Amprentarea Telefoanelor Mobile Folosind Traductoarele Incorporate

Teză de doctorat – Rezumat
pentru obținerea titlului științific de doctor la
Universitatea Politehnica Timișoara
în domeniul de doctorat Calculatoare și Tehnologia Informației
de
Ing. Adriana-Maria Berdich
conducător științific Prof. Bogdan Groza
Mai, 2023

În zilele noastre, smartphone-urile au capacități uimitoare de procesare și de stocare. Ele sunt, de asemenea, echipate o mulțime de senzori inclusiv difuzoare, microfoane, accelerometre, magnetometre şi senzori de frecvenţă radio (NFC, UWB şi GPS). Acestea sunt denumite în general traductoare, componente care convertesc o formă de energie în alta. Datorită procesului de fabricaţie, fiecare traductor are proprietăţi unice. Aceste proprietăţi au potenţialul de a fi utilizate ca o amprentă pentru dispozitivul mobil. Amprentele digitale bazate pe software pot fi de asemenea utilizate, dar în această teză accentul este pus pe amprente digitale bazate pe componente hardware. Acest lucru se datorează faptului că acestea se bazează pe caracteristicile traductoarelor care sunt încorporate în circuitulele telefoanelor şi sunt mai dificil de înlocuit. Acest lucru face ca amprenta să fie mai greu de falsificat.

Fig. 1. Un smartphone generic cu senzorii și traductoarele folosite la amprentare

În Figura 1 este ilustrat un smartphone cu senzorii și traductoarele care pot fi supuse amprentării. Începând cu anii 2000 au fost publicate articole științifice care studiază identificarea circuitelor electronice folosind caracteristicile fizice [1]. Ulterior, funcțiile fizice neclonabile (PUF), bazate pe proprietățile distinctive și unice ale circuitelor, au fost propuse în [2] pentru aplicații de securitate cum ar fi autentificarea dispozitivelor. Autentificarea dispozitiv-la-dispozitiv (D2D) este comună și în scenarii IoT (Internet of Things). Folosirea caracteristicilor dispozitivului pentru a asigura autentificarea este o modalitate de a elimina interacţiunea cu utilizatorul. Acest lucru este deosebit de benefic pentru dispozitivele încorporate din casă sau în interiorul vehiculelor în cazul în care accesibilitatea la interfaţa cu utilizatorul poate fi limitată.

Obiectivele cercetării. Această teză vizează amprentarea smartphone-urilor pe baza senzorilor incorporați: accelerometre, difuzoare, microfoane și camere. De asemenea, aceste tehnici de amprentare sunt extinse către amprentarea ECU-urilor din vehicule. Principalele obiective ale acestei teze pot fi rezumate după cum urmează:

1) Sudiul literaturii existente care se axează pe amprentarea smartphone-urilor pe baza traductoarelor încorporate;
2) Colectarea datelor de la accelerometre, difuzoare, microfoane şi camere de la smartphone-uri diferite şi smartphone-uri identice;
3) Analizarea datelor colectate şi găsirea caracteristicilor fiabile pentru amprentare;
4) Amprentarea smartphone-urilor pe baza datelor colectate de la accelerometre, difuzoare, microfoane şi camere;
5) Analizarea mai multor tehnici de clasificare şi demonstrarea faptului că algoritmii tradiţionali de machine learning pot avea rezultate mai bune decât rețelele neuronale sofisticate;
6) Analizarea şi testarea modului în care tehnicile de amprentare ale smartphone-urilor pot fi extinse la alte componente, cum ar fi ECU-urile din vehicule.

Contribuții majore. În această teză, sunt amprentate mai multe traductoare ale smartphone-urilor: accelerometre, difuzoare, microfoane şi camere. În plus faţă de senzorii smartphone-urilor, de asemenea, este analizată și amprentarea ECU-urilor din vehicule. Contribuţiile acestei teze pot fi rezumate după cum urmează:

1) Au fost realizate mai multe seturi de date consistente care conţin:
   - Date de la accelerometre colectate în diferite moduri de transport: tramvai, tren, masină, pe bicicletă, mergând şi scuturând telefoanele in mână [3];
   - 3,000 de măsurători colectate cu 28 de difuzoare ale smartphone-urilor [4];
   - 19,200 de măsurători colectate cu 32 de microfoane ale smartphone-urilor [5];
   - 300 fotografii întunecate colectate cu 6 camere de telefon identice [6];
2) Mai mulți algoritmi de clasificare au fost utilizați şi a fost analizată performanţa lor în diferite scenarii, folosind, unele tehnici de procesare de semnale atunci când a fost necesar [4], [5], [6], [7], [8];
3) Amprentarea modelelor de smartphone-uri identice şi diferite be baza traductoarelor incorporate: accelerometre, difuzoare, microfoane şi camere [4], [5], [6], [7];
4) Amprentarea smartphone-urilor în prezența diferitelor tipuri și niveluri de zgomot [4], [5];
5) Diverse scenarii de autentificare dispozitiv-la-dispozitiv şi smartphone-la-vehicul au fost abordate ca aplicaţii pentru amprentarea smartphone-urilor [3].

Aceste contribuţii majore sunt reflectate de următoarele publicaţii în reviste şi conferinţe ISI relevante. În [3] autorul a explorat asocierea smartphone-urilor pe baza datelor colectate de la accelerometre în diferite mijloace de transport. Pentru aceasta, mai multe date de la accelerometre au fost colectate în diverse mijloace de transport: tren, tramvai, mașină și bicicletă. Aceste date au fost analizate pentru propunerea şi implementarea unui protocol de schimb de cheie. Amprentarea smartphone-urilor pe baza datelor colectate de la accelerometru a fost studiată în [7]. Experimente cu 5 smartphone-uri identice şi 5 smartphone-uri diferite s-au făcut în scopul de a le amprenta pe baza caracteristicilor extrase din accelerometru. În [4] a fost studiată amprentarea smartphone-urilor pe baza caracteristicilor difuzorului. Un set de date a fost construit, conţinând înregistrări de la 16 difuzoare identice şi 12 difuzoare diferite. Fiecare difuzor emite un semnal linear sweep între 20Hz si 20KHz. Smartphone-urile au fost identificate pe baza caracteristicilor roll-off extrase din semnalele emise de difuzoare. De asemenea, pentru o clasificare mai precisă au fost utilizate reţelele neurale recurente. În [5], am studiat amprentarea microfonului. Un set de date a fost construit, conţinând experimente cu 16 smartphone-uri identice care înregistrează sunete de locomotivă, barieră, claxon de mașină şi scârțâit de roți. Aceste sunete au fost reproduse de un sistem audio de înaltă fidelitate. De asemenea, setul de date contine și inregistrari live ale claxonului masinii, sunetului luminilor de avarii și ștergatoarelor inregistrate cu 16 smartphone-uri diferite. Spectrul de putere al fiecărui semnal a fost extras din sunetele înregistrate și folosit ca intrare pentru mai multe clasificatoare pentru a separa smartphone-urile. Acest set de date a fost, de asemenea, făcut public pentru a servi la investigaţii viitoare. Amprenta smartphone-urilor pe baza caracteristicilor camerei a fost discutată de către autor în [6]. Caracteristicile extrase din 50 de imagini colectate utilizând 6 smartphone-uri identice au fost utilizate ca intrare pentru mai mulți algoritmi de clasificare.

Algoritmii de clasificare utilizați pentru identificarea smartphone-urilor în lucrările menționate anterior au fost utilizați și în [9] pentru a amprenta ECU-urile din vehicule folosind un set de date existent. De asemenea, autorul a contribuit la alte lucrări de cercetare axate pe interacţiunea vehicul-smartphone, care, deşi acestea nu fac parte din acestă teză, au oferit o mare oportunitate pentru autor pentru a obţine experiență în securitatea ecosistemului smartphone-vehicul. Aceste lucrări discută interactiunea dintre vehicul și smartphone [10], drepturile de acces în vehicul bazat pe servicii cloud [11], accesul in mașină pe baza smartphone-urilor [12] şi schimbul de cheie între smartphone şi vehicul pe baza datelor audio și vizuale [13].

Pentru a rezuma contributiile autorului, acesta a contribuit la 11 lucrări axate pe sistemul de securitate al telefoanelor şi prezenţa lor în mediul vehiculelor, din care primele 7 lucrări formează corpul principal al tezei:

1) A. Berdich, B. Groza, R. Mayrhofer, E. Levy, A. Shabtai, and Y. Elovici, “Sweep-to-unlock: Fingerprinting smartphones based on loudspeaker roll- off characteristics,” *IEEE Transactions on Mobile Computing*, 2021.
2) B. Groza, A. Berdich, C. Jichici, and R. Mayrhofer, “Secure accelerometer based pairing of mobile devices in multi-modal transport,” *IEEE Access*, vol. 8, pp. 9246–9259, 2020.
3) A. Berdich, B. Groza, E. Levy, A. Shabtai, Y. Elovici, and R. Mayrhofer, ”Fingerprinting smartphones based on microphone characteristics from environment affected recordings,” *IEEE Access*, vol. 10, pp. 122 399–122 413, 2022.
4) A. Berdich and B. Groza, ”Smartphone camera identification from low-mid frequency dct

coefficients of dark images," *Entropy*, vol. 24, no. 8, p. 1158,x 2022.
5) S. Murvay, A. Berdich, and B. Groza, "Physical layer intrusion detection and localization on CAN bus," Machine Learning and Optimization Techniques for Automotive Cyber-Physical Systems, *Springer*, 2023, **(accepted for publication)**.
6) A. Berdich, B. Groza, and R. Mayrhofer, "A survey on fingerprinting technologies for smartphones based on embedded transducers," **(under submission)**.
7) A. Berdich, P. Iosif, C. Burlacu, A. Anistoroaei, and B. Groza, "Fingerprinting smartphone accelerometers with traditional classifiers and deep learning networks," *IEEE 17th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, 2023, **(accepted for publication)**.
8) B. Groza, H. Gurban, L. Popa, A. Berdich, and S. Murvay, "Car-to- smartphone interactions: Experimental setup, risk analysis and security technologies," in *5th International Workshop on Critical Automotive Applications: Robustness & Safety*, 2019.
9) A. Berdich, A. Anistoroaei, B. Groza, H. Gurban, S. Murvay, and D. Iercan, "Antares-anonymous transfer of vehicle access rights from external cloud services," in *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, IEEE, 2020, pp. 1–5.
10) B. Groza, T. Andreica, A. Berdich, P. Murvay, and E. H. Gurban, "Prestvo: Privacy enabled smartphone based access to vehicle on-board units," *IEEE Access*, vol. 8, pp. 119 105–119 122, 2020.
11) A. Anistoroaei, A. Berdich, P. Iosif, and B. Groza, "Secure audio-visual data exchange for android in-vehicle ecosystems," *Applied Sciences*, vol. 11, no. 19, p. 9276, 2021.

Capitolul II a prezentat pe scurt principiile de funcţionare din spatele traductoarelor smartphone-urilor: accelerometre, difuzoare, microfoane şi camere. De asemenea au fost prezentate cele mai populare metode de extracție a caracteristicilor, algoritmi de clasificare și o imagine de ansamblu a metodelor de evaluare. Acest capitol a ilustrat de asemenea unele scenarii de aplicare şi măsuri preventive împotriva exploatării amprentelor smartphone-urilor cu scopul de a scurgere informații confidenţiale. În ceea ce priveşte fiecare senzor prezentat în teză, lucrările aferente existente în literatură, au arătat următoarele. Accelerometre au fost utilizate pe scară largă pentru autentificarea dispozitivelor (asocierea) şi este surprinzător faptul că doar câteva lucrări discută amprentarea smartphone-urilor pe baza datelor colectate de la accelerometre. Difuzoarele au fost folosite mult mai puţin frecvent în cercetare decât microfoanele. Este posibil ca semnale audio de la difuzoare sa fie folosite mai puțin pentru amprentare, deoarece, aceste date sunt simplu de evaluat, dar sunt mai dificil de colectat. Există mai multe seturi de date accesibile publicului pentru microfoane (majoritatea dintre ele concentrându-se pe recunoaşterea vorbirii şi investigaţii criminalistice), care sunt, de asemenea, utilizate pentru identificarea dispozitivului pe baza caracteristicilor microfoanelor. Din cunoştinţele autorului, singurul set de date public disponibil pentru identificarea difuzoarelor este rezultatul cercetării efectuate pentru această teză. Pe baza lucrărilor studiate în această teză, subiectul amprentării camerei a fost abordat de cele mai multe de lucrări de cercetare în comparaţie cu toţi ceilalţi senzori. Acest lucru este de aşteptat, având în vedere faptul ca astfel de date sunt relativ uşor de colectat, dar de asemenea ar putea duce la preocupări legate de confidenţialitate. În plus, fotografiile pot fi folosite pentru a extrage o mare varietate de caracteristici.

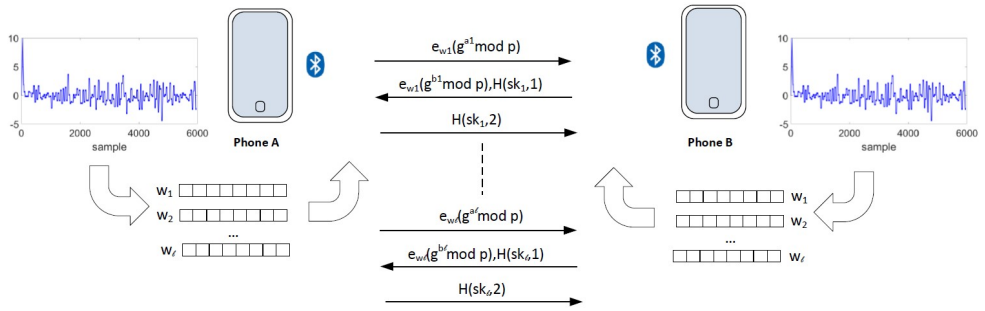

Fig. 2. Colectarea datelor si schimbul de cheie dintre două smartphone-uri

Capitolul III a discutat despre asocierea smartphone-urilor în mai multe mijloace de transport pe baza datelor colectate de la accelerometre și, de asemenea, amprentarea smartphone-urilor pe baza datelor de la accelerometre. Datele de la accelerometre au fost colectate folosind trei smartphone-uri în diferite moduri de transport: în tramvai, tren, mașină, pe bicicletă cu smartphone-urile în buzunar, mergând cu smartphone-urile în buzunar și scuturând smartphone-urile în mână. Semnalele de la accelerometre diferă în mod substanțial în funcție de mijlocul de mișcare. Concluziile acestei teze au demonstrat că obţinerea unei entropii suficiente din datele accelerometrului a fost posibilă pentru a crea o cheie de sesiune în toate mediile de transport. Extragerea entropiei scăzute poate duce, de asemenea, la asigurarea unei chei de sesiune generată și interschimbată între dispozitive folosind protocoale rezistente la atacuri de tip guessing. Au fost folosite mai multe tehnici de procesare a semnalelor cum ar fi scaralrea simplă, modulareea sigma-delta, filtru high-pass și smoothness. Majoritatea metodelor de filtrare utilizate au dat rezultate comparabile. Totuşi, scalarea simplă a datelor colectate de la accelerometru a fost cea mai potrivită alegere din cauza simplicităţii sale. Entropia a fost crescută prin extinderea vectorilor de caracteristici folosind modularea sigma-delta, dar acest lucru necesită mai multe calcule, deoarece mai multe caracteristici au trebuit extrase. Având în vedere variaţiile din mijloacele de transport, parametrii specifici pot fi avantajoși în funcţie de caz şi de compromisul dintre nivelul de securitate şi probabilitatea de împerechere. Folosind avantajul adversarului şi rata de succes de împerechere, a fost furnizată o imagine mai precisă a acestei abordări. Protocolul de schimb de chei începe cu sincronizarea temporală între smartphone-uri, urmată de colectarea datelor, procesarea și împărțirea acestora în mai multe ferestre. Aceste ferestre sunt apoi utilizate pentru a genera cheile, care sunt transferate între smartphone-uri prin conexiune Bluetooth utilizând protocoalele EKE-DH și SPEKE. SPEKE este un protocol rezistent atacuri de tip guessing și a fost propus în [14]. Schimbul de chei între două smartphone-uri este descris în Figura 2. Timpul de calcul pentru operația de împerechere folosind EKE-DH este între 25ms și 230ms pentru calculul share-ului și între 39ms și 411ms pentru recuperarea cheii pentru modulele de 1024 biți și 2048 biți. În cazul SPEKE, timpul de calcul este între 20ms și 145ms pentru calculul share-ului și între 7ms și 70ms pentru recuperarea cheii. Timpul de calcul depinde și de performanța smartphone-ului. Acest capitol a discutat și amprentarea smartphone-urilor pe baza datelor colectate de la accelerometre. Datele au fost colectate folosind 5 smartphone-uri identice si 5 smartphone-uri diferite. Cu fiecare smartphone au fost colectate peste 40 de minute de date la o rată de eșantionare de 10ms. Din datele colectate au fost extrase 7 caracteristici în domeniul timp (Kurtosis, Skewness, SNR, STD, RMS, valoarea de vârf şi SINAD). Aceste caracteristici au fost apoi folosite ca input

pentru 5 algoritmi de clasificare (NN, KNN, SVM, Ensemble și Decision Trees). Clasificatorul Ensemble a furnizat o acurateţe maximă de recunoaştere de 100% pentru setul de date colectat de la 5 telefoane diferite şi 5 telefoane identice. Rezultatele au demonstrat că algoritmii clasici de clasificare pot produce rezultate bune pentru amprentarea smartphone-urilor pe baza datelor colectate de la accelerometre. Rețelele neuronale sofisticate nefiind necesare, mai ales atunci când datele de antrenare sunt limitate.

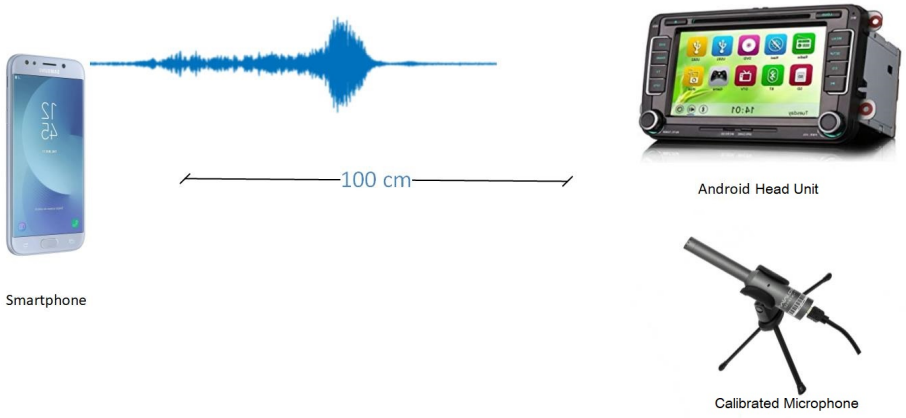

Fig. 3. Reprezentare sugestivă a setup-ului: o unitate de infotainment Android sau un microfon care înregistrează sunetul emis de un smartphone

Capitolul IV a abordat amprenta digitală a smartphone-urilor pe baza caracteristicilor difuzoarelor. Smartphone-urile pot fi amprentate folosind metodele rezumate în această teză. Amprentarea smartphe-urilor poate fi utiă în viața de zi cu zi ca alternativă pentru chei de mașină (chei inteligente) identificabile bazate pe caracteristicile fizice ale smartphone-urilor. În această teză, a fost investigată o tehnică de amprentare eficientă care poate fi aplicată rapid pentru identificarea smartphone-urilor bazată pe caracteristicile de roll-off ale difuzorului. Pentru experimente a fost folosit un sistem de infotainment din mașină, care a înregistrat sunetele emise de 28 de difuzoare (16 identice și 12 diferite). Fiecare difuzor a emis un semnal liniar sweep cu o durată de aproximativ 10 secunde. Distanța dintre sistemul de infotainment și difuzoare a fost de 1 metru. În aceast setup, au fost efectuate 3,000 de măsurători. O descriere sugestivă a setup-ului este prezentată în Figura 3. Spectrul de putere a fost extras din fiecare semnal înregistrat de unitatea de infotainment și apoi a fost folosit fie pentru a determina panta caracteriticilor roll-off low și high, fie pentru a folosi tehnici de machine learning mai complicate. De asemenea, folosind 4 smartphone-uri, au fost făcute măsurători la diferite niveluri de volum, (50%, 75%, 100%) și unghiuri de orientare ($0°$, $45°$ și $90°$). Caracteristicile roll-off ale difuzorului oferă o amprentă de încredere, care este rezistentă la variaţile nivelului de volum. În schimb, anumite tehnici pot fi înşelătoare, în timp ce panta de roll-off a fost adecvată pentru a identifica modele diferite de smartphone-uri, rețelele neuronale recurente au fost necesare pentru o analiză mai amănunţită a difuzoarelor provenite de la aceleaşi modele de smartphone-uri. Separarea între difuzoarele identice se poate face cu o precizie de 90–99% utilizând reţelele neurale recurente

LSTM şi BiLSTM. A fost analizat și impactul zgomotului, ținând cont de faptul că într-un scenariu real, zgomotele de fond sunt prezente și pot afecta mecanismul de amprentare al difuzoarelor. Au fost luate în considerare două tipuri semnificative de zgomot: zgomotul alb Gaussian aditiv (AWGN), care imită impactul mai multor procese aleatorii observate în natură și poate, de asemenea, să țină cont de zgomotul din interiorul mașinilor și zgomotul stradal, care este unic pentru scenariul în care sunt implicate mașini. În [15], atenuarea sunetului de la difuzor la microfon a fost, de asemenea, simulată folosind zgomotul alb Gaussian aditiv. Separarea dintre difuzoare era încă vizibilă după ce s-a introdus zgomot identic în înregistrări. Măsurătorile repetate efectuate în interiorul vehiculului în stradă, pe o stradă aglomerată, cu geamul din stânga deschis au relevat o separare mai puțin distinctă. Un scenariu de aplicare discutat a fost utilizarea smartphone-urilor în interiorul vehiculelor, motiv pentru care cele mai multe dintre experimentele efectuate în acest capitol a fost făcute cu o unitate de infotaiment din mașină care înregistrează sunetele emise de smartphone-uri. Identificarea a avut o rată mare de succes, indicând faptul că unităţile de infotainment din vehicule sunt utilizabile în astfel de scenarii.

Capitolul V a investigat amprentarea microfonului pe baza spectrului de putere extras din semnalul înregistrat folosind diferitele metode de clasificare (Linear Discriminant, Ensemble-Subspace Discriminant, Fine Tree, Fine KNN și Linear SVM). Analiza s-a concentrat pe trei scenarii separate, așa cum se arată în Figura 4: scenariul A, amprentarea smartphone-urilor diferite pe baza vocii umane, scenariul B, amprentarea smartphone-urilor identice pe baza sunetului ambiental folosind sunete preînregistrate și scenariul C, amprentarea smartphone-urilor diferite pe baza înregistrărilor live. Pentru scenariu A, a fost folosit setul de date MOBIPHONE deja existent [16]. Acest set de date conține voci umane înregistrate cu 21 de smartphone-uri diferite. Setul de date pentru fiecare smartphone include 24 de înregistrări audio de la 12 bărbați și 12 femei. Pentru scenariul B, înregistrările au fost realizate folosind 16 microfoane de la același smartphone (un Samsung Galaxy S6) care au fost utilizate pentru a capta zgomote de pe drum și din vehicul (locomotivă, barieră, claxonul mașinii și scarțâitul roților mașinii). Aceste sunete au fost redate de un sistem audio de înaltă fidelitate. Pentru scenariul C a fost creat un set de date live prin înregistrarea sunetului cu 16 smartphone-uri atât în afara cât și în interiorul unei mașini. Fiecare smartphone înregistrează trei sunete diferite: claxonul mașinii, sunetul avariilor și al ștergătoarelor. S-a introdus un zgomot suplimentar pentru toate scenariile pentru a face clasificarea mai dificilă. Ultimul scenariu a fost cu atât mai provocator. Când s-a adăugat zgomot, clasificatorul LD produce rezultate slabe de identificare pentru două telefoane (LG și Nexus 7). Clasificatorul LD poate fi totuși preferat deoarece utilizează puțină memorie și are o durată de rulare scurtă. Alte clasificatoare convenționale au avut rezultate mai slabe decât LD în ceea ce privește acuratețea. Clasificatorul LD a acţionat perfect în primele două cazuri. Aceste amprente digitale au o gamă largă de potențiale utilizări. De exemplu, verificarea dreptului de proprietate asupra unui anumit telefon pentru a servi la autentificare folosind caracteristici fizice care nu pot fi clonate. Cu toate acestea, astfel de amprente digitale ar putea fi, de asemenea, folosite abuziv de aplicații mobile pentru a amprenta dispozitive fără acces la identificatori unici ai dispozitivului. Aplicațiile rău intenționate (sau bibliotecile ascunse) cu acces de înaltă fidelitate la datele de la microfon au deja un impact mai semnificativ asupra securității și confidențialității [17] decât asupra amprentei digitale a dispozitivului.

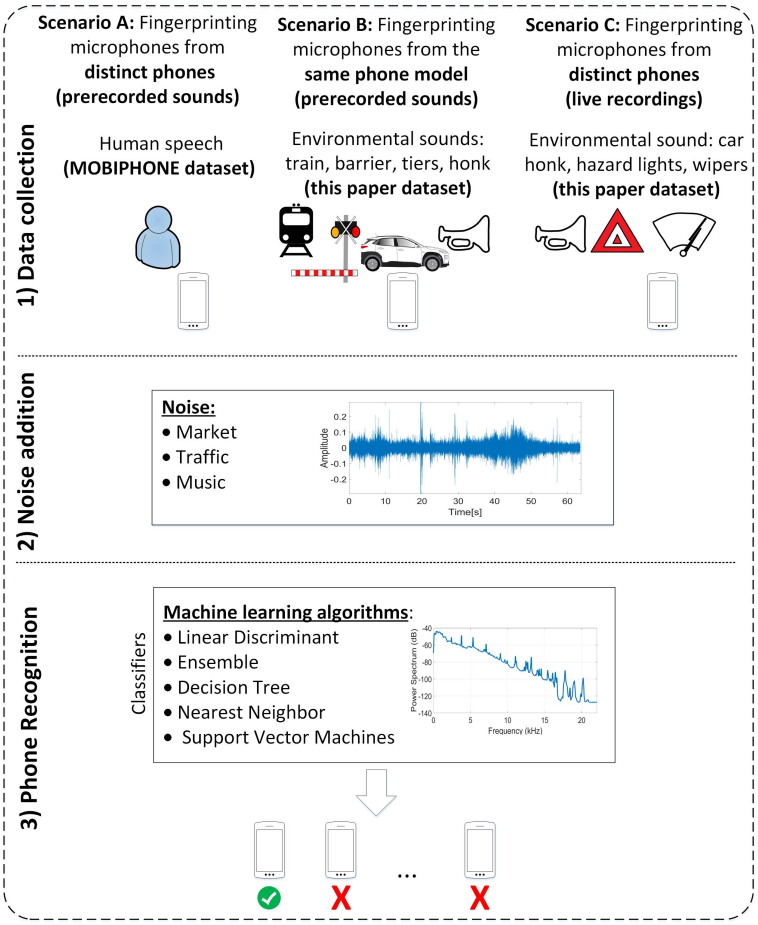

Fig. 4. Prezentare generală a metodologiei și scenariilor utilizate în capitolul V

În capitolul VI, amprentele smartphone-ului pe baza camerei au fost de asemenea investigate utilizând coeficienţii AC de frecvenţă medie și joasă obţinuţi aplicând transformata cosinus discretă 2-D (2-D DCT) pe fotografii întunecate. Conform analizei, canalul albastru este mai eficient în recunoaşterea camerei. O imagine întunecată trebuie facută în acest scop, ţinând smartphone-ul în palma utilizatorului. Șase algoritmi de clasificare au fost folosiți pentru identificarea dispozitivelor (Nearest Neighbor (KNN), Ensemble-Subspace Discriminant, Support Vector Machines, Linear Discriminant, Naive Bayes și o rețea neuronală wide.). Pentru clasificare, 50 de fotografii au fost colectate folosind şase camere identice de la Samsung Galaxy J5. Pentru a elimina zgomotul a fost foloist un filtru adaptiv 2-D din Matlab numit filtru wiener2. Folosind 10x10 vecini, acest filtru calculează varianța și media locală din jurul fiecărui pixel. Pentru a recupera variațiile pixelilor, zgomotul rezidual a fost calculat ca diferență între imaginea originală și imaginea filtrată. Zgomotul rezidual a fost împărțit în blocuri de 8x8 care nu se suprapun. Transformata cosinus discretă 2-D (2-D DCT) a fost calculată pentru fiecare bloc și au fost extrași coeficienții AC de frecvență joasă și medie. Fiecare bloc de 8x8 a fost convertit într-o matrice de 35 de elemente, care a fost apoi concatenată pentru a produce amprenta. Pașii

de procesare sunt descriși în Figura 5. Datorită constrângerilor de memorie și a timpului de procesare, au fost folosite doar 100 sau 1000 de rânduri de câte 35 de coloane din fiecare imagine ca intrare pentru clasificatoare. Reţeaua neurală (WNN) a avut cele mai bune rezultate, ajungând la o precizie de 97% pentru 1000 de caracteristici şi aproximativ 70% pentru 100 de caracteristici. Algoritmul convenţional KNN, de asemenea, a dat rezultate promiţătoare, cu o precizie de aproximativ 80% pentru 100 şi 1000 de caracteristici. Pentru a demonstra nivelul de securitate, au fost calculată entropia Shannon și entropia minimă atât pe imaginea originală cât și pe coeficienții AC extrași. Nivelul de securitate este suficient de bun, deoarece cea mai scăzută entropie este de 2-3 biți pentru fiecare octet din coeficienți, ceea ce este de două ori mai mult decât în cazul imaginilor neprocesate.

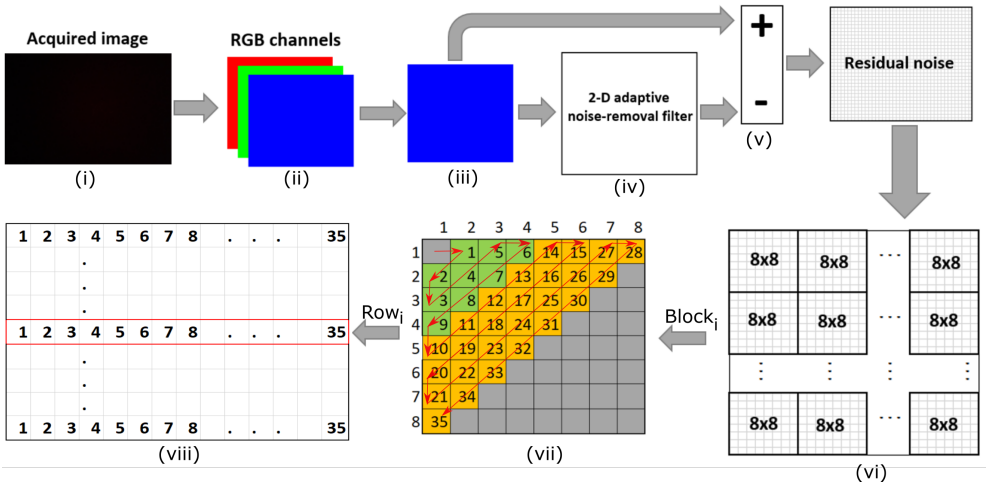

Fig. 5. Procesul de extragere al amprentelor: de la capturarea imaginii până la extragerea coeficienților AC

Nu în ultimul rând, în capitolul VII, datorită interesului autorului în domeniul securității automotive, un obiectiv secundar al cercetării actuale a fost aplicarea tehnologiilor de amprentare pe ECU-urile (Electronic Control Units) din mașini. Deoarece un set de date care conține amprente fizice era deja public [18], aplicarea clasificatoarelor anterior folosite din Matlab a fost imediată. Acest capitol prezintă rezultatele autorului în această direcție și nu este surprinzător faptul că aceste tehnicile care dau rezultate bune pentru smartphone-uri, funcționeaza bine și în acest domeniu. Cinci algoritmi de clasificare: Linear Discriminant (LD), Decision Trees (Tree), SVM, KNN și wide neural network (NN) au fost folosiți și pentru smartphone-uri, dar au fost folosiți și aici pentru a clasifica 51 de ECU-uri pe baza unui set de date disponibil public. Clasificatoarele au fost testate pe toate caracteristicile din setul de date. Când au fost utilizate toate caracteristicile, NN a atins o precizie de 99,9%, iar când au fost folosite numai două caracteristici, performanța clasificatorului KNN nu a fost atât de bună, ceea ce sugerează, aşa cum este deja cunoscut în literatura de specialitate, că un număr redus de caracteristici nu este suficient pentru clasificarea corectă.

Capitolul VIII concluzionează această teză. Pentru a rezuma, această teză a furnizat rezultate pozitive pentru clasificarea smartphone-urilor pe baza datelor colectate de la 4 traductoare: accelerometre, difuzoare, microfoane şi camere. Una dintre principalele constatări ale acestei teze a fost că algoritmii tradiționali de clasificare pot da rezultate chiar mai bune decât rețelele neuronale complexe pentru amprentarea senzorilor. De asemenea, seturile de date cuprinzătoare

cu datele colectate de la difuzoare și microfoane, care au fost folosite pentru evaluarea a peste 60 de smartphone-uri au fost făcute publice. Rezultatele din această teză de doctorat au fost prezentate şi acceptate pentru publicare în reviste şi conferinţe ISI relevante.

REFERINȚE

[1] K. Lofstrom, W. R. Daasch, and D. Taylor, "Ic identification circuit using device mismatch," in *2000 IEEE International Solid-State Circuits Conference. Digest of Technical Papers (Cat. No. 00CH37056)*. IEEE, 2000, pp. 372–373.

[2] B. Gassend, D. Clarke, M. Van Dijk, and S. Devadas, "Silicon physical random functions," in *Proceedings of the 9th ACM conference on Computer and communications security*, 2002, pp. 148–160.

[3] B. Groza, A. Berdich, C. Jichici, and R. Mayrhofer, "Secure accelerometer-based pairing of mobile devices in multi-modal transport," *IEEE Access*, vol. 8, pp. 9246–9259, 2020.

[4] A. Berdich, B. Groza, R. Mayrhofer, E. Levy, A. Shabtai, and Y. Elovici, "Sweep-to-unlock: Fingerprinting smartphones based on loudspeaker roll-off characteristics," *IEEE Transactions on Mobile Computing*, 2021.

[5] A. Berdich, B. Groza, E. Levy, A. Shabtai, Y. Elovici, and R. Mayrhofer, "Fingerprinting smartphones based on microphone characteristics from environment affected recordings," *IEEE Access*, vol. 10, pp. 122 399–122 413, 2022.

[6] A. Berdich and B. Groza, "Smartphone camera identification from low-mid frequency dct coefficients of dark images," *Entropy*, vol. 24, no. 8, p. 1158, 2022.

[7] A. Berdich, P. Iosif, C. Burlacu, A. Anistoroaei, and B. Groza, "Fingerprinting smartphone accelerometers with traditional classifiers and deep learning networks," in *2023 IEEE 17th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, 2023.

[8] A. Berdich and B. Groza, "Secure by design autonomous emergency braking systems in accordance with iso 21434," *Machine Learning and Optimization Techniques for Automotive Cyber-Physical Systems*, 2023.

[9] S. Murvay, A. Berdich, and B. Groza, "Physical layer intrusion detection and localization on can bus," *Machine Learning and Optimization Techniques for Automotive Cyber-Physical Systems*, 2023.

[10] B. Groza, H. Gurban, L. Popa, A. Berdich, and S. Murvay, "Car-to-smartphone interactions: Experimental setup, risk analysis and security technologies," in *5th International Workshop on Critical Automotive Applications: Robustness & Safety*, 2019.

[11] A. Berdich, A. Anistoroaei, B. Groza, H. Gurban, S. Murvay, and D. Iercan, "Antares-anonymous transfer of vehicle access rights from external cloud services," in *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*. IEEE, 2020, pp. 1–5.

[12] B. Groza, T. Andreica, A. Berdich, P. Murvay, and E. H. Gurban, "Prestvo: Privacy enabled smartphone based access to vehicle on-board units," *IEEE Access*, vol. 8, pp. 119 105–119 122, 2020.

[13] A. Anistoroaei, A. Berdich, P. Iosif, and B. Groza, "Secure audio-visual data exchange for android in-vehicle ecosystems," *Applied Sciences*, vol. 11, no. 19, p. 9276, 2021.

[14] D. P. Jablon, "Extended password key exchange protocols immune to dictionary attack," in *Proceedings of IEEE 6th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises*. IEEE, 1997, pp. 248–255.

[15] G. Baldini, I. Amerini, and C. Gentile, "Microphone identification using convolutional neural networks," *IEEE Sensors Letters*, vol. 3, no. 7, pp. 1–4, 2019.

[16] C. Kotropoulos and S. Samaras, "Mobile phone identification using recorded speech signals," in *2014 19th International Conference on Digital Signal Processing*. IEEE, 2014, pp. 586–591.

[17] I. Shumailov, L. Simon, J. Yan, and R. Anderson, "Hearing your touch: A new acoustic side channel on smartphones," 2019.

[18] L. Popa, B. Groza, C. Jichici, and P.-S. Murvay, "Ecuprint—physical fingerprinting electronic control units on can buses inside cars and sae j1939 compliant vehicles," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 1185–1200, 2022.