Tampering Detection in A Digital Record Based on Enf Criterion Under Noisy Environment

Thushara Mathew[1], Maria Joseph[2]
[1, 2] Dept of Electronics and Communication Engineering
[1, 2] Idukki, Kerala, India

Abstract- *The electric network frequency (ENF) can be used as an important criterion for the digital record authentication in forensic laboratories. The authentication is performed by extracting the ENF signals from the test and reference signals. In this method, we calculate the absolute error between the test and reference signals. The observations from absolute error map (AEM) are utilized for the tampering location identification. The AEM is obtained from the ENF matching process. Various types of tampering attacks such as insertion, deletion and splicing are considered here. Then we propose a line detection method to identify whether the digital record is altered or not. The AEM shows error in presence of noise. In this paper a navel solution to this problem is presented.*

Keywords- Electric network frequency (ENF), Digital record authentication, Tampering detection

I. INTRODUCTION

The wide availability of media altering software and tools makes the manipulation of them much easier. The digital records such as audio, video can be used as a valid proof for criminal justice. Tampering detection in a digital record is a noteworthy issue looked by our community today. We are for the most part thinking about three types of tampering in this paper. Various types of tampering attacks are insertion, deletion and splicing. Insertion or deletion implies inserting a frame into the original audio record or erasing a frame from the original record. But splicing is the concatenation of more than one frame.

There are mainly two types of tampering detection methods. Active audio tampering detection is one of the approaches used for the authentication of digital records. The authentication based on watermark [1], signature scheme [2] are active type. But the requirement of previous knowledge about the original record is the major problem faced by active tampering detection methods. While passive tampering detection does not require the prior knowledge about the original record. The statistical property of the noise residue extracted from a test audio can be used for the authentication purpose [3]. But this method is not applicable for advanced audio authentication. Detection of digital audio forgeries by checking the frame offsets are applicable only for single compressed audios [4]. The analysis of Bi-spectrum [5] and wavelet singularity [6] are other methods. But both the methods are based on an assumption that the higher order statistics will be introduced in the forged locations.

Recently, the Electric Network Frequency (ENF) which has taken a great number of researcher's attention [7]. It is naturally imprinted in all digital records. Its value ranges from 50 to 60 Hz. The audio tampering detection discussed in [8] is one of the existing work based on ENF. This method examines the ENF phase discontinuity due to tampering. The work in [9] is an alternative method by calculating the maximum offset for cross- correlation (MOCC) between test and reference ENF. But the ENF phase estimation will be disturbed by noise and disturbances present in the frequency band. These noise and disturbances can create phase discontinuities as ENF signals are much weaker than audio content. Digital record authentication by plotting the Absolute-Error-Map (AEM) is a tampering detection technique [10]. This paper is a solution for the problems faced by the authentication techniques by calculating Minimum Mean Square Error (MMSE). But the AEM will not provide the correct data for a noisy audio. Hence, the authentication and tampering detection will be improper.

This paper is a solution to the problems faced by the works in [8], [9], [10]. Here we propose a normalised LMS filter to cancel the noise present in the audio record. Normalised LMS algorithm overcomes the slow rate of convergence and misadjustment problems of the LMS algorithm. The digital record authentication based on MMSE has been showed some fault results. Because, the segments before and after the tampered location will makes the MSEs biased. Therefore, we propose a new measurement method by calculation the absolute error between extracted ENF signals. Further, a line detection based on the observations from AEM is used for the tampering detection.

II. TAMPERING DETECTION BASED ON ENF

A. Flow Chart

The audio authentication system based on ENF signals is completely described in fig.1.

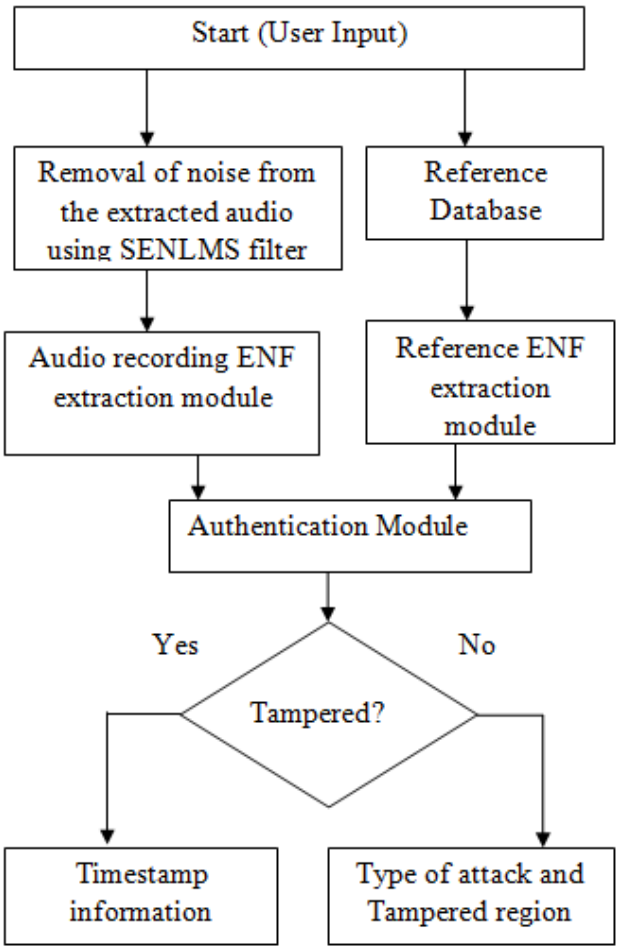


Fig.1: Audio authentication system based on ENF signals

The user inputs a questioned audio or video into the system. The system first removes the noise present in the questioned audio by using Signed Error Normalised LMS (SENLMS) filter. The reference ENF is taken from the reference database. Let *y(n)* is the filter output, then it is given by,

$$y(n) = w(n) * x(n) \qquad (1)$$

Where *x(n)* is the input audio vector and *w(n)* is the weight vector. Then updated weight vector is,

$$w(n+1) = w(n) + \mu(n)e(n)x^*(n) \quad (2)$$

Here, *e(n)* is the error vector. At the ENF extraction module, we extract ENF signals from the test and reference signals. Since the ENF signals are continuous in nature, Short-Term Fourier Transform is (STFT) and a quadratic interpolation is used for the frequency domain analysis. Then a sampling and band pass filtering procedure is applied for the extraction of ENF from both the test and reference.

B. The Absolute-error-map

At the authentication module, we compare the extracted ENF signals. Then we calculate the absolute error between the ENF signals. In this paper, we consider the tampering attacks in time-amplitude domain. So we can observe them in time-frequency domain also. Let M and N are the sample length of reference and test signals, then M>>N. That is, the length of reference signal should be greater than the length of test signal. AEM is proposed after the ENF matching process. AEM is a two-dimensional measurement which contains all local errors between test and reference signals. The AEM can be represented mathematically as two dimensional matrix $\mathbf{of\ the\ order}\ (M-N+1)\times N.ie,$

$$M_{i,j} = |r_{i+j} - s_j| \qquad (3)$$

where *i* and *j* are the indices of element in *M*.

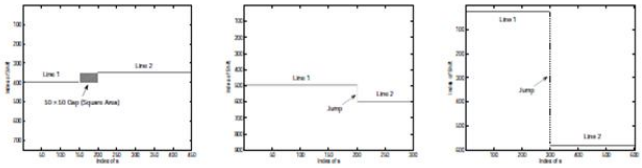


Fig.2. Demonstration graph of Insertion, Deletion and Splicing

C. Authentication based on line detection

By an intensive analysis of the AEM plot, we propose a line detection strategy to identify various types of tampering attacks and location in which the tampering occurred. If the test audio is not tampered, the AEM plot shows a single line. If it is tampered, the AEM plot demonstrates two lines; Line 1 and Line 2. The first exhaustive search algorithm described in [10] is followed here for identifying the tampering attack. The original samples of the ENF will shift into the future time indices by the insertion of a foreign sample. Here, the Line 1 appears before Line2. While on account of deletion the original samples are removed from the ENF sequence. Subsequently the original samples are shifted backward. Here, the Line 2 shows up before Line 1. Two segments are concatenated in the case of splicing. The demonstration graphs for insertion, deletion and splicing are described in Fig.2.

III. RESULTS AND DISCUSSION

Two digital records, record 1 and record 2 in wav format are applied to the proposed audio authentication system. The sampling frequency of the audio records is 44.1 kHz. Authentication of both records is performed under noisy environment. The first record considered here is an audio and second one is an audio extracted from a video record in mp4 format. The noise present in the test recordings is removed using SENLMS filter.

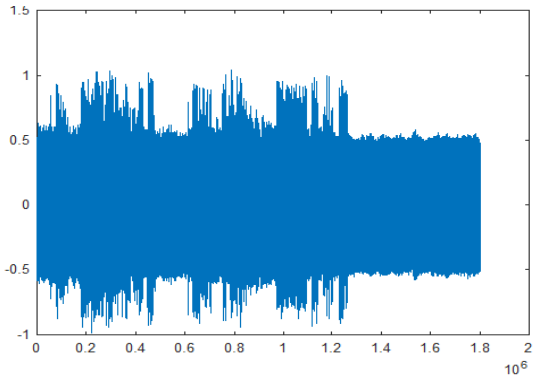
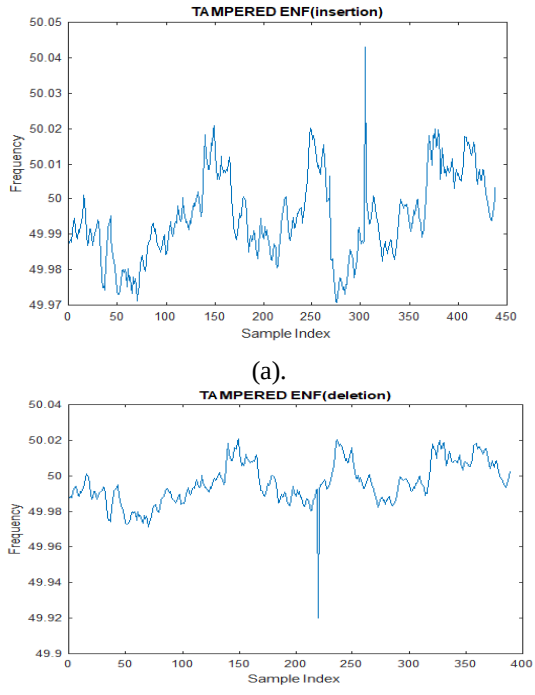


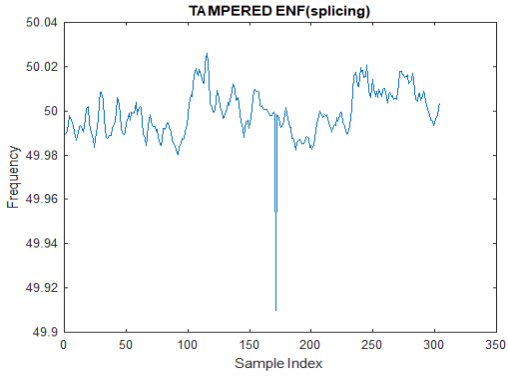
Fig. 3: SENLMS filtered signal

The Fig. 3 shows the filtered signal after noise cancellation using SENLMS filter for an audio record which is not tampered. For both recordings record 1 and record 2, three types of tampering attacks are considered here and they are insertion, deletion and splicing. After the noise cancellation, the next step for ENF extraction is performed.



(a).

(b)



(c)

Fig. 4: Extracted ENF signals for (a). Insertion,(b). Deletion,(c). Splicing

A low pass filter with 60 Hz cut of frequency has designed to remove all values higher than 60 Hz. Then butter worth band pass filter with centre frequency 50 Hz has designed to obtain the power supply frequency of 50 Hz. To analyse the extracted ENF signals in frequency domain STFT is applied. It was then followed by a quadratic interpolation to obtain the maximum power vector. The ENF signals extracted from both records 1 and 2 in case of insertion, deletion and splicing are shown in Fig.4 (a), (b), (c).

For both recordings 1 and 2, insertion is performed at the same location. In the case of insertion, the system identified the type of tampering attack as 'Insertion' at the line length 275. Index of the Line 1 is 390 and that of the Line 2 is 352 for record 1. While the same for record 2 is at 390 and 354. The line index values are used for identifying the type of tampering. Ending index of Line 1 and starting index of Line 2 provides the tampered location and number of samples inserted. The AEM plot for record 1 under insertion attack is shown in Fig. 5.3 (a).

The deletion attack is also considered at the same location of both records. For deletion, the system identified the type of tampering attack as 'Deletion' at line length 219. The index of Line 1 and Line 2 for records 1 and 2 are at 392 and 405. Then the number of samples deleted from the audio segments is calculated using these index values. The AEM plot for deletion attack for record 1 is shown in Fig. 5 (b).

Splicing attack is sometimes a combination of deletion and splicing. Because here a long portion is completely removed from the audio segment and a foreign segment can be joined to the audio segment from the point where original audio samples are deleted.

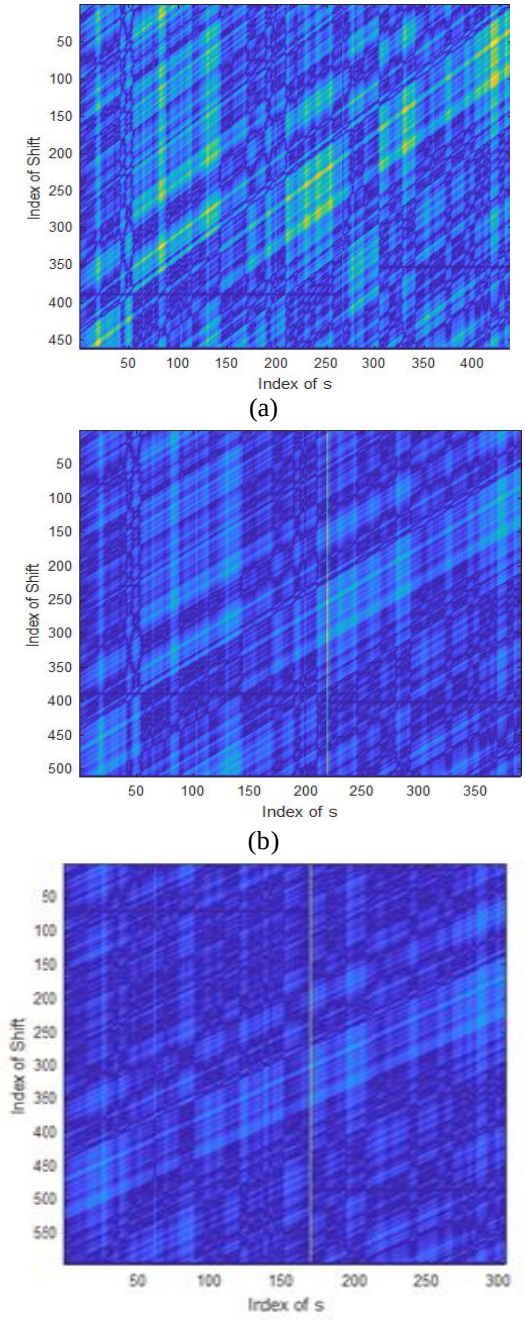


Fig. 5: AEM plots for tampered signals (a). Insertion,(b). Deletion,(c). Splicing

Here, almost 415 samples are deleted from the line length 170 and the portion after deletion from the line length 170 has joined with the segments before this location. Hence there is a large distance between the indices of Line 1 and Line 2 as shown in Fig. 5 (c) with line indices 75 and 490.

IV. CONCLUSION

The proposed system analyses the authentication of a digital record in view of ENF signals. Since the ENF signals are naturally imprinted on a digital record, prior knowledge about the original record is not necessary for authentication purpose. The STFT and quadratic interpolation is used for the estimation of ENF signals. Signed Error Normalized LMS algorithm is then proposed to cancel the noise present in the audio record. The AEM is obtained from an effective ENF matching process. Finally, a line detection method has been proposed to identify the tampering attacks and tampered region. The test results for various types of tampering attacks such as insertion, deletion and splicing are discussed in this paper.

REFERENCES

[1] Mehdi Fallahpour, Shervin Shiramohammadi, " Tampering Detection in Compressed Digital Video Using Watermarking ", IEEE transactions on Instrumentation and measurement,vol.63,no.5,May 2014.

[2] Pradeep K. Atrey, Mohan S. Kanakahalli, "A scalable signature scheme for video authentication", December 2006.

[3] Chin-Chung Hsu, Tzu-Yi Hung, "Video forgery detection using Correlation of Noise-Residue", IEEE Transactions on Information Forensics and Security 2008.

[4] Ruin Yang Zhenhua Qu, "Detecting Digital Audio Forgeries by Checking Frame Offsets", September 22-23, 2008.

[5] Hang Faried, "Detecting Digital Forgeries Using Bi-spectral Analysis", Perceptual Science Group, MIT, Cambridge, MA 02139.

[6] Jiaorong Chen, Shijun Xiang, "Exposing Digital Audio Forgeries in Time Domain by Using Singularity Analysis with Wavelets", June 17-19 2013, Montpellier, France.

[7] Yuming Liu, Zhiyong Yaan, "Application of Power System Frequency for Digital Audio Authentication", IEEE transactions on power delivery, vol.27, no.4, October 2012.

[8] Daniel Patricio Nicolade Rodrignez, "Audio authenticity: Detecting ENF discontinuity with high precision phase analysis", IEEE transactions on Information forensics and Security vol.5, no.3, September 2010.

[9] Zhishebeng Lv1, Yongjian Hu, "Audio forensic Authentication based on MOCC between ENF and reference Signals", IEEE 2013.

[10] Guang Hua, Ying Zhang, Jonathan Goh, Vrizlynn L.L. Thing, "Audio Authentication by Exploring the Absolute-Error-Map of ENF Signals", IEEE Transactions on information forensics Security, vol.2,no.5,May 2016.