University „POLITEHNICA” of Bucharest
PhD School ETTI-B

Doctoral Thesis
Summary

EXPERTIZA CRIMINALISTICĂ A ÎNREGISTRĂRILOR AUDIO-VIDEO
DETECȚIA EDITĂRILOR DIN ÎNREGISTRĂRI AUDIO

FORENSICS FOR MULTIMEDIA RECORDINGS
AUDIO TAMPERING DETECTION

PhD Student: **As. Ing. Valentin-Adrian Niță**

Doctoral Committee

President	**Prof. PhD. Eng. Gheorghe Brezeanu**	from	**Univ. Politehnica of Bucharest**
PhD Supervisor	**Prof. PhD. Eng. Dumitru Stanomir**	from	**Univ. Politehnica of Bucharest**
Reviewer	**Prof. PhD. Eng. Radu Vasiu**	from	**Univ. Politehnica Timișoara**
Reviewer	**Prof. PhD. Eng. Corneliu Rusu**	from	**Tech. Univ. of Cluj-Napoca**
Reviewer	**Prof. PhD. Eng. Cristian Negrescu**	from	**Univ. Politehnica of Bucharest**

BUCHAREST 2018

Content

Abstract 3

Introduction 4

1.1. Presenting the study field 4

1.2. Objective 5

1.3. PhD Thesis Content 5

State of the art, international standards and audio forensic in Romania 6

2.1. Audio forensic laws in Romania 6

2.2. Multimedia forensic working directions 6

Digital recorder for electric network frequency 8

Passive methods for audio tampering detection 9

4.1 Tampering detection based on the hum noise phase analysis 9

4.1.1. Introduction to hum noise phase analysis 9

4.1.2. Multi harmonic analysis 9

4.2. Audio tampering detection using IFA 10

4.3. Fast but-splice edit detection algorithm 11

4.3. Software application for detecting editing points 11

Anti-tampering audio recordings system 12

Conclusions and future work 14

6.1. Results 14

6.2. Original findings 15

6.3. Original papers 15

Abstract

RO: În prezenta teză de doctorat se urmăresc două direcții de lucru, relativ la domeniul foarte cuprinzător al expertizei criminalistice al înregistrărilor audio: autentificarea unei înregistrări audio și verificarea integrității unei înregistrări audio. Autentificarea unei înregistrări audio se bazează pe principiul variației frecvenței rețelei electrice. Din acest motiv în teză sunt dezvoltate două sisteme de monitorizare a variației frecvenței rețelei electrice. Frecvența rețelei electrice este măsurată cu o precizie mai bună de 0.001 Hz. Existența unei baze de date cu variația frecvenței rețelei electrice va permite identificarea momentului de timp în care a fost realizată o înregistrare afectată de brumul de rețea. În direcția verificării integrității sunt dezvoltate și îmbunătățite două metode ce pot fi folosite pentru a verifica dacă o anumită înregistrare a fost editată. O metodă se bazează pe o analiză de tip multi-armonică a fazei brumului de rețea dintr-o înregistrare iar o a două metodă urmărește apariția artefactelor de tip „butt-splice" dintr-o înregistrare editată. În final este propus un sistem inovativ ce poate permite unei persoane publice să se protejeze de apariția în mass-media a unei înregistrări falsificate cu scopul de a-i denigra imaginea.

EN: In the presented paper we are following two working directions, in contrast with the audio forensic area: audio authentication and audio tampering detection. Audio authentication in this paper is based on the electric network frequency. Because of this, in this thesis are developed two frameworks that can be used to recode the electric network frequency. The electric network frequency is measured with precision better than 0.001 Hz. The existence of a database with the electric network variation will allow us to determine exactly the moment at which a recording has been made. Regarding audio tampering detection there are developed and refined two methods. One method relies on analyzing the phase of the electric network signal for the fundamental component and the harmonics. The second method looks for artifacts called „butt-splice" in an edited audio recording. Finally, an innovative system is proposed for helping a public figure to protect itself from a fake audio recording that can appear in the mass-media.

Chapter 1
Introduction

1.1. Presenting the study field

Due to the development of editing audio applications (like: Adobe Audition, Sound Forge, WavePad, AVS Audio Editor, etc.) these days we can forge very easy audio recordings without having a background in this area. Thanks to a user-friendly interface, the existing applications allows to alter audio recordings by almost any persons with general PC skills. In the presented thesis the broad area of audio forensics is following two working directions: audio authentication and audio tampering detection.

Audio tampering detection is based on looking for specific artifacts that can appear because someone has deleted or added audio fragments in a recording. The artifacts that can appear are: waveform discontinuities [1], double compression artifacts [2], ambient noise [3], reverberation artifacts (like multiple reverberation times found in a recording which normally should have only one reverberation time [4]), artifacts due to multiple microphones used [5] or artifacts found in some residual signals found in the recording, like hum noise (ENF – Electric Network Frequency criterion). We would like to emphasis that these methods are called passive methods because we are not forcing any special conditions to the way the recording has been made. On top of these methods there are also the so called active methods which relay on adding an artificial residual signal, a watermark [6].

When we speak about audio tampering detection we have two possible working directions:

- finding tampering in an audio recording;
- proving that an original recording has not been tampered; it can happen that the accused will say that the presented recording is fake, even if is actual real.

The two problems may seem the same, but this is not the case. If someone alters an audio recording most probably there will be some artifacts that can be found to determine the editing points. The fact that we have not found some specific artifacts it does not prove that a recording is original. Especially if the forger is an experienced one [7].

The second approach must be followed from a different direction. If we want to prove that an original recording has not been altered, we must add a security watermark during the recording time very sensitive to editing. If we find this watermark altered it will mean that the recording is damaged, if we find it unchanged the recording is original. Now we have not found any research during this direction. The presented thesis presents probably the first research in this direction.

1.2. Objective

The objective of the presented thesis is to develop new refined methods for audio forensic in audio authentication and tampering detection.

1.3. PhD Thesis Content

The doctoral thesis is based on 4 chapters:

- Chapter 2 **State of the art, international standards and audio forensic in Romania;**
- Chapter 3 **Digital recorder for electric network frequency;**
- Chapter 4 **Passive methods for audio tampering detection;**
- Chapter 5 **Anti-forging audio recording system.**

The idea presented in Chapter 5 is one of the first research in the area of anti-tampering.

Chapter 2
State of the art, international standards and audio forensic in Romania

The present chapter is presenting the laws that have been ruling in audio forensics, from the first article from 1968 to the present days. Also, we present briefly state of the art methods used in the area of audio authentication and audio tampering detection.

2.1. Audio forensic laws in Romania

The first time when have been introduced laws for audio forensic was in 1968. The way on which an audio recording can be used in the court of law has been reglemented first time in 1996.

Table 2.1 Multimedia forensic statistics in Romania INEC 2013-2016 [8]

Forensic area	**2016**	**2015**	**2014**	**2013**
Speech	12	23	7	9
Image	27	14	10	16
Complex multimedia editing	8	5	7	12
Total	**47**	**43**	**24**	**37**

In Tab. 2.1. we can see the number of multimedia forensic analysis made annually in Romania by INEC.

2.2. Multimedia forensic working directions

In [9] we can identify two analysis methods proposed by a Romanian author:

- **Subjective methods:** based on identifying editing by repeatedly listening the audio recording by a group of persons;
- **Objective methods:** based on using a working station for analyzing the spectrum and comparing with voice models.

If we analyses the services proposed by two forensic laboratories from UK and one from China, we can see a demand in the following directions [10]:

- **Audio expertise**

- Cloning recordings
- Changing compression
- Enhancing intelligibility
- Speaker identification
- Etc.

Video expertise:

- Image enhancement
- Decoding video recordings
- Video camera identification
- Speed estimation
- Etc.

Chapter 3

Digital recorder for electric network frequency

These days any public institution or even private enterprises uses audio-video surveillance systems. From these systems we can have multimedia probes in a court of law. Usually a speech forensic expert must analyze if the recording has been compromised.

In the year 2005, Cătălin Grigoraș presented a very interesting application for the hum noise. The residual noise that normally is so unwanted in the audio recordings. The hum noise is the signal from the electric network, with a fundamental frequency around 50Hz (Europe and Asia) or 60Hz (USA, Japan). This signal has a very special particularity, his main frequency varies in time [11], and these variations are random and unique for a time frame window of around 2-5 minutes. If we record in a database these variations, we can determine the time moment when a recording has been made.

ENF is a very good solution for authenticating an audio recording. The electric network signal has same global variations for a large geographical area [12], but at the same time in [13] the authors have showed that you can find also some micro-variations specific to a smaller geographical area which can be used to determine the recording location. Having a database with the electric network signal may prove to be very useful in a forensic audio analysis.

In 3.1 it is proposed a first version for a framework that uses a special probe and a MATLAB application to create the FRE database. The only problem with this first solution is the cost, the MATLAB license is quite expensive if we want to build a network of ENF databases scattered around an entire country. Because of this in 3.2 is presented a second version based on a Raspberry Pi 2 and a software application developed using Python. In the end it was obtained a system 10 times cheaper with same performances as the first proposed version.

Chapter 4

Passive methods for audio tampering detection

In the present chapter are presented three methods, with good results, for solving the problem of audio integrity check. Due to this methods it has resulted an application developed in MATLAB that can be used to detect tampering in an audio recording.

4.1 Tampering detection based on the hum noise phase analysis

In this section we present a method that analysis the fundamental component and the harmonics of the hum noise captured by an audio recording. This method looks for discontinuities in the phase of the main component and in the harmonics of the electric network signal.

4.1.1. Introduction to hum noise phase analysis

Time authentication can be made by comparing ENF from an ENF database with the hum noise frequency variations from an audio recording. However, as it can be seen in [14] , in order to obtain good results, the analyzed signal should have more than 5 minutes. Because of this, small changes like deleting a word from the recording it will not be noticed by using this principle. We need to look for other artifacts if we want to determine editing points. One idea it can be if we look for phase discontinuity artifacts that can appear due to editing an audio recording.

4.1.2. Multi harmonic analysis

Further on, the analysis will be refined by looking for the harmonics of the hum noise in the silence regions. By analyzing the silence regions from a recording, we can reduce the computational complexity and, we can improve the phase analysis resolution. At the same time, we still stay in line with the way the audio tampering is made, the deletion or insertion of an audio segment in a recording is made in the silence areas usually.

Having in mind the observation above we will start to do a multi harmonic analysis and we will also use a VAD block (VAD – Voice Activity Detection, Fig. 4.1). For the VAD we used the solution presented in [15].

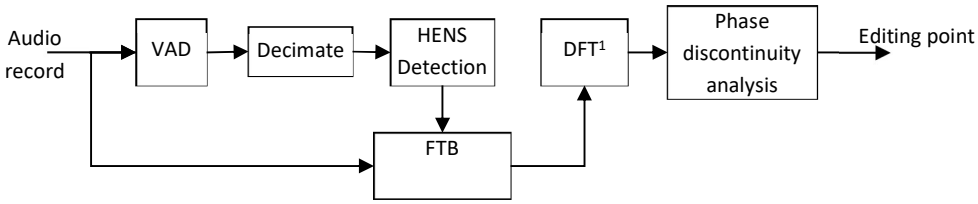

Figure 4.1 *The block diagram of the multi harmonic proposed solution*

An important step of the present method is the block for determining the harmonics from the ENS that can be analyzed. If we do not determine automatically the harmonics that can be analyzed with a good precision, then we will not know to separate a phase estimation error from a phase discontinuity which is due to an editing point.

To analyze the performances of the presented solution we used 72 test signals, sampling rate 8000Hz and each signal has 15s.

Table 4.1 *Results*

Used components	Detection rate [%]	False alarm rate [%]
50 Hz	76.67	1.38
50 Hz, 250 Hz and 350 Hz	44.44	0
At least 2/3	83.33	0

Table 4.1 briefly presents the performances of the presented methods in different circumstance. For all the analyzed signals we used for determining the editing points 3 harmonics (valid harmonics has been placed on 50Hz, 250Hz and 350Hz). If we analyze only the phase for the fundamental component then we will have a detection rate of around 76,67% of situations, and 1,38% false alarm rate. If we enforce that we have found an editing point only if we find phase discontinuity on 3 harmonics hanthetn the detection rate will be 44,44% and we will have a false detection rate of 0%. If we based our decision on finding discontinuity on at least 2 components, then the detection rate will be 83,3% and the false alarm rate will be 0%.

These results have been presented in [16].

4.2. Audio tampering detection using IFA

In this part we still use the same idea of finding editing points in recordings affected by hum noise by analyzing harmonics, but we try to improve the algorithm used for measuring the components phase. For this we use IFA (Instantaneous Frequency Attractors – IFA), which have a good phase analysis precision even for short analyzing fragments [17]. We will try to use a newer criterion for determining the ENS of the hum noise that can be analyzed with good precision.

For determining the performances of the new system, we tested it in different configurations: T1, T2, T3 and on two edited signal databases. T1 is the configuration for the new method, T2 is based on the previous presented configuration and T3 is based on the method presented in [18]. We can see that the new proposed set-up performs slightly better.

Table 4.2 *Performances of the proposed system*

Test type	Signals	Detection rate [%]	Signal type	Signals	Detection rate [%]
T1	FVS	61.2	T1	MVS	73.5
T2	FVS	59.3	T2	MVS	72
T3	FVS	52.8	T3	MVS	—

4.3. Fast but-splice edit detection algorithm

In this subchapter a detailed analysis is made for a method used to look for butt-splice editing points (editing's based on fragment deletion or insertion which have as a result a discontinuity in the signal waveform).

Also, is developed a fast version that can allow to measure hours of recordings in a few minutes.

4.3. Software application for detecting editing points

Based on the methods presented on 4.1, 4.2 and 4.3 a software application that can be used for editing detection has been developed.

Chapter 5
Anti-tampering audio recordings system

The methods presented in the previous chapters, the so called passive methods, are based on some artifacts. This particle artifacts may or may not appear if a person forges an audio recording. For example, if we speak about the Cooper method [1], the butt splice artifacts may appear only if the person that forges the recording does not have too much experience. Also, new editing software, like Adobe Audition, are deleting audio fragments in the zero-crossing region, this way there will not be any discontinuity in the waveform. And, a person that knows about this idea can edit a recording based on the zero-crossing points.

In this chapter, inspired by the ENF criterion [11] and by the live watermarking method presented in [6], an innovative active method used for audio tampering detection is proposed. This method will be the base of our anti-tampering audio recordings system. Moreover, this method will allow us to determine if a recording is also original.

The active method proposed to determine if a recording is tampered or original it is not based on digital processing. This method is based on an analog noise produced by a special designed system found in the recording room. This noise is produced in a way that it will not be noticed by the persons in the room. The recorded person will not be aware of our system.

In a typical audio digital forensic application this method is not to useful. The proposed system is designed to be used by a specific category of users. It can be used by a person who is an important public figure. Our person can use this system in very important meetings. If there is someone that records the meeting, the final product will contain also our noise. Afterward if someone tampers the recording and send it to the mass-media as original the person that used the system will be able to prove that the presented recording is fake.

The performance of our system is analyzed based on the following equation:

$$\text{Precision} = \frac{\text{True detection}}{\text{True detection+Fake detection}}, \qquad (5.6)$$

The performances of the proposed algorithm are presented in Fig. 5.4. The present system can be a very powerful tool for protecting someone against having fake recordings in the mass-media.

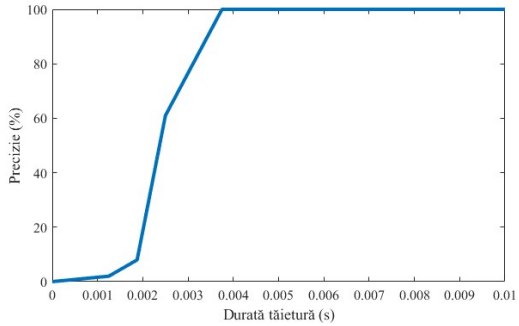

Figure 5.4 Precision based on the editing duration

By looking at the results presented in Fig. 5.4 we can see that the proposed method has 100% precision if the editing is longer than 5ms. If we delete or add a" No" we will have found it.

Chapter 6
Conclusions and future work

The presented paper had as objective the digital audio forensic from the point of view of audio recordings authentication and audio tampering detection.

For authenticating the audio recordings has been used a solution based on the hum noise. Because of these two solutions for creating a ENF and ENS database have been created. A first implementation based on MATLAB and a second version much cheaper based on a Python application, 10 times less.

From the point of view of audio tampering detection there where refined two methods based on hum noise analysis and a third one based on looking for waveform discontinuities. Also, an active method, based on a real time watermarking system has been proposed.

6.1. Results

Chapter 2 presents a synthesis with:

- the laws that have regulated audio forensic from the first draft in 1968 to the last version updated in 2013;
- best practices in an audio forensic laboratory;
- state of the art algorithms for audio tampering detection.

Based on the research presented in Chapter 3 two frameworks for ENF and ENS recoding has been implemented.

The result of the research conducted in Chapter 4 is represented by a software application that can be used to look for tampering in an audio recording. The application is based on two different methods, one based on the hum noise and another that looks for waveform discontinuities in a recording.

Chapter 5 presents the real novelty of the presented thesis, an innovative active method based on an analog audio watermark which can be used to certify that a recording is original.

6.2. Original findings

1. A synthetic study about state of the art methods, standards and algorithms used for audio forensic
2. Design of two hardware/software solution for obtaining a ENF and ENS database [C1, C6].
3. Developing two hardware/software solution for obtaining a ENF and ENS database [C1, C6].
4. A new algorithm for authenticating audio recordings based on hum noise [R1, R2, C3].
5. A software application for finding editing points in an audio recording [R1, R2, C3, C5].
6. A database with audio recordings, affected by hum noise, edited and original, which can be used to determine the performances of audio tampering detection algorithms based on hum noise [R1, R3].
7. A fast algorithm for detecting 'butt-splice' edits [C5].
8. MATLAB implementation of an algorithm for detecting 'butt-splice' edits [C5].
9. A database with 'butt-splice' audio edits [C5].
10. A new innovative method for certifying that an audio recording is 100% original starting from the ideas in [C7, C8] and presented in C9.

6.3. Original papers

Projects

Project Innovation Checks type, contract no. 47CI/2017 (PN-III-P2-2.1-CI-2017-0362), title „Software application for fencing video refereeing" – project manager from **UPB**

ISI Magazines

R1. NIȚĂ, V. A., CIOBANU, A., DOBRE, R. A., NEGRESCU, C., STANOMIR, D., & PREDA, R. O. ENF PHASE DISCONTINUITY DETECTION BASED ON MULTI-HARMONICS ANALYSIS, Scientific Bulletin, Series C, Vol. 4/2015

R2. AMELIA CIOBANU, **VALENTIN A. NIȚĂ**, CRISTIAN NEGRESCU, DUMITRU STANOMIR, IMPROVED AUDIO EDIT DETECTION USING THE PHASE ANALYSIS OF THE HARMONICS OF THE ELECTRIC NETWORK SIGNAL, Revue roumaine des sciences techniques, Série Électrotechnique et Énergétique, Vol. 4/2016, pp. 394-397

ISI Conferences

C1. **V.A. Niță**, R. A. Dobre, A. Drumea, A. Ciobanu, C. Negrescu, D. Stanomir, ”Electrical network signal's waveform and frequency logging for forensic”, ATEE 2015, Bucharest, 7-9 May 2015, pp.156 - 161, DOI 10.1109/ATEE.2015.7133756, INSPEC 15240878.

C2. R. A. Dobre, V.A. **Niță**, A. Ciobanu, C. Negrescu, D. Stanomir, ”A Hum Removal Algorithm Used for Audio Restoration Purposes”, ISSCS 2015, Iaşi, 9-10 July 2015, pp. 1-4 (ISBN 978-1-4799-3193-4), DOI 10.1109/ISSCS.2015.7204000, INSPEC 15382519.

C3. A. Ciobanu, C. Negrescu, **V.A. Niță**, R. A. Dobre, D. Stanomir, ”HIGH ACCURACY FREQUENCY ANALYSIS USING INSTANTANEOUS FREQUENCY ATTRACTORS”, proceedings of Eusipco 2015, 31 Aug. – 4. Sept. 2015, Nisa, pp. 565 – 568

C4. R. A. Dobre, **V.A. Niță**, A. Ciobanu, C. Negrescu, D. Stanomir, ”Low Computational Method for Siren Detection”, SIITME 2015, Brașov, 22-25 Oct. 2015, pp. 291 - 295, DOI 10.1109/SIITME.2015.7342342.

C5. **V.A. Niță**, A. Ciobanu, C. Negrescu, D. Stanomir , ”Fast algorithm for detecting butt-spliced edits”, ISETC 2016, Timisoara , Oct. 2016, DOI: 10.1109/ISETC.2016.7781109

C6. **V.A. Niță**, A. Ciobanu, C. Negrescu, D. Stanomir, ” Low cost electric network signal and frequency recorder”, ATEE 2017, Bucharest, 23-25 March 2017, DOI 10.1109/ATEE.2017.7905094, INSPEC 16836130.

C7. R. A. Dobre, **V.A. Niță**, S. Ciochină, C. Paleologu ”New Insights on the Convergence Analysis of the Affine Projection Algorithm for System Identification”, ISSCS 2015, Iaşi, 9-10 July 2015, pp. 1-4 (ISBN 978-1-4673-7488-0), DOI: 10.1109/ISSCS.2015.7203988, INSPEC 15382533.

C8. **V.A. Niță**, R. A. Dobre, S. Ciochină, C. Paleologu ” Improved Convergence Model of the Affine Projection Algorithm for System Identification”, presented at ISSCS 2017, Iaşi, 13-14 July 2017.

C9. **V.A. Niță**, A. Ciobanu ”TIC-TAC, FORGERY TIME HAS RUN-UP! LIVE ACOUSTIC WATERMARKING FOR INTEGRITY CHECK IN FORENSIC APPLICATIONS”, presented at ICASSP 2018, Calgary, 15-20 April 2018.

6.4. Future work

From our point of view the most important future perspective is represented by the active methods that can be used to find editing points. The passive methods are at an important maturity point. This active method can help someone against fake recordings, that can be used to damage the public image.

Based on the active methods results, two applications can be developed:

- A watch with a tic-tac sound desynchronized with around ±25 ms, this variation will not be noticed by a person that is recorded and can follow a specific template

which, if someone edits a recording, will be found changed, proving that a recording has been altered;

- A software application that introduces our watermark used by the active method; if someone records the phone conversation and then alters the content, the person that has the personal image damaged will be able to prove that the recording is actual fake.

Another important perspective is represented by the method presented in Chapter 3. The cheap system proposed in the second part, for recording the ENF, may be used to develop a national array of ENF databases which can be used to determine also the recording location.

Selective Bibliography

[1] A. Cooper, "Detecting butt-spliced edits in forensic digital audio recordings," in *Proc. Audio Eng. Soc. 39th Conf., Audio Forensics: Practices and Challenges*, Hillerod, 2010.

[2] D. Luo, R. Yang and J. Huang, "Detecting double compressed AMR audio using deep learning," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Florence, 2014.

[3] S. P. Mohanapriya, E. P. Sumesh and R. Karthika, "Environmental sound recognition using Gaussian mixture model and neural network classifier," in *International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE)*, Coimbatore, 2014.

[4] A. Ciobanu, T. Culda, C. Negrescu and D. Stanomir, "Analysis of reverberation time blind estimation used in audio forensics," in *11th International Symposium on Electronics and Telecommunications (ISETC)*, Timisoara, 2014 .

[5] Ö. Eskidere and A. Karatutlu, "Source microphone identification using multitaper MFCC features," in *9th International Conference on Electrical and Electronics Engineering (ELECO)*, Bursa, 2015.

[6] R. Tachibana, "Sonic Watermarking," *EURASIP Journal on Applied Signal Processing,* vol. 13, p. 1955–1964, 2004.

[7] W.-H. Chuang, R. Garg and M. Wu, "Anti-forensics and countermeasures of electrical network frequency analysis," *IEEE Trans. Inf. Forensics Security,* vol. 8, no. 12, pp. 2073-2086, 2013.

[8] INEC, "Rapoarte si Studii," [Online]. Available: http://www.inec.ro/index.php/prezentare/rapoarte-si-studii. [Accessed 26 July 2017].

[9] I. Anghelescu, Expertiza Criminalistică a Vocii și Vorbirii, București: Editura Științifică și Enciclopedică, 1978.

[10] A. T. Ho and S. Li, Handbook of Digital Forensic of Multimedia Data and Devices, John Wiley & Sons, 2015.

[11] C. Grigoraș, "Digital audio recording analysis: the Electric Network Frequency (ENF) criterion," *The International Journal of Speech Language and the Law,* vol. 12, no. 1, pp. 63-76, 2005.

[12] C. Grigoraș, "Application of ENF analysis in forensic authenticity of digital audio," *Journal of the Audio Engineering Society,* vol. 57, no. 9, p. 643–661, 2009.

[13] A. Hajj-Ahmad, R. Garg and M. Wu, "ENF-based region-of-recording identification for media signals," *IEEE Trans. Inf. Forensics Security,* vol. 10, no. 6, p. 1125–1136, 2015.

[14] M. Huijbregtse and Z. Geradts, "Using the ENF criterion for determining the time of recording of short digital audio recordings," *Third International Workshop, IWCF, Proceedings,* vol. 1, pp. 116-124, 2009.

[15] J. Sohn, N. S. Kim and W. Sung, "A statistical model-based voice activity detection," *IEEE Signal Processing Letters,* vol. 6, no. 1, pp. 1-3, 1999.

[16] V. Nita, A. Ciobanu, R. Dobre, C. Negrescu, D. Stanomir and R. O. Preda, "ENF phase discontinuity detection based on multiharmonic analysis," *Scientific Bulletin of the University Politehnica of Bucharest, Series C: Electrical Engineering and Computer Science,* vol. 77, no. 4, pp. 199-212, 2015.

[17] A. Ciobanu, C. Negrescu, V. A. Niță, R. A. Dobre and D. Stanomir, "High accuracy frequency analysis using instantaneous frequency attractors," in *23rd European Signal Processing Conference (EUSIPCO)*, Nice, 2015.

[18] D. Rodriguez, J. Apolinario and L. Biscainho, "Audio Authenticity Based on the Discontinuity of ENF Higher Harmonics," in *Proc. EUSIPCO*, 2013.

[19] J. Chai, Z. Y. L. Y, R. W. Conners and Y. Liu, "Tampering detection of digital recordings using electric network frequency and phase angle," *Audio Engineering Society Convention 135,* 2013.

[20] M. M. Elmesalawy and M. M. Eissa, "New forensic ENF reference database for media recording authentication based on harmony search technique using GIS and wide area frequency measurements," *IEEE Trans. Inf. Forensics Security,* vol. 9, no. 4, pp. 633-644, 2014.

[21] V. A. Niţă, R. A. Dobre, A. Drumea, A. Ciobanu, C. Negrescu and D. Stanomir, "Electrical network signal's waveform and frequency logging for forensic," in *Advanced Topics in Electrical Engineering (ATEE), 2015 9th International Symposium*, Bucharest, 2015.

[22] V. A. Niţă, A. Ciobanu, C. Negrescu and D. Stanomir, "Low cost electric network signal and frequency recorder," in *Advanced Topics in Electrical Engineering (ATEE), 2017 10th International Symposium*, Bucharest, 2017.

[23] A. Petre and C. Grigoraș, Înregistrările audio și audio-video, București: C.H. Beck, 2010.

[24] INEC, "Expetize," [Online]. Available: http://www.inec.ro/index.php/activitate/expertize. [Accessed 25 July 2017].

[25] M. Justiției, "Tabelul nominal cu expertii criminalisti autorizati," Ministerul Justiției, [Online]. Available: http://www.just.ro/profesii-conexe/tabelul-nominal-cu-expertii-criminalisti-autorizati/. [Accessed 25 July 2017].

[26] V. Niță and A. Ciobanu, "TIC-TAC, FORGERY TIME HAS RUN-UP! LIVE ACOUSTIC WATERMARKING FOR INTEGRITY CHECK IN FORENSIC APPLICATIONS," in *ICASSP*, Calgary, 2018.