



**UNIVERSITATEA „POLITEHNICA” din BUCUREȘTI**

**ȘCOALA DOCTORALĂ ETTI-B**

# **TEZĂ DE DOCTORAT**

## **Rezumat**

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

**FORENSICS FOR MULTIMEDIA RECORDINGS  
AUDIO TAMPERING DETECTION**

**Doctorand: As. Ing. Valentin-Adrian Niță**  
**COMISIA DE DOCTORAT**

Președinte	<b>Prof. Dr. Ing. Gheorghe Brezeanu</b>	de la	<b>Univ. Politehnica București</b>
Conducător de doctorat	<b>Prof. Dr. Ing. Dumitru Stanomir</b>	de la	<b>Univ. Politehnica București</b>
Referent	<b>Prof. Dr. Ing. Radu Vasiu</b>	de la	<b>Univ. Politehnica Timișoara</b>
Referent	<b>Prof. Dr. Ing. Corneliu Rusu</b>	de la	<b>Univ. Tehnică Cluj-Napoca</b>
Referent	<b>Prof. Dr. Ing. Cristian Negrescu</b>	de la	<b>Univ. Politehnica București</b>

**BUCUREȘTI 2018**

---

# Cuprins

Abstract.....	3
Introducere .....	4
1.1.    Prezentarea domeniului tezei de doctorat .....	4
1.2.    Scopul tezei de doctorat .....	5
1.3.    Conținutul tezei de doctorat.....	6
Bune practici, standarde internaționale și expertiza criminalistică a înregistrărilor multimedia în România.....	8
2.1. Cadrul legal pentru expertiza criminalistică a înregistrărilor multimedia în România ...	8
2.2. Bune practici, standarde și metode moderne pentru expertiza criminalistică a înregistrărilor multimedia.....	9
Recorder digital pentru frecvența rețelei electrice .....	11
Metode pasive pentru detecția editărilor din înregistrări audio .....	13
4.1 Detecția editărilor din înregistrări audio pe baza saltului de fază în semnalul rețelei electrice.....	13
4.1.1. Noțiuni introductive relativ la detecția editărilor pe baza saltului de fază SRE.....	13
4.1.2. Analiza multi-armonică .....	13
4.2. Detecția editărilor audio pe baza FRE cu ajutorul IFA .....	15
4.3. Algoritm rapid pentru detectarea editărilor de tip butt-splice .....	16
4.3.    Aplicație software pentru detectare editărilor din înregistrări audio .....	16
Sistem de protecție împotriva falsificărilor înregistrărilor audio.....	17
Concluzii generale și perspective.....	19
6.1. Rezultate obținute .....	19
6.2. Contribuții originale .....	20
6.3. Lista lucrărilor originale .....	21
Bibliografie selectivă .....	23

# 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 doua 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 record 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.

# Capitolul 1

## Introducere

### 1.1. Prezentarea domeniului tezei de doctorat

Datorită dezvoltării aplicațiilor de editare audio (câteva exemple: Adobe Audition, Sound Forge, WavePad, AVS Audio Editor, etc.) în zilele noastre se pot falsifica foarte ușor înregistrări audio cu un minim de cunoștințe tehnice. Mulțumită interfeței grafice intuitive aplicațiile existente pot fi folosite doar pe baza unor cunoștințe de operare a calculatorului generale. Expertiza criminalistică a înregistrărilor audio privește două direcții de lucru: verificarea autenticității unei înregistrări audio (determinarea momentului de timp la care a fost făcută o înregistrare [1], contextul în care a fost făcută înregistrarea, subiectul A ar fi putut auzi ce vorbea subiectul B dintr-o scenă audio, și identificarea echipamentului cu care a fost făcută o anumită înregistrare [2]) și verificarea integrității unei înregistrări audio [3] (această idee presupune verificarea dacă o înregistrare audio particulară a fost editată, cu scopul de a altera informația din înregistrarea originală, sau nu).

Verificarea integrității unei înregistrări audio presupune căutarea anumitor artefacte ce pot să apară din cauza unui anumit model de editare de tipul adăugare fragmente audio sau ștergere fragmente audio. Artefactele ce pot să apară sunt: discontinuități în semnalul înregistrat [4], artefacte specifice compresiei duble [5], artefacte în zgomotul de fundal [6], artefacte în reverberația încăperii în care fost făcută înregistrarea, și care a fost captată prin intermediul înregistrării pe baza reflexiilor undelor sonore din încăperea [7], artefacte în neliniaritățile datorate microfoanelor folosite pentru înregistrare [2] sau anumite artefacte în diverse semnale reziduale, ce pot să apară într-o înregistrare, cum ar fi brumul de rețea (Criteriul FRE – Frecvența rețelei electrice sau ENF – Electric Network Frequency). De menționat că aceste metode se mai numesc și metode pasive deoarece nu presupun vreo modalitate specială în care să fie făcută o anumită înregistrare audio. În plus, față de metodele prezentate mai sus, există și așa numitele metode active, acestea presupun integrarea unui semnal rezidual într-o înregistrare audio, în momentul în care aceasta este făcută, metode de tip watermarking [8].

Atunci când vorbim de verificarea integrității unei înregistrări audio există două

paradigme ce pot/trebuie să fie abordate:

- găsirea urmelor de editare dintr-o înregistrare falsificată, această problemă poate fi rezolvată cu ajutorul metodelor pasive prezentate mai sus;
- demonstrarea că o înregistrare audio, nefalsificată, este originală; se poate întâmpla ca o probă audio să fie contestată de către inculpat, acesta poate să pretindă că nu el este persoana care vorbește în înregistrare sau să pretindă că înregistrarea a fost falsificată și i-a fost alternat conținutul cu scopul de a-l incrimina chiar dacă el este „nevinovat”.

Deși problemele par identice, ele au mici diferențe ce le fac separabile, deoarece e adevărat că dacă în urma unei falsificări a unei înregistrări audio apar anumite artefacte specifice aceste vor fi detectate de metodele pasive prezentate mai sus. Însă, dacă aceste artefacte nu au fost găsite de niciuna din metodele menționate anterior nu certifică în realitate faptul că o anumită înregistrare nu a fost editată. Acest lucru certifică faptul că nu a fost găsit niciun artefact specific unei editări audio, dintre cele căutate. Mai ales că o persoană specializată în falsificări de înregistrări audio poate să ascundă anumite artefacte [9].

Cea de-a doua paradigmă trebuie abordată din alt punct de vedere. Dacă vrem să certificăm cu adevărat că o înregistrare nu a fost editată, fără a avea niciun dubiu, trebuie să folosim așa numitele metode active. Aceste metode presupun adăugarea unui watermark special, în momentul înregistrării, ce va fi alterat în cazul în care o înregistrare este falsificată, în caz contrar acest watermark va fi găsit intact. În principiu în literatura de specialitate nu există studii în această direcție. Cel puțin după cunoștințele noastre până în acest moment, iar capitolul 5 din această lucrare este una din primele cercetări în această direcție.

## **1.2. Scopul tezei de doctorat**

Scopul prezentei teze de doctorat îl constituie dezvoltarea de metode noi sau îmbunătățite pentru expertiza criminalistică a înregistrărilor audio prin autentificarea acestora și verificarea integrității.

Autentificarea unei înregistrări audio urmărește metodele bazate pe brumul de rețea, ce poate să apară în anumite înregistrări audio. Brum de rețea a cărui frecvență fundamentală prezintă variații unice în timp, în marea majoritate a timpului în intervalul  $\pm 0.1$  Hz. Pentru aceasta se urmărește dezvoltarea unui sistem hardware și software ce poate crea o bază de date cu aceste variații temporale, folosită ulterior ca referință

pentru a determina momentul de timp la care o înregistrare audio, afectată de brumul de rețea, a fost realizată [10]. Mai nou o astfel de bază de date poate fi folosită pentru a identifica chiar și zona geografică în care o înregistrare a fost realizată [11]. Din acest motiv în această lucrare este prezentată o variantă cu costuri reduse ce poate fi folosită pentru a crea o rețea de baze de date FRE pe teritoriul României (aproximativ 400 de baze de date locale) [12].

### **1.3. Conținutul tezei de doctorat**

Teza de doctorat se bazează pe patru capitole:

- Capitolul 2 **Bune practici, standarde internaționale și expertiza criminalistică a înregistrărilor multimedia în România;**
- Capitolul 3 **Recorder digital pentru frecvența rețelei electrice;**
- Capitolul 4 **Metode pasive pentru detecția editărilor din înregistrări audio;**
- Capitolul 5 **Sistem de protecție împotriva falsificărilor înregistrărilor audio.**

În Capitolul 2 sunt prezentate într-o primă fază legile ce au stat la baza expertizei criminalistice a înregistrărilor audio video în România, de la Codului Penal din 21 iulie 1968 (în care practic aceste lucruri nu erau reglementate, deși în timpul regimului comunist astfel de probe erau des folosite) până la NCPP - actualizat prin Legea nr. 255/2013 - pentru punerea în aplicare a Legii nr. 135/2010 privind Codul de procedură penală și pentru modificarea și completarea unor acte normative care cuprind dispoziții procesual penale din 19 iulie 2013, M. Of. 515/2013 (în care sunt specificate în detaliu procedurile ce pot fi folosite pentru a obține înregistrări multimedia ce pot fi acceptate într-o instanță judecătorească și modul în care acestea pot fi arhivate și sigilate).

În a doua parte a Capitolului 2 sunt prezentate: principalele standarde internaționale ce pot fi folosite pentru buna funcționare a unui laborator de expertiză criminalistică și metode și algoritmi moderni din literatura de specialitate (ce pot fi folosiți pentru a autentifica și a verifica integritatea unei înregistrări audio).

În Capitolul 3 sunt prezentate două sisteme hardware și software pentru crearea unei baze de date cu FRE și SRE în vederea autentificării temporale a înregistrărilor audio afectate de brumul de rețea.

Capitolul 4 urmărește rezolvarea problemei de găsimă a punctelor de editare din înregistrări audio afectate de editări de tip adăugare și ștergere secvențe audio. Pentru a rezolva această problemă sunt propuse două metode principale, o metodă bazată pe discontinuități de fază în armonicile SRE, ce apar dacă o înregistrare este falsificată și

o metodă ce caută discontinuități în forma de undă a semnalului analizat. Această metodă găsește foarte repede salturile de fază din semnal dar are dezavantajul că aceste salturi pot să nu apară în mod natural într-un semnal editat, mai ales din cauza noilor programe de editare audio ce pot fi folosite (care realizează adăugarea și ștergerea de segmente audio din înregistrări în punctele de trecere prin zero astfel încât să nu existe un salt de fază în punctele de editare sau chiar pot fi evitate deliberat de către persoana care realizează editarea, dacă aceasta are minime cunoștințe despre falsificarea înregistrărilor audio).

În capitolul 5 este introdusă o metodă inovativă de verificare a integrității înregistrărilor audio. Este de menționat faptul că problematica verificării integrității înregistrărilor audio este privită dintr-un punct de vedere nou în acest capitol; se dorește să se realizeze un sistem de protecție împotriva calomniei digitale. Prin urmare se propune o metodă activă ce se bazează pe amprentarea digitală a înregistrărilor audio cu o amprentă ce nu poate fi ștearsă. Persoanele care folosesc acest sistem vor putea să dovedească ușor că o înregistrare falsificată cu scopul de a le denatura imaginea publică a fost falsificată. Dacă amprenta este originală atunci și înregistrarea va fi certificată ca fiind originală cu un coeficient de încredere de 100% pentru posibile editări cu o durată mai mare de 5 ms.

Ultimul capitol este dedicat prezentării concluziilor desprinse în urma studiilor efectuate și a evaluărilor subiective și obiective realizate pe parcursul întregii lucrări.

# Capitolul 2

## Bune practici, standarde internaționale și expertiza criminalistică a înregistrărilor multimedia în România

Prezentul capitol are rolul de a scoate în evidență exigențele cerute de Codul de procedură penală din România relativ la expertiza criminalistică a înregistrărilor multimedia. Sunt sintetizate referințe și bune practici conform cu standardele internaționale și modul de lucru a unor laboratoare consacrate pentru a putea cuantifica din punct de vedere comparativ rezultatele metodelor propuse pentru expertiză în capitolele următoare.

### 2.1. Cadrul legal pentru expertiza criminalistică a înregistrărilor multimedia în România

Cadrul legal pentru obținerea de înregistrări multimedia ce pot fi folosite ca probe într-o instanță judecătorească în România este reglementat conform Codului Penal din 21 iulie 1968, ulterior republicat și actualizat.

Relativ la înregistrările multimedia ce pot fi folosite ca probe într-o instanță judecătorească în România primele legi importante au fost adăugate abia în 1996, prin Legea nr. 141/1996 (Monitorul Oficial nr. 289 din 14 noiembrie 1996) [13], pe baza căreia s-a introdus o nouă secțiune (**Secțiunea V - Titlul III, capitolul II**) intitulată „Înregistrările audio sau video”.

În prezent se află în vigoare Noul Cod de Procedură Penală (NCPP - actualizat prin Legea nr. 255/2013 - pentru punerea în aplicare a Legii nr. 135/2010 privind Codul de procedură penală și pentru modificarea și completarea unor acte normative care cuprind dispoziții procesual penale din 19 iulie 2013, M. Of. 515/2013), iar expertiza criminalistică a înregistrărilor multimedia este reglementată prin articolele: 138-153 (**CAPITOLUL IV - Metode speciale de supraveghere sau cercetare**).

În NCPP este de remarcat că sunt specificate în detaliu procedurile care pot fi folosite pentru a obține înregistrări multimedia ce pot fi acceptate într-o instanță judecătorească și modul în care acestea pot fi arhivate și sigilate, însă în continuare nu



sunt definite condițiile în care o expertiză criminalistică a înregistrărilor multimedia este considerată validă. De avut în vedere totuși faptul că INEC (Institutul Național de Expertize Criminalistice) efectuează expertize „numai asupra înregistrărilor originale sau duplicate (copii fidele) ale înregistrărilor originale eliberate și certificate de autoritățile care le-au realizat, cu condiția ca duplicatele să fie admise de organul judiciar care a dispus expertiza” [14].

„Expertiza vocii și a vorbirii” și „Expertiza fotografiilor și a imaginilor video” poate fi realizată de un expert criminalist autorizat de către Ministerul Justiției, listă ce este actualizată anual și poate fi disponibilă la [15].

*Tabelul 2.1 Statistici expertize multimedia INEC 2013-2016 [16]*

Specialități de expertiză	2016	2015	2014	2013
<b>Vocii și Vorbirii</b>	12	23	7	9
<b>Imaginilor</b>	27	14	10	16
<b>A altor urme (Audio+Audio Video) sau complexe</b>	8	5	7	12
<b>Total</b>	<b>47</b>	<b>43</b>	<b>24</b>	<b>37</b>

În Tab. 2.1. se pot vedea numărul de expertize multimedia efectuate anual de către INEC. De remarcat că trendul necesității expertizelor multimedia este crescător.

## **2.2. Bune practici, standarde și metode moderne pentru expertiza criminalistică a înregistrărilor multimedia**

Deși în perioada comunistă se efectuau foarte multe urmăriri și interceptări pe bază de probe audio, Codul Penal nu reglementa modul în care aceste probe pot fi prelevate, arhivate și utilizate într-o instanță judecătorească. Cu toate acestea o primă analiză a expertizei criminalistice a vocii și vorbirii în România este prezentată în [17] prin care sunt identificate din start două metode de analiză:

- **Metode subiective:** prin care identificarea unei persoane se realizează pe bază de ascultări repetate de către un grup de persoane, sau transcrierea vocii este realizată cu ajutorul unui sonograf și examinarea unui expert;

- **Metode obiective:** cu un caracter științific mai pronunțat aceste metode se bazează pe folosirea „calculatorului electronic” care presupunea analiza unei spectrograme a vorbirii și a unor modele de voce.

În zilele noastre lucrurile s-au dezvoltat foarte mult în domeniul expertizei criminalistice a înregistrărilor multimedia, în mod special datorită revoluției digitale care presupune accesul facil atât la echipamente de înregistrare audio sau video cât și la softuri de prelucrare care pot fi folosite pentru a falsifica o înregistrare multimedia. Dacă analizăm serviciile oferite de 2 mari laboratoare din UK, unul din China și INEC, din România, se poate observa o cerere clară pentru următoarele servicii [18]:

➤ **Expertize audio**

- Duplicare înregistrări
- Conversie format codare
- Îmbunătățirea inteligibilității
- Înlăturarea sau cenzurarea anumitor pasaje dintr-o înregistrare
- Deghizarea anumitor voci, pentru persoanele care ar trebui să aibă identitatea secretă
- Autentificarea unei înregistrări audio – verificarea dacă o înregistrare a fost editată prin adăugare sau înlăturare de pasaje
- Determinarea momentului de timp la care a fost efectuată înregistrarea sau chiar locul în care a fost efectuată înregistrarea
- Evaluarea acustică a scenei crimei - o anumită persoană ar fi putut auzi un anumit semnal sonor?
- Identificarea vorbitorului

➤ **Expertize video:**

- Suport pentru vizionarea anumitor înregistrări video codate în formate specifice anumitor DVR-uri
- Decodarea și conversia formatelor anumitor înregistrări video
- Descărcarea înregistrărilor dintr-un dispozitiv de înregistrat
- Identificarea camerei cu care a fost obținută o anumită înregistrare
- Îmbunătățirea calității imaginii
- Estimarea vitezei de deplasare a anumitor obiecte dintr-o înregistrare video

# Capitolul 3

## Recorder digital pentru frecvența rețelei electrice

În ziua de azi aproape orice instituție publică sau chiar diverse sedii sau magazine ale instituțiilor private folosesc sisteme de supraveghere audio-video, ale căror înregistrări pot ajunge ca probe într-o instanță judecătorească. Însă, întotdeauna se pune problema autentificării. De regulă un expert criminalist autorizat de către ministerul justiției pentru expertiza vocii și a vorbirii trebuie să verifice dacă înregistrarea a fost compromisă.

La mijlocul anilor 2000, Cătălin Grigoraș a găsit o utilitate interesantă pentru brumul de rețea. Acel semnal rezidual (nedorit în aplicațiile audio profesionale) de tip sinus, cu frecvența variind ușor în jurul valorii de 50 Hz (Europa, Asia) sau 60 Hz (America, Japonia), care apărea la vremea respectivă în majoritatea înregistrărilor audio digitale, fie din cauza surselor de alimentare folosite, fie din cauza câmpurilor electromagnetice ce pot apărea într-o încăpere. Analizând în detaliu variațiile frecvenței rețelei [1] s-a observat că aceste variații pot fi apreciate ca fiind aleatoare, iar relativ la o durată de 2-5 minute, aceste variații se pot considera unic definite în timp. Prin urmare, dacă avem la dispoziție o bază de date cu variațiile frecvenței rețelei în timp, putem determina ora la care o anumită înregistrare audio a fost efectuată.

FRE este o soluție foarte bună pentru a determina autenticitatea unei înregistrări. Semnalul rețelei electrice, înregistrat în același timp cu semnalul audio util, prezintă variații similare pentru regiuni geografice mari [19], dar în același timp în [20] autorii au demonstrat că există micro variații specifice unei arii geografice mai limitate, idee pe baza căreia se poate autentifica chiar și zona în care a fost făcută o anumită înregistrare. Având în vedere aceste considerente o bază de date în care este stocată FRE și semnalul rețelei electrice în România, sub autoritatea unei instituții publice autonome și obiective (Universitatea Politehnica din București) se poate dovedi deosebit de utilă pentru situațiile în care este necesară expertiza vocii și a vorbirii de către o a treia entitate, cu rol de etalon.

În subcapitolul 3.1 propunem o primă variantă de recorder FRE ce are ca suport software mediul Matlab. Deși rezultatele sunt promițătoare și acest dispozitiv de înregistrare poate fi folosit foarte ușor cu ajutorul interfeței grafice dezvoltate, acesta prezintă costuri destul de ridicate, în principiu un calculator și o licență Matlab. Aceste costuri sunt relativ mici atunci când vorbim de un singur recorder, însă destul de mari dacă vrem să instalăm 100-200 de dispozitive înregistrare, împrăștiate pe teritoriul României, pentru a asigura redundanță în obținerea informațiilor dorite și pentru a putea să autentificăm nu numai momentul înregistrării, ci și locul înregistrării, cel puțin pe o rază de aproximativ 50 km. Din acest motiv în subcapitolul 3.2, plecând de la soluția hardware propusă în subcapitolul 3.1, este dezvoltat un dispozitiv pentru înregistrare FRE cu un cost mult mai scăzut, prețul unei plăcuțe Raspberry Pi 2 și un card micro-sd de 64 Gb, pentru a putea stoca informația dorită, FRE și semnalul rețelei electrice, pentru aproximativ 1 an.

# Capitolul 4

## Metode pasive pentru detecția editărilor din înregistrări audio

În capitolul curent sunt prezentate trei metode, ce prezintă rezultate bune, pentru rezolvarea uneia din cele două paradigme ale detecției editărilor audio, și anume detecția urmelor de editare din înregistrările audio editate și o aplicație software, dezvoltată în Matlab, pentru detecția editărilor din înregistrări audio.

### 4.1 Detecția editărilor din înregistrări audio pe baza saltului de fază în semnalul rețelei electrice

În cadrul acestei secțiuni este prezentată o metodă multi-armonică de detecție a discontinuităților de fază a frecvenței rețelei electrice (FRE), ce poate fi utilizată pentru detectarea posibilelor puncte de editare din înregistrări audio. Această metodă presupune căutarea de discontinuități atât în faza fundamentalei SRE cât și în faza armonicilor superioare ale SRE.

#### 4.1.1. Noțiuni introductive relativ la detecția editărilor pe baza saltului de fază SRE

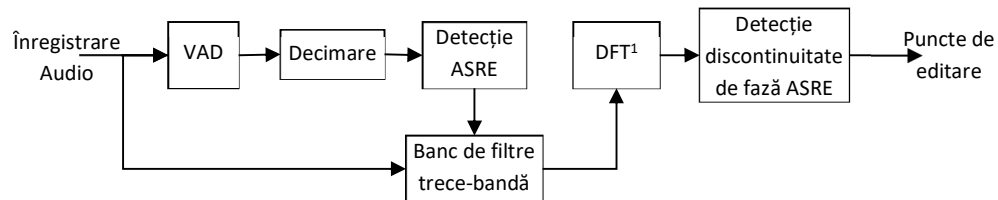
Autentificarea temporală a semnalului audio este posibilă prin compararea semnalului FRE, extras din înregistrare, cu o bază de date ce conține valorile FRE extrase continuu din rețeaua de energie electrică. Totuși, după cum este prezentat în [21], pentru a obține rezultate pertinente, durata semnalului audio investigat trebuie să fie de cel puțin 5 minute. Aceasta înseamnă că modificări minore efectuate asupra înregistrării audio, cum ar fi inserarea de cuvinte sau ștergerea acestora, nu vor fi observate în urma autentificării temporale cu ajutorul FRE. Pentru a crește robustețea metodei FRE pentru înregistrări scurte, în [21] este prezentată o procedură de autentificare bazată pe coeficientul de corelație maximă.

#### 4.1.2. Analiza multi-armonică

În continuare se va determina prezența unei armonici FRE prin realizarea unei analize spectrale numai asupra segmentelor de înregistrare audio cu liniște. Această soluție pe de o parte reduce efortul de calcul total, iar pe de altă parte elimină interferențele cu spectrul semnalului vocal relevant în analiza FRE. Totodată, soluția

este în concordanță cu situațiile reale în care se produc falsificări ale semnalului audio deoarece, în general, o editare audio este realizată pe segmentele de vorbire cu nivel acustic foarte mic (spre exemplu în momentele de liniște) astfel încât modificarea să nu fie audibilă.

Luând în considerare observațiile de mai sus, vom porni analiza multi-armonică propusă în acest capitol cu o procedură de detecție a vorbirii (VAD – Voice Activity Detection, Fig. 4.1). În implementare am folosit soluția descrisă în [22].



**Figura 4.1** Diagrama bloc a analizei multi-armonice propuse

Un pas important în analiza multi-armonică prezentată în cadrul acestei abordări propuse îl constituie decizia prezenței armonicilor SRE în semnalul audio analizat. Fără o decizie solidă în această direcție estimatele fazelor nu pot fi de încredere și, în consecință, nu se poate realiza analiza asupra evoluțiilor fazelor.

Pentru a putea valida sistemul propus de detecție al falsificărilor audio bazat pe analiza multi-armonică, am utilizat un set de 72 de semnale de test eșantionate la frecvența de 8000Hz, fiecare semnal având durata medie de aproximativ 15s.

**Tabelul 4.1** Performanțele sistemului propus

Armonici valide luate în considerare în decizia finală	Detecție [%]	Alarmer false [%]
50 Hz	76.67	1.38
50 Hz, 250 Hz și 350 Hz	44.44	0
Cel puțin două dintre: 50 Hz, 250 Hz sau 350 Hz	83.33	0

Tabelul 4.1 sintetizează rezultatele testelor experimentale în diferite situații. Pentru toate cadrele analizate numărul de armonici valide a fost 3 (armonicile valide erau plasate pe 50Hz, 250Hz și 350Hz). Dacă luăm în considerare doar evoluția fazei pentru prima armonică, atunci sistemul este capabil să detecteze corect existența și locația punctelor de editare în numai 76,67% din cazuri, iar în 1,38% din cazuri sistemul determină o discontinuitate falsă. Dacă monitorizăm toate cele trei armonici și validăm o discontinuitate doar dacă aceasta apare pe toate evoluțiile fazelor atunci obținem 0% alarme false, însă procentul de detecție scade la 44,44%. Dacă validăm o discontinuitate în situațiile în care aceasta apare în cel puțin două dintre cele trei evoluții ale fazelor

atunci performanțele sistemului cresc la o rată de detecție de 83,3% și un procent de 0% alarme false.

Rezultatele din acest subcapitol au fost publicate în articolul [23].

## **4.2. Detecția editărilor audio pe baza FRE cu ajutorul IFA**

În acest subcapitol sunt păstrate ideile de a utiliza estimatele de fază pentru armonicile superioare SRE pentru a detecta posibilele editări din înregistrările audio ce conțin voce și realizarea analizei doar asupra segmentelor de liniște din semnalul audio. Chiar dacă aceste idei previn suprapunerea dintre componentele spectrale ale vocii și cele ale semnalului SRE, tot va trebui să avem mare grijă atunci când estimăm fazele armonicilor SRE deoarece segmentele analizate pot fi foarte scurte (sub 0,25s). Pentru a rezolva această situație este propusă realizarea unei analize spectrale prin utilizarea unei versiuni îmbunătățite a atractorilor de frecvență instantanee (Instantaneous Frequency Attractors – IFA), ce s-au dovedit a fi de o acuratețe foarte ridicată, chiar și pentru cadre de analiză mici [24]. De asemenea, va fi introdus un criteriu mai simplu pentru detecția armonicilor SRE.

Pentru a realiza o evaluare consistentă am testat performanțele sistemului în diferite configurații. Pentru prima configurație, notată cu T1, am folosit setările pentru soluția propusă, mai exact, am analizat numai segmentele de liniște, am utilizat criteriul de detecție ASRE propus în secțiunea 3 și metoda IFAs pentru a extrage componentele ASRE. În configurația T2 am analizat tot numai segmentele de liniște, dar am utilizat criteriul de detecție ASRE descris în [25] și algoritmul  $DFT^1$  pentru a extrage componentele ASRE. Referitor la setările pentru metodele de analiză spectrală, pentru metoda IFA am folosit  $L = 40$  eșantioane și  $N_{DFT} = 2L$ , iar pentru metoda  $DFT^1$  am utilizat un cadru de analiză mai mare,  $L = 60$  eșantioane și  $N_{DFT} = 2000$ .

Am realizat și o a treia configurație, T3, pentru a obține o comparație cinstită între soluția noastră și cea descrisă în [25]. Așadar, în configurația T3 am analizat întregul semnal și am folosit criteriul de detecție ASRE din [25] în conjuncție cu implementarea noastră a metodei  $DFT^1$ .

*Tabelul 4.2 Evaluarea sistemului propus*

Tipul de test	Setul de semnale	Rata de detecție [%]	Tipul de test	Setul de semnale	Rata de detecție [%]
T1	FVS	61.2	T1	MVS	73.5
T2	FVS	59.3	T2	MVS	72
T3	FVS	52.8	T3	MVS	—

### **4.3. Algoritm rapid pentru detectarea editărilor de tip butt-splice**

În acest subcapitol vom realiza o analiză în detaliu a metodelor de referință utilizate pentru detectarea editărilor de tip butt-splice (editări de tip tăiere sau inserare segment prin care rezultă salturi de fază în semnalul audio). În primul rând, vom prezenta o soluție ce reduce semnificativ resursele de timp consumate. Apoi vom prezenta limitările metodei în ceea ce privește fereastra variabilă de analiză și vom testa două metode pentru a face diferența dintre semnalele audio ce au fost falsificate și cele ce nu au fost modificate. De asemenea, am dezvoltat o aranjare experimentală relevantă ce ne va permite să cuantificăm pentru prima dată performanțele metodei, în contextul expertizei criminalistice.

Optimizările din acest subcapitol ne permit să analizăm zile întregi de fișiere audio în câteva ore, sau chiar minute dacă avem la dispoziție un calculator foarte puternic. Spre exemplu, prin utilizarea calculatorului din dotare descris mai sus, am finalizat analiza unui semnal de 65 de secunde eșantionat la 44100Hz în numai 0,5s.

### **4.3. Aplicație software pentru detectare editărilor din înregistrări audio**

Studiile efectuate în subcapitolele 4.1, 4.2, 4.3 au condus în final la realizarea unei aplicații software, în Matlab, ce poate fi folosită pentru detectarea urmelor de editare din înregistrări audio.

Aplicația permite verificarea unei înregistrări audio cu ajutorul unui algoritm bazat pe principiul FRE și a unui algoritm bazat pe detecția salturilor de fază.



# Capitolul 5

## Sistem de protecție împotriva falsificărilor înregistrărilor audio

Metodele prezentate în capitolul anterior, de tip pasiv, se bazează pe anumite artefacte, care pot să apară sau nu, sau chiar pot fi ascunse de către persoana care încearcă să falsifice o înregistrare. Spre exemplu, Metoda Cooper [4] caută discontinuități în forma de undă a semnalului audio, ce a fost editat prin ștergerea sau adăugarea de secvențe audio într-o anumită înregistrare. Însă programele de editare mai noi, cum ar fi Adobe Audition, interpolatează semnalul în zona acestor discontinuități, netezindu-le. Sau, chiar și fără un astfel de program la dispoziție, persoana care realizează o anumită editare poate să fie atentă la punctele pe care le alege pentru editare astfel încât în final să nu apară nicio discontinuitate în înregistrarea finală.

În acest capitol, inspirat din criteriul FRE [1] și de metoda live watermarking propusă pentru concerte live [8], am propus o metodă activă pentru detecția urmelor de editare dintr-o înregistrare audio. Această metodă va sta la baza unui sistem de detecție a falsificărilor dintr-o înregistrare audio. În plus, prin această metodă voi putea spune, cu un coeficient ridicat de încredere, atât că o anumită înregistrare a fost editată, cât și că nu a fost editată (dacă este cazul).

Metoda activă, propusă în acest capitol pentru a fi folosită la detecția urmelor de editare dintr-o înregistrare audio, urmărește să nu facă nicio prelucrare digitală asupra semnalului înregistrat, ci se va baza pe un zgomot generat de un aparat auxiliar aflat în încăperea în care se realizează înregistrarea. Acest zgomot fie va trebui mascat de sunetul produs în încăperea, astfel încât să nu poată fi auzit de persoana înregistrată, fie trebuie să fie un zgomot uzual, ce poate fi auzit într-o încăperea fără a atrage atenția asupra sa.

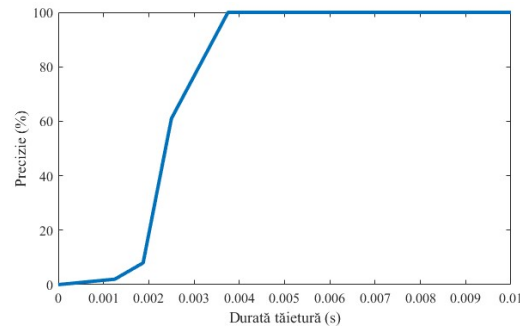
Într-o aplicație tipică de expertiză criminalistică a unei înregistrări audio nu este posibilă folosirea unei metode active. Sistemul pe care urmează să îl prezint este dedicat unei categorii de utilizatori mai restrânsă. Acest sistem poate fi folosit de o persoană cu un statut social ridicat atunci când are întâlniri importante. Astfel în cât dacă cineva înregistrează respectiva întâlnire să nu o poată prezenta în afara contextului prelucrând-

o în vederea alterării conținutului. Folosirea acestui sistem va permite persoanei calomniate să dovedească foarte ușor că înregistrarea respectivă a fost alterată.

Performanțele metodei sunt evaluate cu ajutorul următoarei metrici statistice:

$$\text{Precizie} = \frac{\text{Detectii adevărate}}{\text{Detectii adevărate} + \text{Detectii false}}, \quad (5.6)$$

Rezultatele algoritmului propus, în condițiile enumerate mai sus, sunt sintetizate în Fig. 5.4. Se poate observa că metoda propusă se poate dovedi un utilitar foarte puternic pentru a determina integritatea unei înregistrări audio, relativ la editări de tip tăiere și adăugare secvențe.



**Figura 5.4** Precizia de detecție a urmelor de editare, de tip tăiere sau adăugare secvențe, ca funcție de durata editării

Analizând graficul din Fig. 5.4 se poate observa că algoritmul are o precizie de detecție a editărilor de tip tăiere de 100% dacă durata secvenței tăiate este mai mare de 5 ms. Iar rata de falsă detecție a înregistrărilor needitate este de 0%. Prin urmare metoda propusă poate fi folosită cu succes pentru a asigura integritatea unei înregistrări audio.

# Capitolul 6

## Concluzii generale și perspective

Lucrarea de față a urmărit expertiza criminalistică a înregistrărilor audio din punctul de vedere al autentificării și verificării integrității acestora.

Pentru realizarea autentificării temporale a înregistrărilor audio, afectate de brum de rețea, s-a dezvoltat o soluție hardware și software pentru crearea unei baze de date cu referință de SRE și FRE. O primă variantă bazată pe o soluție software dezvoltată în Matlab și o a doua soluție, mult mai ieftină bazată pe o platformă hardware Raspberry Pi 2 și o soluție software dezvoltată în Python, realizând scăderea costurilor de aproximativ 10 ori.

Din punctul de vedere al verificării integrității înregistrărilor audio, relativ la editări de tip adăugare și ștergere segmente audio, pentru a modifica mesajul final din înregistrare s-au urmărit două metode de abordare a problemei. O variantă clasică în care se folosesc metode pasive, ce nu presupune un mod special de realizare a editărilor, care poate fi folosită la a determina dacă o înregistrare editată a fost falsificată, însă nu poate autentifica o înregistrare needitată. Și, o abordare nouă, care presupune realizarea unei înregistrări într-un anumit context, astfel încât să existe un watermark de tip zgomot sensibil la editări.

### 6.1. Rezultate obținute

Capitolul 2 prezintă o sinteză cu:

- legile care au reglementat expertiza criminalistică a înregistrărilor multimedia, de la Codului Penal din 21 iulie 1968, în care nu erau reglementate aproape deloc aceste lucruri, până la NCPP - actualizat prin Legea nr. 255/2013 - pentru punerea în aplicare a Legii nr. 135/2010 privind Codul de procedură penală și pentru modificarea și completarea unor acte normative care cuprind dispoziții procesual penale din 19 iulie 2013, M. Of. 515/2013, prin articolele: 138-153 (**CAPITOLUL IV - Metode speciale de supraveghere sau cercetare**);
- practici și standarde, folosite de trei mai laboratoare din întreaga lume și INEC din România, de la specializarea personalului implicat în activități de expertiză criminalistică a înregistrărilor multimedia până la standarde de asigurare a calității întregului proces de expertiză;

- în final sunt prezentați principalii algoritmi folosiți în practică și studiați în literatura de specialitate ce realizează expertiza criminalistică a înregistrărilor audio pe baza anumitor artefacte specifice procesului de falsificare a probelor audio.

Pe baza cercetărilor efectuate în Capitolul 3 au fost dezvoltate două soluții hardware și software pentru crearea unei baze de date SRE și FRE ce poate fi folosită pentru a autentifica momentul de timp la care a fost efectuată o înregistrare afectată de brumul de rețea.

Rezultatul final al cercetărilor făcute pentru Capitolul 4 o reprezintă o aplicație software ce poate fi folosită pentru a verifica integritatea unei înregistrări audio, din punctul de vedere al editărilor de tip ștergere și inserare fragmente audio. Aplicația are la bază doi algoritmi, unul bazat pe principiul FRE și poate fi folosit doar pentru înregistrări afectate de brumul de rețea și un al doilea algoritm ce caută artefacte de tip „butt-splice” în înregistrări posibil ediate.

Capitolul 5 reprezintă o idee inovativă în direcția verificării integrității înregistrărilor needitate cu rezultate certe, ce nu pot fi contestate într-o curte judecătorească.

## **6.2. Contribuții originale**

1. Studiul sintetic al tuturor standardelor, practicilor și algoritmilor pentru expertiza criminalistică
2. Proiectarea a două soluții hardware/software pentru realizarea unei baze de date SRE și FRE [C1, C6].
3. Dezvoltarea a două soluții hardware/software pentru realizarea unei baze de date SRE și FRE [C1, C6].
4. Un nou algoritm pentru autentificarea temporală a înregistrărilor audio afectate de brumul de rețea [R1, R2, C3].
5. O aplicație software pentru găsirea punctelor de editare din înregistrările audio editate [R1, R2, C3, C5].
6. O bază de date, cu înregistrări audio afectate de brumul de rețea, editate și needitate, ce poate fi folosită pentru a determina performanțele algoritmilor propuși pentru verificare integrității pe baza principiului FRE [R1, R3].
7. Un algoritm rapid pentru detecția urmelor de editare de tip ‘butt-splice’ [C5].
8. Implementarea în Matlab a unui algoritm rapid pentru detecția urmelor de

editare de tip ‘butt-splice’ [C5].

9. O bază de date cu înregistrări audio cu editări de tip ‘butt-splice’ [C5].
10. O metodă inovativă pentru certificarea integrității înregistrărilor needitate plecând de la anumite idei din articolele [C7, C8] și prezentată parțial în C9.

## 6.3. Lista lucrărilor originale

### Proiecte

**Proiect tip Cecuri de Inovare, contract nr. 47CI/2017 (PN-III-P2-2.1-CI-2017-0362), cu titlul „Aplicație software pentru arbitraj video Scrimă” – în calitate de responsabil proiect partener UPB**

### Reviste indexate ISI/BDI

**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

### Conferințe indexate ISI

**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, București, 7-9 Mai 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, Iași, 9-10 Iulie 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. Nită**, A. Ciobanu, C. Negrescu, D. Stanomir, ” Low cost electric network signal and frequency recorder”, ATEE 2017, București, 23-25 Martie 2017, DOI 10.1109/ATEE.2017.7905094, INSPEC 16836130.

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

**C8. V.A. Nită, R. A. Dobre, S. Ciochină, C. Paleologu** ” Improved Convergence Model of the Affine Projection Algorithm for System Identification”, prezentat la ISSCS 2017, Iași, 13-14 Iulie 2017.

**C9. V.A. Nită, A. Ciobanu** ” TIC-TAC, FORGERY TIME HAS RUN-UP! LIVE ACOUSTIC WATERMARKING FOR INTEGRITY CHECK IN FORENSIC APPLICATIONS”, prezentat la ICASSP 2018, Calgary, 15-20 Aprilie 2018.

## **6.4. Perspective de dezvoltare ulterioară**

Din punctul meu de vedere cele mai importante perspective de dezvoltare ulterioară le au metodele active de găsire a punctelor de editare, acestea reprezintă un subiect mai puțin cercetat, spre deosebire de metodele pasive care au ajuns la un stadiu de maturitate cu rezultate promițătoare. Ele pot oferi protecție împotriva calomniei prin prezentarea unor înregistrări alterate ca fiind originale.

Prin urmare, relativ la metodele active, o dezvoltare ulterioară ar putea fi crearea a două aplicații de watermark analogic specifice situațiilor de verificare a integrității pentru înregistrările audio:

- Un ceas al cărui ticăit să fie asincron, cu mici variații de maxim  $\pm 25$  ms, astfel încât acestea să nu fie observate de cineva care se află în aceeași cameră cu ceasul respectiv, variații ce vor avea un șablon specific care va fi afectat de orice editare de tipul ștergere și inserare fragmente audio dintr-o înregistrare;
- O aplicație software pentru smartphone care va putea fi folosită pentru a realiza înregistrări audio peste care este suprapus același tip de watermark ca în aplicația hardware propusă mai sus.

O altă perspectivă importantă de dezvoltare ulterioară o are dispozitivul de înregistrare FRE, cu preț scăzut, prezentat în Capitolul 3; acesta poate reprezenta punctul de plecare pentru o rețea de baze de date FRE, distribuită la nivel național, ce va putea fi folosită atât pentru autentificarea momentului de timp la care a fost realizată o înregistrare, cât și zona geografică în care a fost realizată aceasta.

# Bibliografie selectivă

- [1] C. Grigoraş, „Digital audio recording analysis: the Electric Network Frequency (ENF) criterion,” *The International Journal of Speech Language and the Law*, vol. 12, nr. 1, pp. 63-76, 2005.
- [2] Ö. Eskidere și A. Karatutlu, „Source microphone identification using multitaper MFCC features,” în *9th International Conference on Electrical and Electronics Engineering (ELECO)*, Bursa, 2015.
- [3] J. Chai, Z. Y. L. Y, R. W. Conners și Y. Liu, „Tampering detection of digital recordings using electric network frequency and phase angle,” *Audio Engineering Society Convention 135*, 2013.
- [4] A. Cooper, „Detecting butt-spliced edits in forensic digital audio recordings,” în *Proc. Audio Eng. Soc. 39th Conf., Audio Forensics: Practices and Challenges*, Hillerod, 2010.
- [5] D. Luo, R. Yang și J. Huang, „Detecting double compressed AMR audio using deep learning,” în *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Florence, 2014.
- [6] S. P. Mohanapriya, E. P. Sumesh și R. Karthika, „Environmental sound recognition using Gaussian mixture model and neural network classifier,” în *International Conference on Green Computing Communication and Electrical Engineering (ICGCCCE)*, Coimbatore, 2014.
- [7] A. Ciobanu, T. Culda, C. Negrescu și D. Stanomir, „Analysis of reverberation time blind estimation used in audio forensics,” în *11th International Symposium on Electronics and Telecommunications (ISETC)*, Timisoara, 2014 .
- [8] R. Tachibana, „Sonic Watermarking,” *EURASIP Journal on Applied Signal Processing*, vol. 13, p. 1955–1964, 2004.
- [9] W.-H. Chuang, R. Garg și M. Wu, „Anti-forensics and countermeasures of electrical network frequency analysis,” *IEEE Trans. Inf. Forensics Security*, vol. 8, nr. 12, pp. 2073-2086, 2013.
- [10] V. A. Niță, R. A. Dobre, A. Drumea, A. Ciobanu, C. Negrescu și D. Stanomir, „Electrical network signal's waveform and frequency logging for forensic,” în *Advanced Topics in Electrical Engineering (ATEE), 2015 9th International Symposium*, Bucharest, 2015.
- [11] M. M. Elmesalawy și 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, nr. 4, pp. 633-644, 2014.
- [12] V. A. Niță, A. Ciobanu, C. Negrescu și D. Stanomir, „Low cost electric network signal and frequency recorder,” în *Advanced Topics in Electrical Engineering (ATEE), 2017 10th International Symposium*, Bucharest, 2017.
- [13] A. Petre și C. Grigoraş, *Înregistrările audio și audio-video*, București: C.H. Beck, 2010.

- [14] INEC, „Expetize,” [Interactiv]. Available: <http://www.inec.ro/index.php/activitate/expetize>. [Accesat 25 Iulie 2017].
- [15] M. Justiției, „Tabelul nominal cu expertii criminalisti autorizati,” Ministerul Justiției, [Interactiv]. Available: <http://www.just.ro/profesii-conexe/tabelul-nominal-cu-expertii-criminalisti-autorizati/>. [Accesat 25 Iulie 2017].
- [16] INEC, „Rapoarte si Studii,” [Interactiv]. Available: <http://www.inec.ro/index.php/prezentare/rapoarte-si-studii>. [Accesat 26 Iulie 2017].
- [17] I. Anghelescu, *Expertiza Criminalistică a Vocii și Vorbirii*, București: Editura Științifică și Enciclopedică, 1978.
- [18] A. T. Ho și S. Li, *Handbook of Digital Forensic of Multimedia Data and Devices*, John Wiley & Sons, 2015.
- [19] C. Grigoraș, „Application of ENF analysis in forensic authenticity of digital audio,” *Journal of the Audio Engineering Society*, vol. 57, nr. 9, p. 643–661, 2009.
- [20] A. Hajj-Ahmad, R. Garg și M. Wu, „ENF-based region-of-recording identification for media signals,” *IEEE Trans. Inf. Forensics Security*, vol. 10, nr. 6, p. 1125–1136, 2015.
- [21] M. Huijbregtse și 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.
- [22] J. Sohn, N. S. Kim și W. Sung, „A statistical model-based voice activity detection,” *IEEE Signal Processing Letters*, vol. 6, nr. 1, pp. 1-3, 1999.
- [23] V. Nita, A. Ciobanu, R. Dobre, C. Negrescu, D. Stanomir și 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, nr. 4, pp. 199-212, 2015.
- [24] A. Ciobanu, C. Negrescu, V. A. Niță, R. A. Dobre și D. Stanomir, „High accuracy frequency analysis using instantaneous frequency attractors,” în *23rd European Signal Processing Conference (EUSIPCO)*, Nice, 2015.
- [25] D. Rodriguez, J. Apolinario și L. Biscainho, „Audio Authenticity Based on the Discontinuity of ENF Higher Harmonics,” în *Proc. EUSIPCO*, 2013.
- [26] V. Niță și A. Ciobanu, „TIC-TAC, FORGERY TIME HAS RUN-UP! LIVE ACOUSTIC WATERMARKING FOR INTEGRITY CHECK IN FORENSIC APPLICATIONS,” în *ICASSP*, Calgary, 2018.