

# A Survey on Authentication of Digital Records

Thushara Mathew<sup>1</sup> Subin Kuriakose<sup>2</sup>

<sup>1,2</sup>Department of Electronics & Communication Engineering

<sup>1,2</sup>Mar Baselios Christian College, Peer Made, Idukki, - 685531, India

**Abstract**— The manipulation of the digital record becomes much easier, because of the wide availability of the digital editing tools or software's. The authentication of a digital record is very important in forensic applications. There are different authentication methods proposed to identify various types of tampering attacks occur in a digital record and to determine the location of tampering. Insertion, deletion and splicing are the common types of attacks occur in a digital record. In this paper, we conduct a deep study about various methods that are used for the authentication of digital records such as audio, video etc.

**Key words:** Electric Network Frequency (ENF), Tampering Detection, Digital Forensics

## I. INTRODUCTION

Digital recording is a technology that can be used for recording and reproduction using audio or video signal that have been encoded in digital format. Digital evidence is often attacked for its authenticity due to the ease with which it can be modified, although courts are beginning to reject this argument without proof of tampering. The process of manipulating a digital record is known as tampering. There are different types of tampering attacks such as insertion, deletion, splicing, replacement, shuffling etc. The accurate detection of tampering is a serious problem we are facing today.

There are mainly two types of tampering detection methods. They are active and passive tampering detection. For active tampering detection, side information about the original record is required. While, there is no need of priori-information about the original record for the passive tampering detection. Tampering detection by extracting the watermark or signatures that are embedded in to a digital audio is an effective solution for audio authentication. But the requirement of previous information about the original record is a problem.

One approach to passive audio tampering detection is based on statistical property of noise residue. The tampering detection is achieved by obtaining the noise residue of each frame by subtracting the original frame from its noise free-version. The wavelet de-noising filter is used to obtain the noise-free version. Then the noise residues are correlated to locate the tampered region.

Local noise level is another factor for detecting the tampering in a digital record. In this work, the abnormal difference between the local noise levels in an audio record is calculated. The local noise levels are estimated based on the observation property of an audio signal, Kurtosis consistency. The inconsistencies in the noise levels are used to identify the tampering. This paper mainly deals with splicing attacks.

The electric network frequency (ENF) analysis is a forensic science technique for validating audio recordings by comparing frequency changes in background mains hum in the recording with long term, high precision historical records of mains frequency changes from a database. The nominal

value of ENF varies from 50 to 60 Hz. In this paper, we present several methods used for the audio tampering detection based on ENF signal.

## II. TECHNIQUES FOR DIGITAL RECORD AUTHENTICATION

The Maximum Offset for Cross Correlation (MOCC) between the extracted ENF signals can be used for the authentication of digital records. Here, we determine the offset where cross correlations between extracted ENF signals are maximum. The manipulation makes abrupt changes in the initial phase of the ENF signals. The MOCC is closely related to the ENF phase change. The tampering detection is based on the evaluation of phase consistency for every block of signals. If the phase is consistent for every block of signal, the MOCC would be same. Then the signal is considered as non-tampered. Otherwise it is considered as tampered.

The high precision phase analysis is used for evaluating the ENF phase discontinuity. A high precision Fourier analysis is used to estimate the ENF phase change. The method can be divided into two parts. The first part comprises a visual mechanism that allows the observation of the behaviour of estimated ENF signals. Second part is a discrimination between original and test signal by means of a decision ratio.

The use of spectral distance aims to obtain the information at every time instant or the abrupt changes in the spectrum. The tampering attacks an audio causes spectral discontinuities. These discontinuities forms unnatural peaks in the spectral distances could be sign of an edited signal. The spectral distance is calculated by obtaining coefficient vectors of a linear predictor. First one is obtained from Euclidean distance of two consecutive coefficient vectors and second one is obtained by using an adaptive filter in time reverse order. Two types of spectral distances are calculated. The authentication only by considering the spectral distance is not efficient. So the phase changes of ENF signal also considered in this work.

## REFERENCES

- [1] Guang Hua, Member, IEEE, Ying Zhang, Jonathan Goh, Member, IEEE, and Vrizlynn L. L. Thing, Senior Member, IEEE " Audio Authentication by Exploring the Absolute-Error-Map of ENF Signals" IEEE Trans. Inf. Forensics Security, vol. 2, no. 5, May 2016.
- [2] Chih-Chung Hsu, Tzu-Yi Hung, "Video Forgery Detection Using Correlation of Noise Residue", IEEE Trans. Inf. Forensics Security 2008.
- [3] Xunyu Pan, Xing Zhang and Siwei Lyu, "Detecting splicing in digital audios using local noise level estimation", IEEE 2012.
- [4] Yuming Liu, Student Member, IEEE, Zhiyong Yuan, " Application of Power System Frequency for Digital Audio Authentication ", IEEE transactions on power delivery, vol. 27, no. 4, October 2012.

- [5] Zhisheng Lv1, Yongjian Hu, “Audio forensic authentication based on MOCC between ENF and reference signals”, IEEE 2013.
- [6] D. P. N. Rodríguez, J. A. Apolinário, and L. W. P. Biscainho, “Audio authenticity: Detecting ENF discontinuity with high precision phase analysis,” IEEE Trans. Inf. Forensics Security, vol. 5, no. 3, pp. 534–543, Sep. 2010.
- [7] Daniel Patricio Nicolalde and Jos´e Antonio Apolin´ario Jr, “Evaluating digital audio authenticity with spectral distances and ENF phase change ” IEEE 2009.

