AFM bands.

B. Tamper detection

In a generic voice based access control systems, authentication of the user is done based on the voice biometrics. But to limit the access for unauthorized users who intentionally record the speech of the authorized user, two different watermarks are added to the speech/audio recorded on a smart phone. Access is granted to the authorized user by correctly retrieving watermark designated for this. Any unauthorized accesses are rejected by way of incorrectly retrieving the other watermark as it would pass through multiple cycles of AD-DA attacks i.e. in one cycle, it is recorded while the authorized user presents it to the access control system, and in another cycle it presented by the malicious user and finally being recorded by the access control systems for watermark retrieval.

Our contribution for this paper is that, we developed a mechanism of validation of the user and traitor detection with just one watermarking algorithm reducing the security threats. This is achieved by selecting right frequency regions and the configuration parameters of the algorithm. These parameters include the watermark strength and embedding capacity.

1) Authentication by watermark extraction: In any watermarking systems a user is represented by unique identification number and this id is embedded into the medium. The access control system when presented with the recorded speech/audio extracts the watermark and verifies it to find if that is a valid request from the registered user. If the request is valid, it gives the access to the concerned user. The information such as user id, access rights are represented in binary form. This binary information is embedded as watermark in the audio or voice.

For the authentication purpose of genuine user, the watermark is added in AFMs of low-frequency regions of LCM values. The system records the presented audio and extracts the watermark information from the low frequency regions and validates the access rights. Due to signal processing operations on the recorded speech and environment conditions the watermark extraction may not be accurate (not 100%, because the data transfered over the air). In order to achieve zero error, error correction codes have been used in this work.

In this experiment, We mimic the access control system with a mobile phone and a laptop (under the assumption that access control system has similar hardware specifications.). The watermarked audio is played on the laptop in front of the mobile phone. The recorded audio by this authorized mobile phone (access control system) is used for validating the access rights. On successful validation access rights are granted to the designated user.

2) Traitor detection: An unauthorized person may record the audio secretly by another mobile phone, while an authorized user presenting the audio for the access. When the secretly recorded audio presented to the access control system by the traitor for access, the access control systems must be able to find if that is coming from a different source. For this purpose we designated the a high frequency region for embedding the watermark for tamper detection. This frequency region has been selected for this purpose because of its vulnerability to inherent multiple cycle DA-AD attacks. Because of these inherent DA-AD conversion the watermark added in high frequency region can't be extracted correctly but when presented by the right user all the watermark bits are extracted correctly.

We need to select a proper threshold according to system environment to differentiate the traitor with a genuine user. In this second watermark case we would not be using any error correction mechanism. Please refer the results section for the robustness of the algorithm. The embedding capacities (watermark bits per second) used for these two scenarios depends on the embedding strength factor, biometric medium (speech or audio) and the surrounding environment. The embedding strength factor and embedding capacity will influence the perceptual quality of watermarked audio.

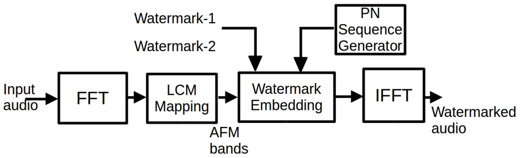

Figure 3. Watermark embedding method

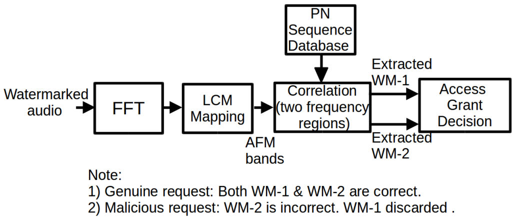
PN Sequence Database
Watermarked audio
FFT
LCM Mapping
Correlation (two frequency regions)
Extracted WM-1
Extracted WM-2
Access Grant Decision
AFM bands
Note:
1) Genuine request: Both WM-1 & WM-2 are correct.
2) Malicious request: WM-2 is incorrect. WM-1 discarded .

Figure 4. Watermark extraction process

V. Implementation

A. Watermark Embedding Process

Audio watermark embedding process block diagram is shown in Fig.3. An user id information (along with access permissions) for the genuine user is embedded into the speech/audio using LCM algorithm. In this process, the input audio divided into frames of fixed number of samples, each of the frame being one second of data (in our experiment it is 44100 audio samples). The size of frame selection depends on the real time and memory requirements of your application system.

Two binary message sequences called as watermark segments created, one for embedding in lower frequency region and the second one for embedding in higher frequency region. The first one being the user id of the genuine user and the second one being a fixed binary pattern common to all the users. Generate a PN sequence of sufficient length based on the number of AFMs. We used a 32-bit PN sequence in our experiments for watermark bit '1' (or bit '0') and its negation to bit '0' (or bit '1').

Each input frame is converted into frequency domain using FFT and defined two frequency region bounds using frequency normalization index. Each frequency region divided into AFM bands using Log Coordinate Mapping(LCM) feature. The number of AFM bands depends on the embedding capacity. PN sequence corresponding to user information watermark, embedded in to low frequency region AFM band frequency coefficients and PN sequence corresponding to unauthorized source detection watermark, embedded into high frequency region AFM band frequency coefficients.

For all frequency coefficients in an AFM band,

$$\begin{aligned} AFM_k(i) &= AFM_k(i) * (1 + \alpha * PN(k)) \; for \; wm \; bit \; '1' \\ &= AFM_k(i) * (1 - \alpha * PN(k)) \; for \; wm \; bit \; '0' \end{aligned} \tag{6}$$

Steps involved in watermark embedding are given as follows.

1) Define the algorithm configuration parameters such as frame size, frequency normalization index , embedding capacity and embedding strength factor.
2) Generate a PN sequence, that identifies a owner of the content. For N users of the content generate N-PN sequences.
3) Generate another PN-sequence that is common to all the users. And is used for malicious user detection.
4) The input audio signal or speech is divided into fixed size frames. Here we used frames of duration 1 second data.
5) Compute Fourier transform on each of the frames.
6) Compute AFM frequency bands using log coordinate mapping feature.
7) Embed the watermark bipolar PN sequence into the AFM frequency band coefficients with pre-defined strength factor, according to equation (6).
8) Apply inverse LCM mapping and inverse FFT to obtain watermarked frames and concatenate all of them to obtain the watermarked signals.
9) Apply the same procedure for both watermarks for different frequency bands.
10) Repeat the steps 4 to 9, for whole audio file.

B. Watermark Extraction Process

To prove the ownership of the content it is required to extract the watermark. The block diagram for watermark extraction process is given in Fig .4. In this process, the audio signal is divided into frames, converted into frequency domain. Frequency region bounds are selected as in embedding process.

This is blind audio watermarking scheme. To extract the watermark, AFM band frequency coefficients are correlated with the PN sequence (the same which is used in embedding process), and the correlation peak decide the watermark bit '1' or '0'. For identification of malicious request both watermarks are extracted from different frequency regions. The extracted watermark segment2 is compared against the one which is embedded.

To prove the ownership of the content it is required to extract the watermark. The implementation steps of the extraction algorithm process are given below.

1) Define the algorithm configuration parameters such as frame size, frequency normalization index , embedding capacity and embedding strength factor.
2) Generate a PN sequence, that identifies a owner of the content. For N users of the content generate N-PN sequences.

3) Generate another PN-sequence that is common to all the users. And is used for malicious user detection.
4) The input audio signal or speech is divided into fixed size frames. Here we used frames of duration 1 second data.
5) Compute Fourier transform on each of the frames.
6) Compute AFM frequency bands using log coordinate mapping feature.
7) Correlate average magnitudes of frequency coefficients with in an AFM band with the PN sequence. For K-bits of watermark,

$$\begin{aligned} &Correlation_k = [AFM_k * PN_k] \\ &where\ '*'\ refers\ correlation\ operator. \end{aligned} \tag{7}$$

8) Threshold the correlation peak and hence extract the bit, based on PN or -PN.
9) Repeat the steps 4 to 8 and extract both the watermarks from both the frequency regions.
10) Compare the extracted watermark with stored ones and grant access accordingly.

C. Working of access control system

The access control system does two verifications. 1.The device it presents the audio. 2.The user when a request for access is received by the access control system. It first extracts the watermark-2 and verifies it for correctness. If the watermark-2 is correct then the access control system extracts watermark-1 also and verifies the user. If the watermark-2 is incorrect then the access control system decides that the access request is receiving from a malicious user and discards it.

VI. Results

In this section, experimental results for the proposed tamper detection method are discussed. The results are shown for one audio and one speech file, having duration of 244 and 509 seconds respectively. The sampling frequency of audio files is 44100 Hz. Audio/Speech signal divided into frames, and the watermark bits are embedding in AFM coefficients of each frame. The length of each frame is 1 second audio/speech data.

Two watermark bit sequences chosen, one for genuine user identification purpose and another for traitor detection. The total number of watermark bits that can be embedded is a function of embedding capacity and the duration of audio signal.

$$\begin{aligned} Total\ WM\ Bits = Duration(insecs) * \\ Embedding\ capacity(in\ bits\ per\ sec) \end{aligned} \tag{8}$$

Using the procedure described earlier both the watermarks are extracted. The extracted watermark is in error means at least one-bit of extracted watermark is in error. For genuine user access request all the watermark bits in the first watermark must be extracted correctly. For a malicious access request at least one watermark bit must in error in the second watermark extracted.

TABLE I
Bit Error Rate (BER) analysis of the proposed algorithm for different embedding strength factors

	Embedding Strength Factor = 0.3		Embedding Strength Factor = 0.5		Embedding Strength Factor = 1.0	
Embed Capacity (in BPS)	BER without ECC (%)	BER with ECC (%)	BER Without ECC (%)	BER with ECC (%)	BER without ECC (%)	BER with ECC (%)
5	0.69	0	0	0	0	0
10	0.31	0	0	0	0	0
20	0.58	0	0	0	0	0
30	0.57	0	0	0	0	0
40	2.78	0	0.07	0	0.07	0
50	5.03	1.39	1.62	0	1.50	0
60	14.78	10.06	11.93	3.74	11.78	3.16

TABLE II
Bit Error Rate (BER) analysis of the proposed algorithm for MP3 compression attack

	MP3 Bitrate = 32 kbps		MP3 Bitrate = 64 kbps		MP3 Bitrate = 128 kbps	
Embed Capacity (in BPS)	BER without ECC (%)	BER with ECC (%)	BER Without ECC (%)	BER with ECC (%)	BER without ECC (%)	BER with ECC (%)
5	0	0	0	0	0	0
10	0	0	0	0	0	0
20	0	0	0	0	0	0
30	0.1	0	0	0	0	0
40	0.66	0	0.22	0	0.07	0
50	3.33	0	1.91	0	1.62	0
60	13.12	6.18	12.12	3.8	11.97	3.88

Initially we tested the algorithm for different embedding capacities with different embedding strength factors. The results are shown in table I. After that we tested for signal processing attacks sampling conversion and compression attacks. The algorithm showed approved performance and the results are showed in Table II, III & IV.

We can observe that the bit errors are nil for embedding capacities 0-30, for both the watermarks. So we chosen these embedding capacities and the strength for the practical situations. Watermark has been embedded into both the lower and high frequency regions. The watermark files are played on a laptop. Recorded using two separate smart phones. One smart phone resembling the access control system and other smart phone resembling the traitor. The recorded audio checked for both the watermarks. The recorded audio on the other (traitor) smart phone is played again for extraction of watermark. The access control system expected to fail, to extract correct watermark in this case.

The frequency region used for user and access control information extraction is 2205-4410 Hz with a scale factor of 0.8. For different embedding capacities, the watermark

TABLE III
BIT ERROR RATE (BER) ANALYSIS OF THE PROPOSED ALGORITHM FOR AAC COMPRESSION ATTACK

	AAC Bitrate = 32 kbps		AAC Bitrate = 64 kbps		AAC Bitrate = 128 kbps	
Embed Capacity (in BPS)	BER without ECC (%)	BER with ECC (%)	BER Without ECC (in %)	BER with ECC (in %)	BER without ECC (in %)	BER with ECC (in %)
5	0	0	0	0	0	0
10	0.62	0	0.62	0	0.62	0
20	1.32	0	0.58	0	0.58	0
30	2.39	0	0.96	0	0.67	0
40	3.23	0.22	1.17	0	1.32	0
50	5.32	2.78	3.65	0.69	3.01	0.52
60	14.8	7.61	13.17	5.46	12.92	5.03

TABLE IV
BIT ERROR RATE (BER) ANALYSIS OF THE PROPOSED ALGORITHM FOR SAMPLING CONVERSION ATTACK

	Up sampling attack		Down sampling attack	
Embedding Capacity (in BPS)	BER without ECC (in %)	BER with ECC (in %)	BER Without ECC (in %)	BER with ECC (in %)
5	0	0	0	0
10	0	0	0	0
20	0	0	0	0
30	10.15	3.45	10.15	3.45
40	25.88	24.34	25.88	24.34
50	36.11	33.33	36.11	33.33
60	36.11	33.33	36.11	33.33

segments extraction and the overall BER (Bit Error Rate) are tabled in Table V. Error bits are zero in all segments till the embedding capacity is 20 bps. Error correction code (Reed-Solomon) is used to achieve 0% BER.

Watermark-2 for traitor detection is added in the frequency region 4410-8820 Hz with a scale factor of 0.4. The watermark extraction results are given in Table VI. It is expected that when the watermark is added in the high frequency region (4410-8820 Hz) it results in zero error when directly presented by genuine smart phone. But when presented by malicious smart phone it results in non zero errors in the extracted watermark, enabling detection of it. Table VI, VII shows how the watermark-2 is in error, when presented by genuine user and a traitor.

TABLE V
USER IDENTIFICATION PROCESS FOR AN AUDIO FILE: BIT ERROR RATE (BER) ANALYSIS FOR GENUINE AUDIO

File: test_audio.wav Sampling frequency : 44100 Hz Active Freq region: 2205 to 4410 Hz Scale factor : 0.8 Segment length: 36 wm bits One Wm bit: 32 bit PN seq Duration: 244 seconds				
Embed Capacity (in BPS)	No.of Total Segments	No.of Error Segments	BER Without ECC in %	BER With ECC in %
10	67	0	0	0
15	101	0	0	0
20	135	0	0	0
30	203	0	0	0
40	271	3	0.96	0

TABLE VI
TRAITOR DETECTION PROCESS FOR AN AUDIO FILE:
SEGMENT ERROR RATE (SER) ANALYSIS FOR 'GENUINE' AUDIO SOURCE

File: test_audio.wav Sampling frequency : 44100 Hz Active Freq region: 4410 to 8820 Hz Scale factor : 0.4 Segment length: 36 wm bits One Wm bit: 32 bit PN seq Duration: 244 seconds Threshold(Th.): 5%					
Embed Capacity (in BPS)	No.of Total Segments	No.of Error Segments	BER Without ECC in %	SER Without Th. in %	SER With Th. in %
10	67	0	0	0	0
15	101	1	0.05	2	0
20	135	3	0.07	4.5	0
30	203	6	0.96	7	0
40	271	11	4.05	10.7	0

TABLE VII
TRAITOR DETECTION PROCESS FOR AN AUDIO FILE:
SEGMENT ERROR RATE (SER) ANALYSIS FOR 'TRAITOR' AUDIO SOURCE

File: test_audio.wav Sampling frequency : 44100 Hz Active Freq region: 4410 to 8820 Hz Scale factor : 0.4 Segment length: 36 wm bits One Wm bit: 32 bit PN seq Duration: 244 seconds Threshold(Th.): 5%					
Embed Capacity (in BPS)	No.of Total Segments	No.of Error Segments	BER Without ECC in %	SER Without Th. in %	SER With Th. in %
10	67	67	6.97	100	100
15	101	101	7.19	100	100
20	135	135	8.3	100	100
30	203	203	10.15	100	100
40	271	271	18.26	100	100

BER threshold of 5% is used for identifying the correct or incorrect watermarks. Table VI represents the use case for watermark-2 extraction for a genuine user access request and Table VII & VIII for the use case for malicious user access request.

VII. CONCLUSION

In this paper a mechanism for malicious user detection has been proposed for access control system that use speech/audio commands for access control. The proposed

TABLE VIII
TRAITOR DETECTION PROCESS FOR A SPEECH FILE:
SEGMENT ERROR RATE (SER) ANALYSIS FOR 'TRAITOR' SPEECH RECORD

<table>
<tr><td colspan="6">File: test_speech.wav
Sampling frequency : 44100 Hz
Active Freq region: 4410 to 8820 Hz
Scale factor : 0.4
Segment length: 36 wm bits
One Wm bit: 32 bit PN seq
Duration: 509 seconds
Threshold(Th.): 5%</td></tr>
<tr><td>Embed Capacity (in BPS)</td><td>No.of Total Segments</td><td>No.of Error Segments</td><td>BER Without ECC in %</td><td>SER Without Th. in %</td><td>SER With Th. in%</td></tr>
<tr><td>10</td><td>103</td><td>100</td><td>8.37</td><td>97.09</td><td>100</td></tr>
<tr><td>15</td><td>170</td><td>165</td><td>11.23</td><td>97.06</td><td>100</td></tr>
<tr><td>20</td><td>227</td><td>219</td><td>17.3</td><td>96.47</td><td>100</td></tr>
<tr><td>30</td><td>339</td><td>328</td><td>20.43</td><td>96.75</td><td>100</td></tr>
<tr><td>40</td><td>394</td><td>363</td><td>33.78</td><td>92.36</td><td>100</td></tr>
</table>

method is robust to compression and geometric distortions that are inherent in the process. The simulation results proved that access control systems provides access to genuine user and access is denied in case of traitor. This is achieved by proper selection of configuration parameters like embedding capacity, embedding strength factor and frequency region during embedding. In addition to D/A to A/D, the algorithm also tested for general signal processing attacks like sampling conversion, MP3 compression and AAC compression. As a future work, we would like to extend the access control system performance for longer recording distances.

REFERENCES

[1] Xiangui Kang; Rui Yang; Jiwu Huang, Geometric Invariant Audio Watermarking Based on an LCM Feature, Multimedia, IEEE Transactions on , vol.13, no.2, pp.181,190, April 2011.

[2] Garlapati, Bala Mallikarjunarao, and Krishna Rao Kakkirala. "Malicious audio source detection using audio watermarking." Multimedia and Broadcasting (APMediaCast), 2015 Asia Pacific Conference on. IEEE, 2015.

[3] Shijun Xiang; Audio watermarking robust against D/A and A/D conversions, EURASIP Journal on Advances in Signal Processing, 2011, Volume 2011.

[4] J. Haitsma, T. Kalker, and F. Bruekers, Audio watermarking for monitoring and copy protection, in Proc. 8th ACM Multimedia Workshop, Los Angeles, CA, 2000, pp. 119122.

[5] Xing He Watermarking in Audio, Key techniques and technologies , Published by Cambria Press (2008-01-28).

[6] Cheng, Qiang, and Jeffrey Scott Sorensen. "Spread spectrum signaling for speech watermarking." U.S. Patent No. 6,892,175. 10 May 2005.

[7] D. Kirovski and H. S. Malvar, Spread-spectrum watermarking of audio signals, IEEE Trans. Signal Process., vol. 51, no. 4, pp. 10201033, Apr. 2003.

[8] R.Garcia, Digital Watermarking of Audio Signals Using a Psychoacoustic Auditory Model and Spread Spectrum Theory, in AES 107 Convention, New York, 1999.

[9] Omar Farooq, S. Datta, Jonathan Blackledge, Blind Tamper detection in Audio using Chirp based Robust Watermarking, WSEAS Trans. On Signal Processing, ISSN: 1790-5052, Volume 4, Issue 4, April 2008.

[10] Lei, Bai Ying, Yann Soon, and Zhen Li. "Blind and robust audio watermarking scheme based on SVDDCT." Signal Processing 91.8 (2011): 1973-1984.

[11] Hussain, Iqtadar. "A novel approach of audio watermarking based on S-box transformation." Mathematical and Computer Modelling 57.3 (2013): 963-969.

[12] Xing He and Michael S. Scordilis Efficiently Synchronized Spread-Spectrum Audio Watermarking with Improved Psychoacoustic Model, Research Letters in Signal Processing Volume 2008.

[13] Steinebach, M.; Lang, A.; Dittmann, J.; Neubauer, C., Audio watermarking quality evaluation: robustness to DA/AD processes, Information Technology: Coding and Computing, 2002. Proceedings. International Conference on , vol., no., pp.100,103, 8-10 April 2002.

[14] Darabkh, Khalid A. "Imperceptible and Robust DWT-SVD-Based Digital Audio Watermarking Algorithm." Journal of Software Engineering and Applications 7.10 (2014): 859.